CHANGE HEALTHCARE

EMS Billing Services

RFP # 002-18

Proposal for
City of Key West

Mauricio.Chavez@McKesson.com
Specialty Vice President, EMS
305.970.2780
Mauricio.Chavez@McKesson.com
01.24. 2018

Software and Analytics | Network Solutions | Technology-enabled Services

CHANGE HEALTHCARE

01.24.2018

City Clerk
1300 White Street
Key West, Florida 33040

RE: RFP #002-18 – EMS Billing Services

Dear Members of the Evaluation Committee:

The City of Key West seeks to partner with a billing vendor that can provide timely, accurate, and compliant billing services. Change Healthcare Technology Enabled Services LLC (Change Healthcare) is that vendor. We own our own EMS billing specific software. This means we can interface with your transport hospitals and ePCR solution for faster and more accurate claims processing. In addition, our compliance team maintains current knowledge of all laws affecting EMS billing. We can update our processes quickly to react to changing healthcare regulations because we maintain our own software.

On March 2, 2017, McKesson and Change Healthcare formed a new healthcare information technology and services company to address some of the most pressing and emerging challenges in healthcare. The new company, Change Healthcare, combines most of McKesson's technology businesses with legacy Change Healthcare to deliver wide-ranging financial, operational and clinical benefits to payers, providers, and consumers. McKesson owns approximately 70% of the new company. The new Change Healthcare is one of the largest, independent healthcare technology companies in the United States.

We have 27 years of EMS billing experience. We manage over 200 accounts and process more than one million billable EMS transports every year. This makes Change Healthcare one of the leading EMS revenue recovery companies in America. We specialize in EMS billing and medical revenue management. Our trained personnel and expertise will improve all aspects of your EMS billing and claims management.

The following individuals are authorized to represent Change Healthcare in negotiating and signing any agreement resulting from this proposal:

- Mark Vachon, Executive Vice President, Sales & Operations
- Loretta Cecil, Secretary
- Chris Robertson, Senior Vice President, Operations
- Jimmy Stuart, Senior Vice President Hospital-Affiliated Physicians & EMS Operations

We welcome the opportunity to provide you with more information in an interview with our experienced team. Please contact me if you need further information or to schedule a time for presentations. I look forward to hearing from you.

Change Healthcare
7955 NW 12th Street, Suite 100
Doral, Florida 33126

P 305.229.4302
F 305.229.4322

changehealthcare.com

Sincerely,

Mauricio Chavez

Mauricio Chavez
Specialty Vice President, EMS

P 305.970.2780
E mauricio.chavez@mckesson.com

Confidential Information

The following content in this proposal is confidential and shall not be shared with anyone not involved in the evaluation of this proposal.

- Client descriptions (page 8)
- Client references (page 15)

The information and data contained in this proposal to the City of Key West is (i) confidential and proprietary commercial or financial information of Change Healthcare Technology Enabled Services LLC (Change Healthcare) and (ii) provided for exclusive use in evaluating a business arrangement between the City of Key West and Change Healthcare. Notwithstanding anything to the contrary in this proposal, Change Healthcare is the sole owner of the material in this proposal, and Change Healthcare retains all rights, title, and interest thereto

Contents

1. Cover Letter i
2. Response to RFP **1**
3. Attachments **16**
Table of Attachments **32**

2. Response to RFP

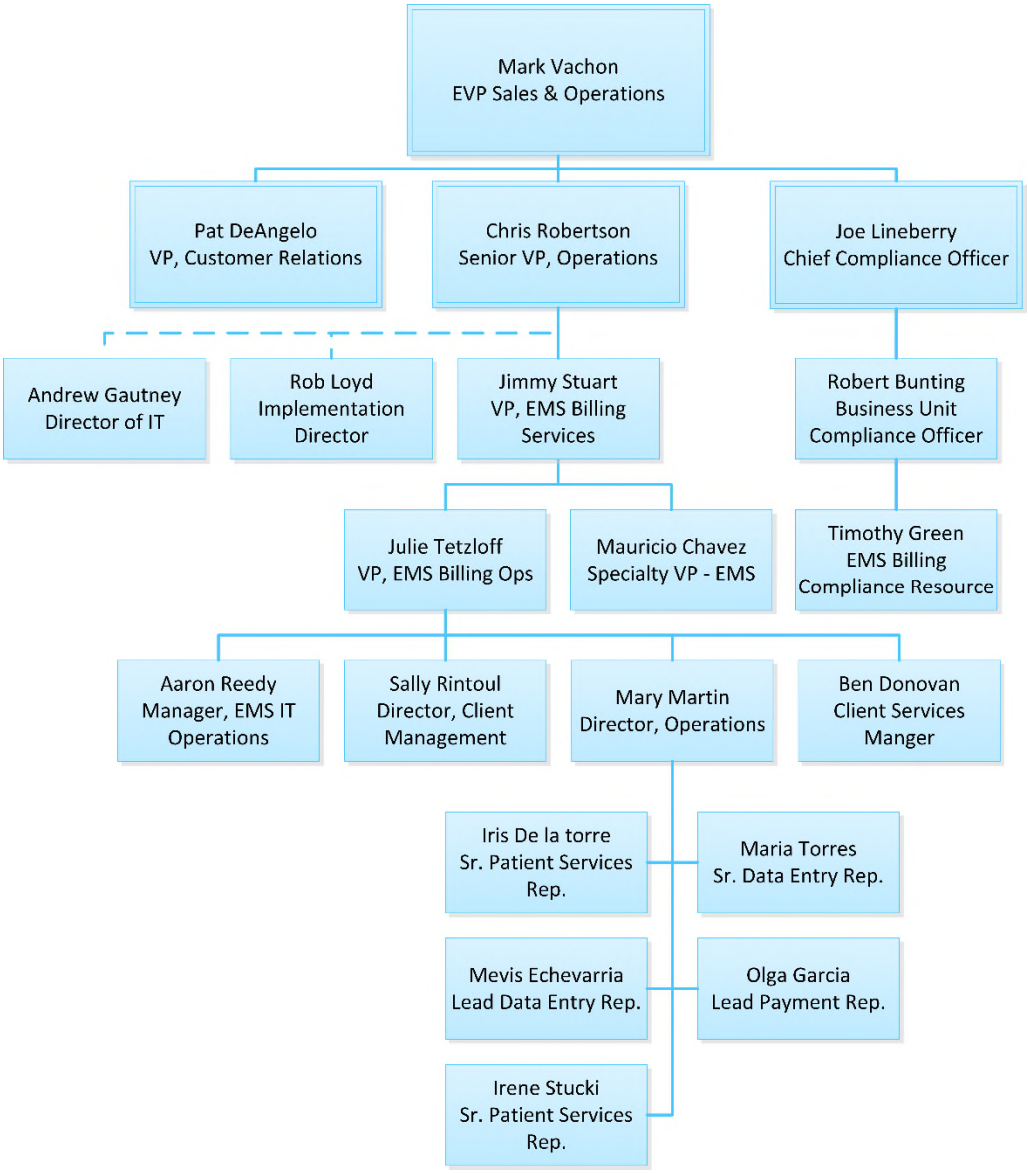
Organization chart, number of employees, company information (founding and history, service areas, and awards or other forms of recognition), financial information (filed for bankruptcy in the past, is currently in bankruptcy or has bankruptcy action pending), litigation (list project name and nature of litigation of any past, pending or present litigation, arbitration or dispute relating to the services described herein, that you or your firm has been involved in within the last five (5) years), summary of current workload.

On March 2, 2017, McKesson and Change Healthcare formed a new healthcare information technology and services company to address some of the most pressing and emerging challenges in healthcare. The new company, Change Healthcare, combines most of McKesson's technology businesses with legacy Change Healthcare to deliver wide-ranging financial, operational and clinical benefits to payers, providers, and consumers. McKesson owns approximately 70% of the new company. The new Change Healthcare is one of the largest, independent healthcare technology companies in the United States.

Change Healthcare Technology Enabled Services LLC is financially stable. Change Healthcare is a joint venture of McKesson Corporation, a Fortune 5 company with $192.5 billion in annual revenue, and The Blackstone Group with $7.5 billion in annual revenue. Change Healthcare Technology Enabled Services LLC is formerly a subsidiary of McKesson Corporation, a publicly traded company. As of March 2, 2017, Change Healthcare Technology Enabled Services LLC is an affiliate of Change Healthcare, which holds public debt, and therefore conforms to public reporting requirements. Correspondingly, information about the affiliated companies, including information about material litigation or regulatory investigations, is available in the annual and quarterly reports that are filed with the Securities and Exchange Commission. The annual and quarterly reports of Change Healthcare Technology Enabled Services LLC are available at www.mckesson.com under the Investors link.

We have 27 years of EMS billing experience. We manage over 200 accounts and process more than one million billable EMS transports every year. This makes Change Healthcare one of the leading EMS revenue recovery companies in America. We specialize in EMS billing and medical revenue management. Our trained personnel and expertise will improve all aspects of your EMS billing and claims management.

Change Healthcare has approximately 12,380 team members. Our EMS billing division includes approximately 220 team members. The following is an organization chart for the Doral, Florida EMS billing Center of Excellence that will provide billing services and manage the City's account.



- **Qualifications: Please provide documentation of the professional qualifications of the key personnel to be employed. Such documentation shall include, but not be limited to:**

  1. **Resumes of academic training and employment in the area of EMS Billing**

Our experienced team of professionals has the education and training necessary to implement and manage a successful ambulance billing program for you. In addition to these lead team members (biographies below), we will also assign your account to a billing team to ensure we have an adequate number of specialists and resources to serve you. We are proud of the strength of our team and encourage your selection staff to read the following biographies.

Mark Vachon – Executive Vice President, Sales & Operations

Mr. Vachon is EVP & President, Sales and Operations at Change Healthcare. Prior to this, he was an Operating Advisor to Thomas H. Lee Partners. He has over 30 years of operating experience at General Electric and is a former GE Company Officer and Member of the GE Corporate Executive Council. Mr. Vachon was the President and CEO of GE Healthcare Americas, where he led the ground-up development of the Americas $9B region (U.S., Canada, Latin America) and President and CEO of GE Global Diagnostic Imaging, where he led the turnaround and rebranding of the largest product and service business ($8B) within GE's Healthcare division. Prior to these roles, Mr. Vachon was the Executive Vice President & CFO of NBC. He also served as GE's Vice President of Investor Relations and held numerous financial and operating roles after starting his career with GE in 1982. Mr. Vachon is on the board of bluebird bio, Numotion Mobility, Northeastern University and the Charitable Health and Retirement Trust. He holds a B.S. from Northeastern University and an M.A. from Boston College.

Christopher Robertson, MHA, Vice President

Mr. Robertson is vice president of operations for our revenue cycle management business. He has been with our company since May 1999. Starting his Change Healthcare career as an account manager, he advanced to regional vice president, and, in 2004, was named vice president for the west division of radiology operations. Mr. Robertson holds a Bachelor of Science in Biology and a Master of Health Administration from the University of Missouri.

Jimmy Stuart, Senior Vice President, Hospital Affiliated Physicians and Emergency Medical Services Operations

Mr. Stuart has responsibility for hospital affiliated physicians operations including emergency medicine, emergency medical services, and anesthesia revenue cycle management services. In his previous position, he was responsible for the radiology operations in the eastern United States. He joined the company in 1995, has served in various radiology operational roles for the past 15 years, and was previously responsible for the southeast operations. Mr. Stuart earned his Bachelor of Business Administration degree from Texas Tech University and Master of Business Administration degree from the University of West Florida.

Patrick DeAngelo, Vice President and Chief Information Officer

Joining our team in 2005, Mr. DeAngelo is currently responsible for information security, infrastructure, development, implementation, optimization and maintenance of all information technology systems. He has over 15 years of healthcare financial operations management and technical experience for the two largest companies in the business, Siemens and McKesson. He was a major contributor in developing the technical and operational BPO infrastructure for Siemens Medical Solutions, Zavata, and McKesson.

Kenneth E. Hooper, CPA/CFF, CFE, CHC, Interim Chief Compliance Officer Change Healthcare Technology Related Services

Mr. Hooper is a licensed Certified Public Accountant in Georgia, Idaho, and Washington as well as a Certified Fraud Examiner and Certified in Healthcare Compliance. Mr. Hooper has been retained as a compliance officer or consulted on compliance matters for hospitals, third-party billing companies, home health and hospice agencies and physician practices for over 30 years. Mr. Hooper has testified, been deposed, or consulted on cases in both Federal and state courts and has served as an independent review organization member and compliance and ethics board member for providers in compliance with Office of Inspector General Corporate Integrity Agreements.

Joe Lineberry, Vice President of Operations, Coding

Mr. Lineberry leads our Coding and Compliance Advocate offerings, encompassing Facility and Professional Coding, Clinical Documentation Improvement, Auditing and Consulting Services. Since joining our team in 1997, Mr. Lineberry has also served as the Chief Compliance Officer of our Revenue Cycle Services business, and prior to joining our team, Mr. Lineberry served as a claims manager for CIGNA Healthcare in Atlanta, Georgia. He is Nationally Certified in Healthcare Compliance and previously served as a Coding Instructor of the American Academy of Professional Coders Certified Professional Coder Curriculum at Herzing College in Atlanta, Georgia. Mr. Lineberry's areas of expertise include denial management, Medicare billing regulations, coding, compliance plan development, and clinical documentation analysis for completeness. His payer and billing company experience provides unique insight to help clients resolve coding, billing, and compliance challenges.

Robert P. Bunting, CPC, CPC-H, CHC, CEDC, CEMC – Compliance Program Director, Emergency Medicine and Hospitalists

Mr. Bunting is the Compliance Program Director (CPD) for EMS billing. Since 1995, he served as a medical coder, Quality Assurance team member, Assistant Coding Group Leader, Facility Coding Manager, Account Manager, and in 2002 assumed the role as Compliance Program Manager (CPM), now Compliance Program Director (CPD). Mr. Bunting holds a Bachelor of Business Administration, Finance Track degree, from the University of North Florida (UNF), is a Certified Professional Coder (CPC), Certified Professional Coder – Hospital (CPC-H), and Certified in Healthcare Compliance (CHC), Certified Professional Coder – Emergency Department Services (CEDC), Certified Professional Coder – Evaluation and Management Auditor (CEMC). He is also a member of the American Health Information Management Association (AHIMA). Prior to his employment with our team, Robert served in the United States Navy for 8-1/2 years as a legal Yeoman for administration. Robert's focus in coding and compliance efforts has been in Emergency Medicine and Hospitalists services since his initial employment with our team.

Timothy Green, CAC, CACO, CAPO, CADS – EMS Compliance Training/Compliance Instructor

Mr. Green is the compliance liaison for our EMS billing division and reports to Mr. Bunting. He is a former EMS Director with over 30 years' experience as a firefighter/paramedic and is a graduate of the National Fire Academy (NFA) EMS Leadership, Advanced EMS Leadership and Command and Control of Fire Department Operations Courses. He has an associate degree in Fire Sciences and Emergency Medical Services from Sinclair Community College in Dayton, Ohio and has completed multiple leadership courses at the Ohio Fire Academy. Mr. Green also completed the Ohio State University, Management Series while employed with the Kettering Fire Division.

After retiring from the fire service, he was hired as the Operations Manager for careNOW, an innovative pathway management project owned by Premier Healthcare Services and the Greater Dayton Hospital Association in Dayton, Ohio. Mr. Green has also worked in the EMS transport billing industry for almost 18 years, helping to build a high-performance billing company, focused on emergency transports. During that time, he was the Director of Client Services for MBI-Solutions, Fire/EMS Division and later he became the Director of Client Services, for MED3000, Fire/EMS Division in Ohio.

Mr. Green is also a member the International Association of Fire Chiefs (IAFC), EMS Section and the International Association of Firefighters (IAFF). He currently holds certifications as a Certified Ambulance Coder (CAC), Certified Ambulance Compliance Officer (CACO), and a Certified Ambulance Privacy Officer (CAPO). Tim's job functions focus on EMS compliance, training and coding.

Rob Loyd, Director of Implementations

Mr. Loyd is responsible for leading our implementations team in its commitment to the development of successful long-term partnerships with our new office-based, hospital-based, and academic clients. He and his team provide accountability in all implementation tasks using well-planned and documented transition services that deliver predictable and consistent results. Beginning his career with our company in 1994 as an operations manager, Rob has had the opportunity to work in various arenas of revenue cycle management including front-end and back-end processes, as well as high-level interface development/management skills. His roles with the organization include operations manager, system support manager, process improvement analyst, business analyst, project manager; and interface development manager.

Julie Tetzloff, Vice President, Operations Emergency Medical Services Billing

Ms. Tetzloff is responsible for operations and account management in the Emergency Medical Services billing division of Change Healthcare. She has been with the company since 1996 and has served in various roles during her tenure. She has experience with operations, account management, Six Sigma process improvement methodology, new client implementations, and acquisition integration. Ms. Tetzloff earned her Bachelor of Arts degree from Miami University and a Master of Public Health degree from Tulane University.

Mauricio Chavez, Specialty Vice President – EMS

Mr. Chavez is responsible for all EMS billing operations in our Doral, Florida EMS billing Center of Excellence. He is responsible for overall client satisfaction. Mr. Chavez meets with clients on an as needed basis to tackle issues, answer questions, review financials, provide training, and other responsibilities that arise in the day-to-day business operations. Mr. Chavez joined our company in 1989. Through the years, he has served in many roles with in the company, from computer operations, programming, report writing, client management, and director of operations.

Mary Martin, Director of Operations

Ms. Martin is responsible for overseeing the day-to-day operations of data entry, payment posting, coding, customer service, and AR management departments. Her experience and attention to detail is what sets her apart from others. She has worked with all EMS agencies that are processed from the EMS Center of Excellence in Doral, Florida. Change Healthcare recognizes her 40+ years of service with the company.

Sally Rintoul, Director, Client Management, EMS billing

Ms. Rintoul started with our company in June 2016, having spent over 20 years in the physician practice management and billing arena. She has served as executive director for large anesthesiology practices in Cleveland and Cincinnati. Most recently, she was in client management for anesthesiology practices throughout Ohio. Ms. Rintoul has managed large physician practices throughout Ohio and has extensive experience in revenue cycle management, compliance, and contracting. She has been an active member of MGMA, having spoken at many conferences and earned her Certified Medical Practice Manager status. She holds a BS degree from Miami University, an MBA from the University of Cincinnati and is a CPA.

Benjamin Donovan, Client Manager

Mr. Donovan has been with our company for five years and is responsible for the overall performance of client accounts. He ensures goals are being met and challenges are overcome. Mr. Donovan meets with clients, engages in strategic planning, performs data analysis, and consults with clients about changes occurring in the industry.

Aaron Reedy, IT Manager EMS Billing Division

Mr. Reedy leads the EMS billing information technology team. He is also the data manager for the Columbus Division of Fire project, a significant Change Healthcare client. Since beginning that role in December 2007, he has been instrumental in the success of this project, assuring excellent customer service and quick responses. Before that, Mr. Reedy worked at T. Marzetti Company as supervisor of EDI and network services. From June 1995 to October 2007, he was responsible for taking that company from 50 stand-alone PCs to a networked system of 400+ PCs and servers. As lead EDI person, he was responsible for electronic processing of all business documents between 300+ trading partners. He managed a team of PC and network personnel who provided 24/7 support for over 800 users and 25+ locations across the country. Since 2000, Mr. Reedy has been the Clerk-Treasurer for the Village of Thurston, OH; he manages every financial aspect for the Village and provides advice to the other elected officials.

In addition to Mauricio and Mary (resumes provided in the Attachments section of our proposal), the below billing specialists will manage the day-to-day billing activities for the City. These individuals have a long tenure with our company and significant EMS billing expertise.

Mevis Echeverria, Data Entry

Ms. Echeverria has been working with Change Healthcare in a data entry capacity for over 25 years. In that time, she has worked with many EMS billing accounts. She has extensive knowledge of what data is needed for the billing process.

Maria Torres, Data Entry

Ms. Torres has been working for Change Healthcare for over 15 years in the data entry department. She currently performs data entry for many of our EMS billing clients.

Olga Garcia, Payment Posting

Ms. Garcia has been working for Change Healthcare for over 35 years. She has extensive experience with the posting of monies to accounts, balancing to lockboxes, and processing refunds for clients.

Iris De La Torre, Governmental Specialist

Ms. De La Torre has been working with Change Healthcare for over 25 years. She has extensive experience in working with governmental payers to get your claims paid. She oversees all Medicare and Medicaid denials, submits claims for review, tracks trends, and provides feedback to upper management. Iris has the appropriate training so that she can stay on top of all changes to governmental payer's rules and regulations. She currently oversees all the of governmental payer denials for all EMS billing clients for Change Healthcare.

Irene Stucki, Accounts Receivable Management Specialist

Ms. Stucki has been working with Change Healthcare for 25 years. Her expertise is in working accounts receivables to maximize revenues for our clients. She has been working on EMS billing accounts since she began with Change Healthcare in 1990.

2. **Include three (3) examples of EMS Billing including pricing methodology used.**

City of Miami, Florida

Change Healthcare has been providing EMS billing services to the City of Miami for over a decade. Revenue for the City of Miami has increases year over year. In addition to excellent customer service and superior reporting tools, Change Healthcare has provided several training sessions to all City of Miami Fire Rescue personnel to ensure that patient care reports are documented appropriately. In fiscal 2014, Change Healthcare increased the revenue for the City of Miami by over one million dollars.

Change Healthcare also provides EMS billing services for some of Miami's neighboring cities – such as Village of Key Biscayne and the City of Coral Gables.

Indian River County, Florida

One of our first steps upon contracting with Indian River was to establish electronic interfaces with each of the hospitals that receive Indian River patients. Before the end of the first fiscal year, Indian River's cash collections had jumped nearly 30%. Over time, their gross collection rate has increased to 66%; the national average is about 50%. Indian River's current revenue per transport is $343.

Fernandina Beach, Florida

The City of Fernandina Beach contracted with Change Healthcare to provide EMS billing services in June 2009. Fernandina Beach is on Amelia Island and is among Florida's northernmost cities. With a mix of permanent residents and many tourists, they have their own unique set of challenges when it comes to ambulance billing. They chose Change Healthcare from over 10 vendors during the RFP process in 2009. Fernandina Beach was looking for a company that could improve its collection rate, improve patient response times, and improve the customer service provided to the City. Upon taking over, we met all three of these objectives and subsequently took over the AR from the previous vendor. When it came time to renew the contract in June 2014, the City of Fernandina did not hesitate, and signed a new five-year deal with Change Healthcare. Change Healthcare currently collects $330 per transport for the City of Fernandina Beach.

Lee County, Florida

Lee County EMS chose Change Healthcare to provide a full spectrum of revenue cycle management services following a rigorous RFP process. Services include coding, claims, collections, compliance, customer service, denial management, and business intelligence reporting. Change Healthcare began billing in October 2014. In the County's last fiscal year, Change Healthcare exceeded collection expectations by $2 million.

Billing methodologies: All the clients listed bill all patients in the same manner – regardless of residency status. However, we do have clients that write-off a patient's balance if the patient happens to be a resident of the municipality. In those cases, a Request for Information letter may still be sent to the patient to obtain insurance or other needed information. Once the

insurance pays, the balance is written off. If the patient is a resident and a self-pay with no insurance, the account is written off. Other clients may do a form of "soft billing" for residents where only one statement is sent and the account is written off if it is not paid. We can certainly discuss the different options available to the City.

- **Program Approach and Price: Please submit a program approach for the completion of the scope of services requested above and price for a three (3) year period. The approach and price, at a minimum, shall include the following:**

  1. **From a technical perspective, explain why your organization should be selected for performing the services covered under this Request for Proposals and how you can add value to the goals and objectives of the City. Include examples of your success in performing such services with other entities.**

     The following elements are true differentiators between Change Healthcare and our competitors and allow us to provide outstanding EMS billing services to our customers.

     - Unlike most other billing vendors, we own virtually every significant software system, tool, and process involved in revenue cycle management. Owning all pieces of the billing process end-to-end allows us to eliminate paperwork, accelerate processing, and reduce costs through automated processing.
     - We provide billing services using our own platform, MDIV, supported by a team of 29 information technology professionals. A team of 29 professionals, including nine full-time programmers, provides customization to our proprietary billing platform, MDIV to meet your program requirements. Using our own billing software system allows us to respond rapidly to changes in the market for our expanding client base.
     - Because we own and develop our billing platform, we can capture and report on virtually any data element you request. Our billing platform, MDIV, feeds a sophisticated data warehouse that houses our clients' data. Our clients use this warehouse to access custom reports, standard reports, and inquiries. Practice Focus, our business intelligence and reporting tool, enables our clients to access medical billing and accounts receivable management information on-demand using a Web browser and any Internet-enabled device. From high-level dashboards to drill-down and linked reports that provide the detail to make changes, Practice Focus helps get the answers needed to improve your performance. Custom dashboards, predefined alerts, dynamic charts, and flexible reports enable you to monitor key performance indicators and identify trends unique to you.
     - We put your customers first because we understand the special bond that exists between you and the citizens you serve. Our communication with your customers on a day-to-day basis is professional, and we will conduct all interactions, whether verbal or written, with the highest standards. We have the experience, expertise, and passion to you with your ambulance billing program. We possess extensive knowledge and professional relationships with many EMS agencies, not only in the state of Florida, but throughout America.

- We have an unparalleled commitment to compliance invest more money in ensuring we are always compliant in every aspect of our business than any other vendor.
- We are the only billing company that owns its own clearinghouse. Relay Health, our internal electronic clearinghouse, used by many billing vendors to manage their electronic transactions. Our system manages over 1.9 billion financial transactions annually, valued at over $1.1 trillion. Many billing vendors use our clearinghouse solution to manage their electronic transactions. Relay Health also provides an online insurance verification tool, providing the ability to confirm insurance coverage before filing a claim.
- We have the financial stability of a large company and yet we are still able to offer you personalized service like that of a small billing company. Because our business is divided by specialty, we can staff our programs with individuals with significant ambulance billing-specific experience and we can provide personalized service. The stability of our company provides us with the technology, people, and economic resources to provide the City of Key West with outstanding EMS billing services.

2. **From a logistics perspective, explain how your organization intends to interact and interface with the City in the performance of the Services covered under the Request for Proposals.**

   We will always interact with the City in a professional and courteous manner. Our number one priority is to provide outstanding service to our customers. We can provide this high level of service because we use take a team approach to managing our client accounts. However, your client manager is your number one contact. He or she will meet with the City for in-person meetings on a regular basis. Your client manager will also communicate with the City as needed via phone calls, webinars, video chat, and emails.

   You will always be free to contact the person who you feel is best suited to answer your questions quickly. You will not only have access to your client manager, you will also have access to our operations director, our data entry director, and our payment posting supervisor. Of course, you can always choose to call your client manager and he or she will obtain the answer you need. If your client manager is on vacation, we will provide clear direction on who to call, and that person will provide the same high level of service to which you are accustomed.

   If you ever feel that you are not receiving superior customer service, you can escalate your concerns to Change Healthcare management – this has never happened.

3. **Specify address of Firm's designated office where the majority of work on this project will be performed, call center location. Indicate percentage total overall of the Services to be performed by the Firm's office specified above. Specify address of Firm's other office(s) where any part of the work for these Services will be performed, if applicable.**

   We will perform all billing activities from our Doral, Florida EMS billing Center of Excellence. Our office in Doral is the closest billing office to the City of Key West of all our competitors.

4. **Describe any limitations that may exist that would impact your organization's ability to perform the services covered under this RFP.**

   We do not know of any limitations that exist that would impact our ability to perform the services covered under this RFP.

5. **Proposed price for EMS Billing Services as specified in the Scope of Services.**

   Change Healthcare will provide the services described in this proposal for 8.50% of net cash receipts for the duration of any agreement between the City of Key West and Change Healthcare. We will charge a flat fee of $7.00 per Medicaid claim pursuant to Florida law.

   Percentages defined are the percentage of revenue collected each month by Change Healthcare on behalf of the City of Key West. We define net cash receipts as gross cash receipts less refunds.

   The fees quoted above include comprehensive EMS billing services and ESO ePCR software as well as the following:

   Annual Audit: Estimated value - $5,000 (required per the City's RFP)

   Bank Lockbox Fees: Estimated value - $4,800 (use of a lockbox is an industry standard and is the safest way to manage the City's money.

   Hardware:

Getac V110-G3 11.6" Rugged Convertible Laptop				
Model #	**Description**	**Qty**	**Unit Price**	**Extended Price**
VE21YQKABHXX	V110 G3 Premium Getac - Intel® Core™ i5-6200U Processor 2.3GHz, 11.6" With Webcam, Microsoft Windows 10 Professional x64 with default RAM 4GB, OPAL 2.0 128GB SSD, Sunlight Readable (LCD+ Touchscreen), Multi language + US KBD + US Power cord, Mechanical Backlit KBD, Wifi+BT+ GPS + Gobi + Passthrough, Without any extra option, Default -21C, IP65, HD webcam, Smart Card Reader, 3 Year B2B Warranty	8	$3,042.00	$24,336.00

6. **Any other material as may be helpful to establish that the respondent has the necessary facilities, ability, and financial resources to furnish the required services in a satisfactory manner.**

   Change Healthcare Technology Enabled Services LLC, a Change Healthcare company, is financially stable. Change Healthcare is a joint venture of McKesson Corporation, a Fortune 5 company with $192.5 billion in annual revenue, and The Blackstone Group with $7.5 billion in annual revenue. As such, we have the financial resources necessary to support the needs of a new client.

   The following elements are true differentiators between Change Healthcare and our competitors.

   - Unlike most other billing vendors, we own virtually every significant software system, tool, and process involved in revenue cycle management. Owning all pieces of the billing

process end-to-end allows us to eliminate paperwork, accelerate processing, and reduce costs through automated processing.

- We provide billing services using our own platform, MDIV, supported by a team of 29 information technology professionals. A team of 29 professionals, including nine full-time programmers, provides customization to our proprietary billing platform, MDIV to meet your program requirements. Using our own billing software system allows us to respond rapidly to changes in the market for our expanding client base.
- Because we own and develop our billing platform, we can capture and report on virtually any data element you request. Our billing platform, MDIV, feeds a sophisticated data warehouse that houses our clients' data. Our clients use this warehouse to access custom reports, standard reports, and inquiries. Practice Focus, our business intelligence and reporting tool, enables our clients to access medical billing and accounts receivable management information on-demand using a Web browser and any Internet-enabled device. From high-level dashboards to drill-down and linked reports that provide the detail to make changes, Practice Focus helps get the answers needed to improve your performance. Custom dashboards, predefined alerts, dynamic charts, and flexible reports enable you to monitor key performance indicators and identify trends unique to you.
- We put your customers first because we understand the special bond that exists between you and the citizens you serve. Our communication with your customers on a day-to-day basis is professional, and we will conduct all interactions, whether verbal or written, with the highest standards. We have the experience, expertise, and passion to assist you with your ambulance billing program. We possess extensive knowledge and professional relationships with many EMS agencies, not only in your region, but throughout America.
- We have an unparalleled commitment to compliance invest more money in ensuring we are always compliant in every aspect of our business than any other vendor.
- We are the only billing company that owns its own clearinghouse. Relay Health, our internal electronic clearinghouse, used by many billing vendors to manage their electronic transactions. Our system manages over 1.9 billion financial transactions annually, valued at over $1.1 trillion. Many billing vendors use our clearinghouse solution to manage their electronic transactions. Relay Health also provides an online insurance verification tool, providing the ability to confirm insurance coverage before filing a claim.
- We have the financial stability of a large company and yet we are still able to offer you personalized service like that of a small billing company. Because our business is divided by specialty, we can staff our programs with individuals with significant ambulance billing-specific experience and we can provide personalized service. The stability of our company provides us with the technology, people, and economic resources to provide the City of Key West with outstanding EMS billing services.

Best Practices for EMS Coding and Billing

Our billing and collection cycle solution focuses on improving our clients' billing process, resulting in lower costs, increased collections, and more effective accounts receivable management. We achieve this by implementing our Lean Six Sigma best practice process management including specific billing protocols, pre-claims submission editing follow-up, along with payer-specific claims follow-up guidelines, patient/guarantor billing and follow-up, client and staff education, and the overall application of our management methodologies which have proven very effective in other comparable companies.

Our process in handing an account, from start to finish, entails the steps illustrated in the diagram below:

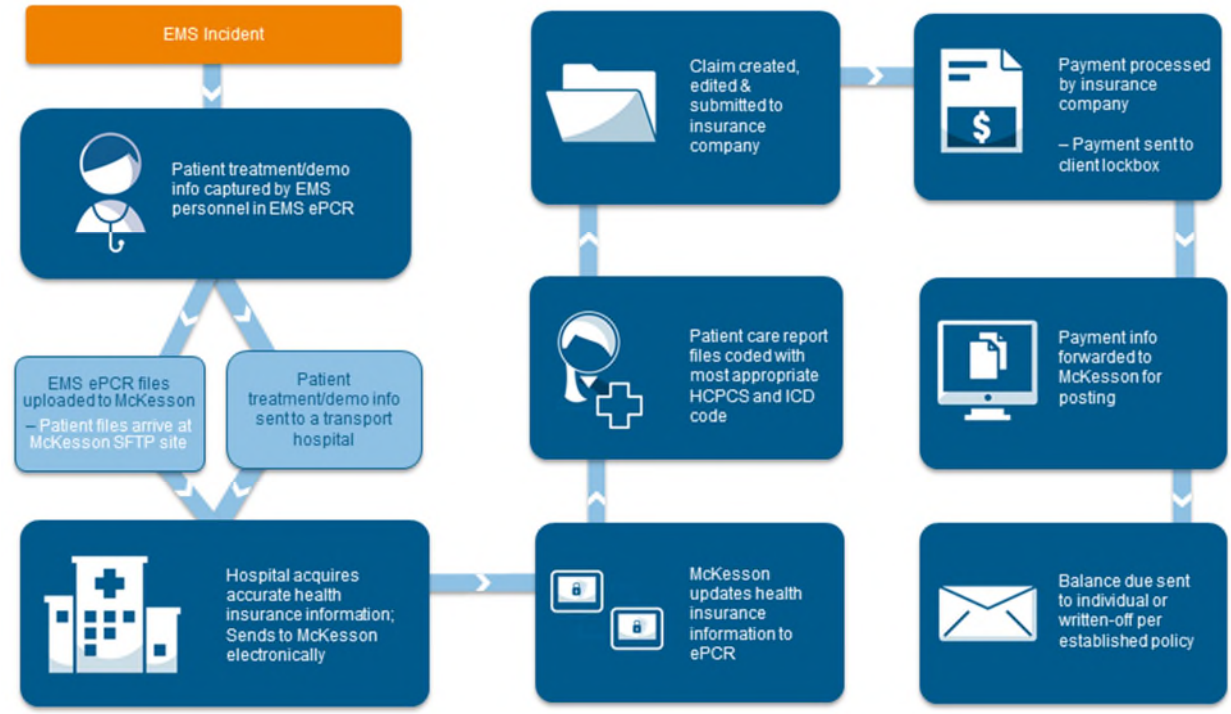


Figure 1: Change Healthcare's Best Practice Process Management using our proprietary EMS billing system. Your revenue cycle processes and collections will improve through our accurate data collection, specific billing protocols, application of pre-claims submission editing, payer-specific claims submission and follow-up, patient/guarantor billing and follow-up, client and staff education, and our management methodologies.

EMS Revenue Cycle Process Overview

1. **Demographics Interfaced** – Our system interfaces with the Hospital Information System (HIS) to import patient demographic information.
2. **Charges Interfaced** – Patient care records interface into the system.
3. **Transports Coded** – Certified coders code and enter transports into EMS Coding. They use web-based Requests for Additional Information (RAI) to clarify missing or incomplete information.

4. **Claims Editing** – The system automatically edits claims. Team members perform rejection follow-up.
5. **Claims Submission** – Claims are generated and sent electronically to our clearinghouse (Relay Health) for transmission to over 1,800 payers, including commercial and government (Medicare, Medicaid, TRICARE, etc.). Claims can also be printed and mailed.
6. **Patient Statements Generation** – We print and mail patient statements for self-pay and patient responsibility billing using the latest in United States Postal Service (USPS)-approved software to ensure we have the most accurate addresses.
7. **Remittance Receipt** – The system automatically receives Electronic Remittance Advices (ERAs) from the payers posts them by line item. Team members key and post paper remittance advices by line item.
8. **Payment Posting** – The system processes and posts payments sent to your lockbox (Electronic Funds Transfer, Cash Deposits, Checks, etc.) by line item.
9. **Payment Verification** – Payments are compared to expected reimbursement. Team members identify, follow-up on, and resolve under-payments and over-payments.
10. **Payer Monitoring and Follow-Up** reports are generated and denials are tracked and resolved.
11. **Accounts Receivable Follow-Up** – Our specialists perform account follow-up with payers and patients to ensure timely payment, including automated outstanding balance reminder calls by our Tele Collect system.
12. **Patient Services** – For inquiries or to make payments, patients can:
    - Contact the Change Healthcare customer service center during normal business hours to speak with a customer service specialist. The toll-free number is printed on their statements.
    - Call the Change Healthcare Integrated Voice Response (IVR) system 24/7 using the same toll-free number as our Customer Service Center which is printed on each statement, and enter their account numbers. Our IVR is HIPAA compliant and has a Spanish speaking option. Through the IVR, your patients (or their guarantors) can:
      - Verify account balances.
      - Confirm insurance information and filing status.
      - Make payments using a credit or debit card.
      - Transfer easily to a customer service specialist (during normal business hours).
    - Visit the Change Healthcare PerYourHealth.com web portal 24/7 using the web address and unique account number and password printed on their statements to securely:
      - Access their balances
      - Update demographic and insurance information
      - Make payments via credit card or debit card or PayPal online.

Due to the page limit stated in the RFP, we are unable to provide a full description of our coding and billing process in this proposal. We are happy to provide to the City upon request, if desired.

- **Familiarity with Florida and the Florida Keys: Describe experience with EMS billing in Florida and, particularly, the Florida Keys.**

  We have been providing EMS billing services to Florida clients for 27 years. Our director of operations grew up in the Florida Keys and has family currently residing there. Most every employee in our Doral Operations Center has traveled to the Florida Keys and are very familiar with the demographics of the City of Key West.

- **Client References: Please provide a minimum of three (3) client references for which you have provided a similar service within the past five years of the scope and nature required by this RFP along with contact name, phone number, and email for the references.**

Change Healthcare EMS Billing Client References			
Organization Name	**Contact Person**	**Telephone**	**Email**
City of Miami Fire-Rescue	Robert Hevia, Assistant Fire Chief	305.416.5404	Robhevia@miamigov.com
Indian River County Fire Department	Brian Burkeen, Chief	772.226.3864	bburkeen@ircgov.com
Coral Gables Fire Department	Marcos De La Rosa, Division Chief	305.460.5771	mdelarosa@coralgables.com

3. Attachments

All required attachments listed in Instructions to Proposer.

13. PROPOSER'S DECLARATION AND UNDERSTANDING

The undersigned, hereinafter called the Proposer, declares that the only persons or parties interested in this Proposal are those named herein, that this Proposal is, in all respects, fair and without fraud, that it is made without collusion with any official of the Owner, and that the Proposal is made without any connection or collusion with any person submitting another Proposal on the Contract Documents.

The Proposer further declares that he has carefully examined the Contract Documents and that this Proposal is made according to the provisions and under the terms of the Contract Documents, which Documents are hereby made a part of this Proposal.

14. ADDENDA

The Proposer hereby acknowledges that he has received Addenda No's. 1, _____, _____. Proposer shall insert No. of each Addendum received and agrees that all addenda issued are hereby made part of the Contract Documents, and the Proposer further agrees that his Proposal(s) includes all impacts resulting from said addenda.

15. SALES AND USE TAXES

The Proposer agrees that all federal, state, and local sales and use taxes are included in the stated unit prices for the work.

BID PROPOSAL FORM

To: The City of Key West

Address: 1300 White Street, Key West, Florida 33040

Project Title: EMS Billing Services

Bidder's contact person for additional information on this Proposal:

Company Name: Change Healthcare Technology Enabled Services LLC

Contact Name & Telephone #: Mauricio Chavez, Specialty Vice President, EMS 305.970.2780

Email Address: Mauricio.Chavez@McKesson.com

BIDDER'S DECLARATION AND UNDERSTANDING

The undersigned, hereinafter called the Bidder, declares that the only persons or parties interested in this Proposal are those named herein, that this Proposal is, in all respects, fair and without fraud, that it is made without collusion with any official of the Owner, and that the Proposal is made without any connection or collusion with any person submitting another Proposal on this Contract.

The Bidder further declares that he has carefully examined the Contract Documents for the construction of the project, that he has personally inspected the site, that he has satisfied himself as to the quantities involved, including materials and equipment, and conditions of work involved, including the fact that the description of the quantities of work and materials, as included herein, is brief and is intended only to indicate the general nature of the work and to identify the said quantities with the detailed requirements of the Contract Documents, and that this Proposal is made according to the provisions and under the terms of the Contract Documents, which Documents are hereby made a part of this Proposal.

CONTRACT EXECUTION AND BONDS

The Bidder agrees that if this Proposal is accepted, he will, within 10 days, not including Saturdays and legal holidays, after Notice of Award, sign the Contract in the form annexed hereto and will provide evidence of holding required licenses and certificates as indicated in the Contract Documents.

CERTIFICATES OF INSURANCE

Bidder agrees to furnish the Owner, before commencing the work under this Contract, the certificates of insurance as specified in these Documents.

ADDENDA

The Bidder hereby acknowledges that he has received Addenda No's. _1___, _____, _____, _____, _____, _____, _____, _____, _____, _____, _____, _____,
(Bidder shall insert No. of each Addendum received) and agrees that all addenda issued are hereby made part of the Contract Documents, and the Bidder further agrees that his Proposal(s) includes all impacts resulting from said addenda.

SALES AND USE TAXES

The Bidder agrees that all federal, state, and local sales and use taxes are included in the stated bid prices for the work.

SURETY

Berkley Insurance Company whose address is

475 Steamboat Road, Floor 1 , Greenwich , CT , 06830
Street City State Zip

BIDDER

The name of the Bidder submitting this Proposal is Change Healthcare Technology

Enabled Services LLC doing business at

7955 NW 12th Street, Suite 100 , Doral , FL , 33126
Street City State Zip

which is the address to which all communications concerned with this Proposal and with the Contract shall be sent.

The names of the principal officers of the corporation submitting this Proposal, or of the partnership, or of all persons interested in this Proposal as principals are as follows:

Neil de Crescenzo, President & CEO	Randy Giles, CFO & Treasurer
Dennis Robbins, VP Finance	Derrick Kirkwood, VP, Tax
Loretta Cecil, Secretary	Denise Ceule, Assistant Secretary
Joe Ashkouti, Assistant Secretary	

If Sole Proprietor or Partnership

IN WITNESS hereto the undersigned has set his (its) hand this _____ day of _____ 2017.

_____
Signature of Bidder

_____
Title

If Corporation*

IN WITNESS WHEREOF the undersigned corporation has caused this instrument to be executed and its seal affixed by its duly authorized officers this 8th day of January 2018.

(SEAL)

Change Healthcare Technology Enabled Services LLC
Name of Corporation

By _____ Mark Vachon

Title Executive Vice President

Attest_____

Sworn and subscribed before this 8th **day of** January, 2018

NOTARY PUBLIC, State of Georgia, **at Large**

My Commission Expires: 03/04/2019

DAWN E HERRINGDINE NOTARY PUBLIC FORSYTH COUNTY, GA MY COMMISSION EXPIRES MARCH 4, 2019

*Change Healthcare Technology Enabled Services LLC is a limited liability company, not a corporation or a sole-proprietorship/partnership.

ANTI-KICKBACK AFFIDAVIT

STATE OF Georgia)

: SS

COUNTY OF Forsyth)

I, the undersigned hereby duly sworn, depose and say that no portion of the sum herein bid will be paid to any employees of the City of Key West as a commission, kickback, reward or gift, directly or indirectly by me or any member of my firm or by an officer of the corporation.

By: Mark Vachon

Sworn and subscribed before me this 8th day of January 2018.

NOTARY PUBLIC, State of Georgia at Large

DAWN E HERRINGDINE NOTARY PUBLIC FORSYTH COUNTY, GA MY COMMISSION EXPIRES MARCH 4, 2019

My Commission Expires: 03/04/2019

* * * * * *

SWORN STATEMENT UNDER SECTION 287.133(3)(A)
FLORIDA STATUTES ON PUBLIC ENTITY CRIMES

THIS FORM MUST BE SIGNED IN THE PRESENCE OF A NOTARY PUBLIC OR OTHER OFFICER AUTHORIZED TO ADMINISTER OATHS.

1. This sworn statement is submitted with Bid or Proposal for RFP# 002-18 for EMS Billing Services

2. This sworn statement is submitted by Change Healthcare Technology Enabled Services LLC
(Name of entity submitting sworn statement)

whose business address is 5995 Windward Parkway, Alpharetta, Georgia 30005

and (if applicable) its Federal Employer Identification Number (FEIN) is 58-1953146

(If the entity has no FEIN, include the Social Security Number of the individual

signing this sworn statement

3. My name is Mark Vachon
(Please print name of individual signing)

and my relationship to the entity named above is Executive Vice President, Sales & Operations

4. I understand that a "public entity crime" as defined in Paragraph 287.133(1)(g), Florida Statutes, means a violation of any state or federal law by a person with respect to and directly related to the transaction of business with any public entity or with an agency or political subdivision of any other state or with the United States, including but not limited

to, any bid or contract for goods or services to be provided to any public or an agency or political subdivision of any other state or of the United States and involving antitrust, fraud, theft, bribery, collusion, racketeering, conspiracy, material misrepresentation.

5. I understand that "convicted" or "conviction" as defined in Paragraph 287.133(1)(b), Florida Statutes, means a finding of guilt or a conviction of a public entity crime, with or without an adjudication guilt, in any federal or state trial court of record relating to charges brought by indictment information after July 1, 1989, as a result of a jury verdict, nonjury trial, or entry of a plea of guilty or nolo contendere.

6. I understand that an "affiliate" as defined in Paragraph 287.133(1)(a), Florida Statutes, means

   a. A predecessor or successor of a person convicted of a public entity crime; or

   b. An entity under the control of any natural person who is active in the management of the entity and who has been convicted of a public entity crime. The term "affiliate" includes those officers, directors, executives, partners, shareholders, employees, members, and agents who are active in the management of an affiliate. The ownership by one person of shares constituting controlling interest in another person, or a pooling of equipment or income among persons when not for fair market value under an arm's length agreement, shall be a prima facie case that one person controls another person. A person who knowingly enters into a joint venture with a person who has been convicted of a public entity crime in Florida during the preceding 36 months shall be considered an affiliate.

7. I understand that a "person" as defined in Paragraph 287.133(1)(8), Florida Statutes, means any natural person or entity organized under the laws of any state or of the United States with the legal power to enter into a binding contract and which bids or applies to bid on contracts for the provision of goods or services let by a public entity, or which otherwise transacts or applies to transact business with public entity. The term "person" includes those officers, directors, executives, partners, shareholders, employees, members, and agents who are active in management of an entity.

8. Based on information and belief, the statement which I have marked below is true in relation to the entity submitting this sworn statement. (Please indicate which statement applies).

   _X_ Neither the entity submitting this sworn statement, nor any officers, directors, executives, partners, shareholders, employees, members, or agents who are active in management of the entity, nor any affiliate of the entity have been charged with and

convicted of a public entity crime subsequent to July 1, 1989, AND (Please indicate which additional statement applies.)

_____There has been a proceeding concerning the conviction before a hearing of the State of Florida, Division of Administrative Hearings. The final order entered by the hearing officer did not place the person or affiliate on the convicted vendor list. (Please attach a copy of the final order.)

_____The person or affiliate was placed on the convicted vendor list. There has been a subsequent proceeding before a hearing officer of the State of Florida, Division of Administrative Hearings. The final order entered by the hearing officer determined that it was in the public interest to remove the person or affiliate from the convicted vendor list. (Please attach a copy of the final order.)

_____The person or affiliate has not been put on the convicted vendor list. (Please describe any action taken by or pending with the Department of General Services.)

_____
(Signature)

01/08/2018
(Date)

STATE OF Georgia

COUNTY OF Forsyth

PERSONALLY, APPEARED BEFORE ME, the undersigned authority,

Mark Vachon who, after first being sworn by me, affixed his/her
(Name of individual signing)

signature in the space provided above on this 8th day of January, 2018.

My commission expires: 03/04/2019

DAWN E HERRINGDINE NOTARY PUBLIC FORSYTH COUNTY, GA MY COMMISSION EXPIRES MARCH 4, 2019

_____
NOTARY PUBLIC

EMS BILLING SERVICES
CITY OF KEY WEST

CITY OF KEY WEST INDEMNIFICATION FORM

To the fullest extent permitted by law, the CONSULTANT expressly agrees to indemnify and hold harmless the City of Key West, their officers, directors, agents and employees (herein called the "indemnitees") from any and all liability for damages, including, if allowed by law, reasonable attorney's fees and court costs, such legal expenses to include costs incurred in establishing the indemnification and other rights agreed to in this Paragraph, to persons or property, caused in whole or in part by any act, omission, or default by CONSULTANT or its subcontractors, material men, or agents of any tier or their employees, arising out of this agreement or its performance, including such damages caused in whole or in part by any act, omission or default of any indemnitee, but specifically excluding any claims of, or damages against an indemnitee resulting from such indemnitee's gross negligence, or the willful, wanton or intentional misconduct of such indemnitee or for statutory violation or punitive damages except and to the extent the statutory violation or punitive damages are caused by or result from the acts or omissions of the CONSULTANT or its subcontractors, material men or agents of any tier or their respective employees.

Indemnification by CONSULTANT for Professional Acts. CONSULTANT hereby agrees to indemnify the City of Key West and each of its parent and subsidiary companies and the directors, officers and employees of each of them (collectively, the "indemnitees"), and hold each of the indemnitees harmless, against all losses, liabilities, penalties (civil or criminal), fines and expenses (including reasonable attorneys' fees and expenses) (collectively, "Claims") to the extent resulting from the performance of CONSULTANT'S negligent acts, errors or omissions, or intentional acts in the performance of CONSULTANT'S services, or any of their respective affiliates, under this Agreement. If claims, losses, damages, and judgments are found to be caused by the joint or concurrent negligence of the City of Key West and CONSULTANT, they shall be borne by each party in proportion to its negligence.

The indemnification obligations under the Contract shall not be restricted in any way by any limitation on the amount or type of damages, compensation, or benefits payable by or for the CONSULTANT under Workers' Compensation acts, disability benefits acts, or other employee benefits acts, and shall extend to and include any actions brought by or in the name of any employee of the CONSULTANT or of any third party to whom CONSULTANT may subcontract a part or all of the Work. This indemnification shall continue beyond the date of completion of the work.

CONSULTANT: Change Healthcare Technology Enabled Services LLC SEAL:

5995 Windward Parkway, Alpharetta, Georgia 30005
Address

Signature

Mark Vachon
Print Name

Executive Vice President, Sales & Operations
Title

DATE: 01/08/2018

EMS BILLING SERVICES
CITY OF KEY WEST

EQUAL BENEFITS FOR DOMESTIC PARTNERS AFFIDAVIT

STATE OF Georgia)

: SS

COUNTY OF Forsyth)

I, the undersigned hereby duly sworn, depose and say that the firm of Change Healthcare Technology Enabled Services LLC provides benefits to domestic partners of its employees on the same basis as it provides benefits to employees' spouses, per City of Key West Code of Ordinances Sec. 2-799.

By: MLM Mark Vachon

Sworn and subscribed before me this 8th day of January, 2018.

Dawn E Herringdine

NOTARY PUBLIC, State of Georgia at Large

DAWN E HERRINGDINE NOTARY PUBLIC FORSYTH COUNTY, GA MY COMMISSION EXPIRES MARCH 4, 2018

My Commission Expires: 03/04/2018

* * * * * *

CONE OF SILENCE AFFIDAVIT

STATE OF Georgia)

: SS

COUNTY OF Forsyth)

I, the undersigned hereby duly sworn, depose and say that all owner(s), partners, officers, directors, employees and agents representing the firm of Change Healthcare Technology Enabled Services LLC have read and understand the limitations and procedures regarding communications concerning City of Key West issued competitive solicitations pursuant to City of Key West Ordinance Section 2-773 Cone of Silence.

By: Mark Vachon

Sworn and subscribed before me this

8th day of January 2018.

NOTARY PUBLIC, State of Georgia at Large

DAWN E HERRINGDINE NOTARY PUBLIC FORSYTH COUNTY, GA MY COMMISSION EXPIRES MARCH 4, 2019

My Commission Expires: 03/04/2019

* * * * * *

CITY OF KEY WEST
CONSULTANT RANKING FORM

Project Name: EMS Billing Services

Project Number: RFP #002-18

Firm Change Healthcare Technology Enabled Services LLC

Date _____

SELECTION CRITERIA	POINTS ALLOWED	POINTS EARNED
Program Approach	25	
Experience and Capacity of the Firm	25	
Cost Proposal and Pricing Methodology	25	
Familiarity with Local Area	15	
Subtotal Points	**90**	
References	10	
Total Points	**100**	

Table of Attachments

Attachment	Name
Attachment A	Sample Contract
Attachment B	Sample Reports
Attachment C	Staff Resumes
Attachment D	Getac Hardware Spec Sheet
Attachment E	SSAE-16 Audit Report
Attachment F	HIPAA Compliance Checklist & Billing Policies Table of Contents

MASTER SERVICES AGREEMENT

This MASTER SERVICES AGREEMENT (this "MA") is effective the latest date in the signature block below (the "Effective Date") between Change Healthcare Technology Enabled Services, LLC ("Service Provider") and _____ ("Client"), consisting of the MA Terms and Conditions and all Exhibits, Schedules, and Amendments. This MA governs all the Services described on a Service Schedule that is included in this MA during the term.

Subject to the terms and conditions of this MA, Client agrees to purchase from Service Provider, and Service Provider agrees to provide Client with, the service(s) listed in the table below (individually, a "Service" and collectively, the "Services"). The description of each Service provided under this MA and any additional terms and conditions relating to such Service are set forth in the Service Schedule referenced in the table below and attached hereto.

SERVICES	SERVICE SCHEDULE
Emergency (Ambulance) Medical Services	Service Schedule 1
Business Performance Insight Services	Service Schedule 2

This MA is executed by an authorized representative of each party.

[CLIENT]		**[SERVICE PROVIDER]**	
By:	_____	By:	_____
Printed Name:	_____	Printed Name:	_____
Title:	_____	Title:	_____
Date:	_____	Date:	_____
Tax ID:	_____		

Client:
<Address>
<City>, <State> <Zip Code>
Attention: <Insert Name or Title>

Service Provider:
5995 Windward Parkway
Alpharetta, Georgia 30005
Attention: President

With a copy to the General Counsel at the same address

yes ☐ invoices sent to above address
no ☐

If no, list invoice address below:

_____
<Address>

_____
<City>, <State> <Zip Code>

Attention: _____

MA TERMS AND CONDITIONS

1. TERM

1.1 This MA will begin on the Effective Date and continues until termination or expiration of each Schedule or amendment attached hereunder, unless earlier terminated as set forth herein.

1.2 Further, this MA will remain in force so long as there is an active Service Schedule(s).

2 SERVICES

2.1 Responsibilities.

2.1.1 Service Provider will perform the Services set forth on the applicable Service Schedule(s) on behalf of Client.

2.1.2 Service Provider agrees to perform the Services in accordance with all material applicable laws, rules and regulations, including applicable third-party payer policies and procedures.

2.1.3 Client will provide Service Provider with the necessary data in the proper format to enable Service Provider to properly furnish the Services and any information set forth in the Service Schedule(s) on a timely basis and in a format reasonably acceptable to Service Provider (the "Client Responsibilities"). Client authorizes, to the extent necessary, and directs Service Provider to release any or all necessary data and information (including, without limitation, "Individually Identifiable Health Information" as such term is defined in 45 C.F.R. § 160.103) received by Service Provider. Further, Client shall obtain all necessary consents and agreement from patients to ensure that Service Provider can comply with all applicable federal and state laws and regulations in providing the Services including, but not limited to, HIPAA (as defined herein), and the Telephone Consumer Protection Act (47 U.S.C. Section 227) and related regulations, as well as similar state laws and regulations governing telephone communications with consumers. Client shall ensure that all information it provides to Service Provider may be used by Service Provider for telephone contacts, including obtaining and maintaining a record of the consent Client has obtained from patients to receive telephone contacts from or on behalf of Client.

2.2 Operating Procedures.

2.2.1 Client acknowledges (i) that the Services or obligations of Service Provider hereunder may be dependent on Client providing access to data, information, or assistance to Service Provider from time-to-time (collectively, "Cooperation"); and (ii) that such Cooperation may be essential to the performance of the Services by Service Provider. The parties agree that any delay or failure by Service Provider to provide the Services hereunder which is caused by Client's failure to provide timely Cooperation, as reasonably requested by Service Provider, shall not be deemed a breach of Service Provider's performance obligations under this MA. Therefore, Client hereby acknowledges that such variables are specifically excluded from Service Provider's liability under this MA.

2.2.2 Client acknowledges that Service Provider has every incentive to perform the Services in a timely and proficient manner, but the timing and amount of collections generated by the Services are subject to numerous variables beyond Service Provider's control including, without limitation, (i) the inability of third parties or systems to accurately process data, (ii) the transmission of inaccurate, incomplete or duplicate data to Service Provider, (iii) untimely reimbursements or payer bankruptcies, (iv) late charge documentation submissions by Client, or (v) managed care contract disputes between payers and Client. Therefore, Client hereby acknowledges that such variables are specifically excluded from Service Provider's liability under this MA.

2.2.3 Service Provider will be the sole provider of the Services to Client.

3 PAYMENT

3.1 Lockbox. An electronic lockbox will be maintained in Client's name at a bank designated by Client. All cash receipts will be deposited into the lockbox. Service Provider will have no ownership rights in the lockbox and will have no right to negotiate or assert ownership of checks made payable to Client. Client will be responsible for all fees associated with such lockbox.

3.2 Invoicing Terms. Beginning on the Commencement Date (as defined in each Service Schedule), Client will pay all fees and other charges in U.S. dollars within 30 days after the invoice date. Prior to the Commencement Date, Client further agrees to establish an automatic electronic funds debit arrangement for paying Service Provider's invoices.

3.3 Late Payments. Service Provider may charge Client interest on any overdue fees, charges, or expenses at a rate equal to the lesser of 1.5% per month or the highest rate permitted by law. Client will reimburse Service Provider for all reasonable costs and expenses incurred (including reasonable attorneys' fees) in collecting any overdue amounts.

3.4 Suspension of the Services. Service Provider reserves the right to suspend performance of the Services (i) for nonpayment of sums owed to Service Provider that are 30 days or more past due, where such breach is not cured within ten days after notice to Client, or (ii) if such suspension is necessary to comply with applicable law or order of any governmental authority.

3.5 Fee Change. Either party may request a fee change in the event of a material change in legislation, Client's business or other market conditions which result in a material change in either the cost associated with Service Provider's provision of the Services or Service Provider's anticipated revenues under this MA. In addition, Service Provider may request a fee change in the event (i) Client fails to disclose to Service Provider information relating to Client's practice, which information, if disclosed prior to the Effective Date, would have led Service Provider to propose a higher fee or (ii) any of the information provided by Client to Service Provider upon which the practice assumptions set forth in any applicable Service Schedule are based, is or becomes inaccurate. In the event either party requests a change in the Fee, the requesting party will provide the non-requesting party with ninety (90) days' prior written notice (the "Notice Period") of the requested change (the "Notice") and such fee change will be effective at the end of the Notice Period. If the non-requesting party provides the requesting party written notice during any such Notice Period that any such fee change request is unacceptable to the non-requesting party, the Agreement will terminate at the end of the Notice Period and the Fee in place at that time will remain in effect until the end of the Workout Period, if any.

4 GENERAL TERMS

4.1 Confidentiality and Proprietary Rights.

4.1.1 Use and Disclosure of Confidential Information. Each party may disclose to the other party confidential information. Except as expressly permitted by this MA, neither party will: (i) disclose the other party's confidential information except (a) to its employees or contractors who have a need to know and are bound by confidentiality terms no less restrictive than those contained in this MA, or (b) to the extent required by law following prompt notice of such obligation to the other party, or (ii) use the other party's confidential information for any purpose other than performing its obligations under this MA. Client will not disclose nor cause its employees, agents and representatives to disclose to anyone Service Provider's business practices, trade secrets or Confidential Information, except as legally required. Each party will use all reasonable care in handling and securing the other party's confidential information and will employ all security measures used for its own proprietary information of similar nature. Notwithstanding the foregoing, Client agrees that Service Provider may de-identify Client information consistent with the

HIPAA Privacy Rule and use Client information and data from transactions received or created by Service Provider for statistical compilations or reports, research and for other purposes (the "Uses"). Such Uses shall be the sole and exclusive property of Service Provider.

4.1.2 Use and Disclosure of Billing Software.

(a) Client agrees that the software Service Provider uses to perform the Services (the "Billing System") is proprietary and confidential and that Service Provider is the sole owner or licensee of the Billing System. All report formats and reports generated by the Billing System are produced and will be made available to Client for internal operational purposes only.

(b) Client will not disclose or cause its employees, agents and representatives to disclose to anyone the Billing System or any information it receives about the Billing System, except as legally required.

4.1.3 Period of Confidentiality. The restrictions on use, disclosure and reproduction of confidential information set forth in Section 4.1, which are a "trade secret" (as that term is defined under applicable law) will be perpetual, and with respect to other confidential information such restrictions will remain in full force and effect during the term of this MA and for three years following the termination of this MA. Following the termination of this MA, each party will, upon written request, return or destroy all of the other party's tangible confidential information in its possession and will promptly certify in writing to the other party that it has done so.

4.1.4 Injunctive Relief. The parties agree that the breach, or threatened breach, of any provision of this Section 4.1 may cause irreparable harm without adequate remedy at law. Upon any such breach or threatened breach, the breached party will be entitled to seek injunctive relief to prevent the other party from commencing or continuing any action constituting such breach, without having to post a bond or other security and without having to prove the inadequacy of other available remedies. Nothing in this Section 4.1.4 will limit any other remedy available to either party.

4.1.5 Retained Rights. Client's rights in the Services will be limited to those expressly granted in this MA. Service Provider and its suppliers reserve all intellectual property rights not expressly granted to Client. All changes, modifications, improvements or new modules made or developed with regard to the Services, whether or not (i) made or developed at Client's request, (ii) made or developed in cooperation with Client, or (iii) made or developed by Client, will be solely owned by Service Provider or its suppliers. Service Provider retains title to all material, originated or prepared for Client under this MA. Client is granted a license to use such materials in accordance with this MA. For purposes of clarification, all data used in the reports prepared by Service Provider in the performance of Services for Client, and all rights and interests therein, shall be the sole property of Client. The form of the reports, work product, including processes and templates used to prepare such reports shall be the sole property of Service Provider.

4.2 Termination.

4.2.1 Termination for Default. Either party may terminate this MA by providing 30 days prior written notice of termination to the other party, if the other party (i) materially breaches this MA and fails to remedy or commence reasonable efforts to remedy such breach within 15 days, and materially cure within 45 days, after receiving notice of the breach from the terminating party, (ii) materially breaches this MA in such a way that cannot be remedied, (iii) commences dissolution proceedings or (iv) ceases to operate in the ordinary course of business.

4.2.2 Termination for Payment Default. Service Provider may terminate this MA immediately if Client defaults on its payment obligations under this MA and such payment default is not cured within ten days of written notice from Service Provider.

4.2.3 Termination by Service Provider.

(a) Service Provider may immediately terminate this MA without incurring any liability to Client if Service Provider does not receive the clean test file or completed implementation discovery packet within three months of the Commencement Date of a Service Schedule and Client will pay Service Provider for all expenses incurred prior to the termination date; or

(b) If Service Provider uses third-party software to provide the Services, Client agrees to execute additional documents other than the MA, including but not limited to nondisclosure or proprietary material documentation that is reasonably required by Service Provider or any other third-party software licensor. If Client is unwilling to sign such additional documentation, Service Provider may terminate this MA 90 days after Service Provider presented the documentation to Client.

4.2.4 Termination by Client. Client may terminate this MA immediately if Service Provider fails to cure any material breach of the "Business Associate Agreement" (set forth on Exhibit A to this MA) within 30 days of Service Providers receipt of written notice from Client specifying the breach.

4.2.5 Termination Procedures – Service Provider Billing System. In the event this MA or any Service Schedule is terminated or expires, Client will notify Service Provider in writing no later than ten business days prior to the expiration or termination of the Service Schedule of its choice of either the option set forth in sub-Section (a) below or the option set forth in sub-Section (b) below as a means of transferring its accounts receivable from Service Provider to another provider of billing services (except as otherwise set forth in sub-Section (c) below, in which case only the procedures set forth in sub-Section (b) will apply).

(a) Workout Period. Upon the effective date of termination/expiration, Service Provider shall cease to enter new patient and charge data into the Billing System on behalf of Client, but will continue to perform the Services identified in the applicable Service Schedule at the then-current rates hereunder, for a period of 90 days with respect to all of Client's accounts receivable arising from charges rendered prior to the termination date (such period hereinafter referred to as the "Workout Period"). After the Workout Period, Service Provider will discontinue processing such accounts receivable, and after full payment of all fees owed (1) deliver to Client a final list of accounts receivable and (2) provide reasonable transitional services, as set forth on Exhibit C to this MA. After completion of the above, Service Provider will have no further obligations to Client, except as expressly set forth in this MA. The parties agree that all applicable terms and conditions of this MA will be in full force and effect until the end of the Workout Period.

(b) Fees. For Client's accounts receivable for which Service Provider receives a Fee based on a percentage of the Net Collections (as defined in the Service Schedule[s]), Client shall pay Service Provider, on or before the effective date of termination/expiration, a one-time fee equal to the average monthly invoice for the six (6) months immediately preceding the effective date of such termination multiplied by one and one-half (1.5) (the "Services Rendered Fee"). With respect to Client's accounts receivable for which Service Provider receives a Fee based on a set dollar amount, no additional fees shall be owed to Service Provider as of the effective date of

termination/expiration. Upon the effective date of termination/expiration of this MA or Service Schedule, Service Provider shall be immediately relieved of its obligation to provide any further Services on behalf of Client. After full payment of all fees owed, including but not limited to the Services Rendered Fee, Service Provider will deliver to Client a final list of accounts receivable and provide reasonable Transitional Services, as set forth on Exhibit C to this MA. After completion of the above, Service Provider will have no further obligations to Client, except as expressly set forth in this MA. The Services Rendered Fee does not limit the rights and remedies Service Provider may have against Client arising out of any breach of this MA.

(c) Default Selection. If (i) this MA is terminated by Service Provider pursuant to the terms set forth in Section 4.2.2, or (ii) Client fails to make the above-required selection in the allotted time, only the procedures set forth in Section 4.2.5(b) will apply with regards to any termination/expiration transition.

4.2.6 Survival of Provisions. Those provisions of this MA that, by their nature, are intended to survive termination or expiration of this MA will remain in full force and effect, including, without limitation, the following Sections of this MA: 3 (Payment), 4.1 (Confidentiality), 4.3 (Limitation of Liability), 4.6.3 (Books and Records), and 4.10-4.26 (Governing Law – Entire Agreement).

4.3 Limitation of Liability.

4.3.1 Total Damages. Service Provider's total cumulative liability in connection with, or related to this MA will be limited to the sum of fees paid by Client to Service Provider during the 12-month period preceding the date of the claim, as applicable, whether based on breach of contract, warranty, tort, product liability, or otherwise. Service Provider will have no liability for systems beyond the control of Service Provider.

4.3.2 Exclusion of Damages. IN NO EVENT WILL SERVICE PROVIDER BE LIABLE TO CLIENT UNDER, IN CONNECTION WITH, OR RELATED TO THIS MA FOR ANY SPECIAL, INCIDENTAL, INDIRECT, OR CONSEQUENTIAL DAMAGES, INCLUDING, BUT NOT LIMITED TO, LOST PROFITS OR LOSS OF GOODWILL, WHETHER BASED ON BREACH OF CONTRACT, WARRANTY, TORT, PRODUCT LIABILITY, OR OTHERWISE, AND WHETHER OR NOT SERVICE PROVIDER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

4.3.3 Material Consideration. THE PARTIES ACKNOWLEDGE THAT THE FOREGOING LIMITATIONS ARE A MATERIAL CONDITION FOR THEIR ENTRY INTO THIS MA.

4.4 Internet Disclaimer. CERTAIN PRODUCTS AND SERVICES PROVIDED BY SERVICE PROVIDER UTILIZE THE INTERNET. SERVICE PROVIDER DOES NOT WARRANT THAT SUCH SERVICES WILL BE UNINTERRUPTED, ERROR-FREE, OR COMPLETELY SECURE. SERVICE PROVIDER DOES NOT AND CANNOT CONTROL THE FLOW OF DATA TO OR FROM SERVICE PROVIDER'S OR CLIENT'S NETWORK AND OTHER PORTIONS OF THE INTERNET. SUCH FLOW DEPENDS IN LARGE PART ON THE INTERNET SERVICES PROVIDED OR CONTROLLED BY THIRD PARTIES. ACTIONS OR INACTIONS OF SUCH THIRD PARTIES CAN IMPAIR OR DISRUPT CLIENT'S CONNECTIONS TO THE INTERNET (OR PORTIONS THEREOF). ACCORDINGLY, SERVICE PROVIDER DISCLAIMS ANY AND ALL LIABILITY RESULTING FROM OR RELATED TO THE ABOVE EVENTS.

4.5 Civil Monetary Fine or Penalty. Service Provider will pay any civil or monetary fine or penalty and interest (but not overpayments) assessed against Client by Medicare, Medicaid

or other third-party health insurance provider arising out of Service Provider's sole negligence or willful misconduct in the performance of its obligations under this MA. Overpayments received by Client are the sole responsibility of Client.

4.6 Audits.

4.6.1 Internal Audit by Client. Client may use its own internal resources ("Internal Auditors") to perform audits of Service Provider's accuracy and correctness of the accounting and internal controls performed and maintained by Service Provider. Service Provider will provide the Internal Auditors with information that the Internal Auditor determines to be reasonably necessary to perform and complete the audit procedures. Client agrees that an audit conducted under this section will be conducted at such times and in a manner that avoids undue disruption of Service Provider's operations.

4.6.2 Third-Party Audit by Client. Client may engage, at its own expense, independent, external, third-party auditors ("Third-Party Auditors") to perform audits of Service Provider's accuracy and correctness of the accounting and internal control performed and maintained by Service Provider. If Client engages Third-Party Auditors, who perform, or are associated with a group who performs, billing and accounts receivable management services substantially similar to any of the Services identified on any Service Schedule to this MA, such Third-Party Auditors may not visit Service Provider's processing facility or audit the actual billing and collection process. Service Provider will provide the information that the Third-Party Auditors determine to be reasonably necessary to perform and complete all audit procedures. The Third-Party Auditors shall execute Service Provider's "Confidentiality Agreement", substantially in the form attached hereto as Exhibit B, prior to the start of the audit. Client agrees that an audit conducted under this section will be conducted at such times and in a manner that avoids undue disruption of Service Provider's operations.

4.6.3 Books and Records. If required by Section 952 of the Omnibus Reconciliation Act of 1980, 42 U.S.C. Section 1395x(v)(I)(i) and (ii), for a period of four years after the Services are furnished, the parties agree to make available, upon the written request of the Secretary of Health and Human Services, the Comptroller General, or their representatives, this MA and such books, documents, and records as may be necessary to verify the nature and extent of the Services with a value or cost of $10,000 or more over a twelve month period.

4.7 Warranties.

4.7.1 Service Provider.

(a) Prior to the Commencement Date. Unless Service Provider provided Services prior to the Commencement Date of any Service Schedule, Client will be responsible for all matters related to Client's practice prior to the Commencement Date, including, but not limited to, Client's billings, collections, third party reimbursements, accounts receivable and credit balances.

(b) Disclaimer of Warranties. Service Provider disclaims any warranties or representations pertaining to the timing and amount of collections generated by the Services. Client acknowledges and agrees that Client is solely responsible for refunding any overpayments and processing any unclaimed property payments. Service Provider will provide Client with written notice of unresolved credit balances of which Service Provider becomes aware (such as overpayments or unclaimed property).

4.7.2 Client.

(a) Charges and Information.

(i) Client represents and warrants that it will forward to Service Provider (pursuant to the applicable Service Schedule[s]) only charges for which Client is entitled to bill. Client agrees to monitor and to refrain from knowingly submitting false or inaccurate information, charges, documentation or records to Service Provider and to ensure that the documentation provided by Client or an agent of Client to Service Provider supports the medical services provided by Client. Client acknowledges and agrees it has an obligation to report and correct any credible evidence of deficiencies on the part of Client. Client also acknowledges that Service Provider does not make a determination of medical necessity for any claims.

(ii) Client acknowledges and agrees that Service Provider is not a collection agency. Client represents and warrants that any debt or account referred to Service Provider pursuant to this MA is not in default or delinquent or has not been written off as bad debt. If any accounts are found to be written off, in default or otherwise delinquent, Client agrees to immediately recall those accounts from Service Provider's responsibility under this MA.

(b) Release of Information. Client represents and warrants that Client has obtained a release of information and insurance assignment of benefits from all individuals for whom Client is submitting charges to Service Provider for the provision of the Services and will immediately notify Service Provider if such release of information and insurance assignment of benefits is changed or revoked or if such individual refused/failed to execute such documents. Client further agrees to provide a copy of such signed documents upon Service Provider's request. The term "individuals" in this Section refers to the individual physicians/practitioners, or group members, on whose behalf the Client is directing Service Provider to submit claims

4.8 Business Associate. The parties agree to the obligations set forth in Exhibit A.

4.9 Exclusion From Federal Healthcare Programs. Each party warrants that it is not currently listed by a Federal agency as excluded, debarred, or otherwise ineligible for participation in any Federal health care program. Each party agrees that it will not employ, contract with, or otherwise use the services of any individual whom it knows or should have known, after reasonable inquiry, (i) has been convicted of a criminal offense related to health care (unless the individual has been reinstated to participation in Medicare and all other Federal health care programs after being excluded because of the conviction), or (ii) is currently listed by a Federal agency as excluded, debarred, or otherwise ineligible for participation in any Federal health care program. Each party agrees that it will immediately notify the other in the event that it, or any person in its employ, has been excluded, debarred, or has otherwise become ineligible for participation in any Federal health care program. Each party agrees to continue to make reasonable inquiry regarding the status of its employees and independent contractors on a regular basis by reviewing the General Services Administration's List of Parties Excluded from Federal Programs and the HHS/OIG List of Excluded Individuals/Entities.

4.10 Governing Law. This MA is governed by and will be construed in accordance with the laws of the State of Georgia, exclusive of its rules governing choice of law and conflict of laws and any version of the Uniform Commercial Code. Each party agrees that exclusive venue for all actions, relating in any manner to this MA will be in a federal or state court of competent jurisdiction located in Fulton County, Georgia.

4.11 Claims Period. Any action relating to this MA and any claim for damages, including, but not limited to, a claim for recurring damages arising out of the same cause or event, other than

collection of outstanding payments, must be commenced within six months after the date upon which the cause of action occurred.

4.12 Assignment and Subcontracts. Neither party will assign this MA without the prior written consent of the other party, which will not be unreasonably withheld, delayed or conditioned. Service Provider may, upon notice to Client, assign this MA to any affiliate or to any entity resulting from the transfer of all or substantially all of Service Provider's assets or capital stock or from any other corporate reorganization. Service Provider may subcontract its obligations under this MA.

4.13 Severability. If any part of a provision of this MA is found illegal or unenforceable, it will be enforced to the maximum extent permissible, and the legality and enforceability of the remainder of that provision and all other provisions of this MA will not be affected.

4.14 Notices. All notices relating to the parties' legal rights and remedies under this MA will be provided in writing and will reference this MA. Such notices will be deemed given if sent by: (i) postage prepaid registered or certified U.S. Post mail, then five working days after sending; or (ii) commercial courier, then at the time of receipt confirmed by the recipient to the courier on delivery. All notices to a party will be sent to its address set forth on the cover page hereto, or to such other address as may be designated by that party by notice to the sending party.

4.15 Waiver. Failure to exercise or enforce any right under this MA will not act as a waiver of such right.

4.16 Force Majeure. Except for the obligation to pay money, a party will not be liable to the other party for any failure or delay caused in whole or in material part to any cause beyond its sole control, including but not limited to fire, accident, labor, dispute or unrest, flood, riot, war, rebellion, insurrection, sabotage, terrorism, transportation delays, shortage of raw materials, energy, or machinery, acts of God or of the civil or military authorities of a state or nation, or the inability, due to the aforementioned causes, to obtain necessary labor or facilities.

4.17 Amendment. This MA may be modified, or any rights under it waived, only by a written document executed by the authorized representatives of both parties. To avoid doubt, this MA may not be amended via electronic mail or other electronic messaging service.

4.18 No Third Party Beneficiaries. Except as specifically set forth in a Service Schedule, nothing in this MA will confer any right, remedy, or obligation upon anyone other than Client and Service Provider.

4.19 Relationship of Parties. Each party is an independent contractor of the other party. This MA will not be construed as constituting a relationship of employment, agency, partnership, joint venture or any other form of legal association. Neither party has any power to bind the other party or to assume or to create any obligation or responsibility on behalf of the other party or in the other party's name.

4.20 Non-solicitation of Employees. During the term of this MA and for a period of 12 months following the termination of this MA, each party agrees not to employ, contract with for services, solicit for employment on its own behalf or on behalf of any third party, or have ownership in any entity which employs or solicits for employment, any individual who (i) was an employee of the other or its parent, affiliates or subsidiaries at any time during the preceding 12 months and (ii) was materially involved in the provision or receipt of the Services hereunder without the prior written consent of the other party. Notwithstanding the foregoing, upon any termination of this MA, Client may rehire any individual who was employed by Client on the Effective Date, and who was hired by Service Provider on or after such date. Each party agrees that the other party does not have an adequate remedy at law to protect its rights under this Section and agrees that the non-defaulting party will have the right to injunctive relief from any violation or threatened violation of this Section.

4.21 Publicity. The parties may publicly announce that they have entered into this MA and describe their relationship in general terms, excluding financial terms. The parties will not make any other public announcement or press release regarding this MA or any activities performed hereunder without the prior written consent of the other party.

4.22 Construction of this MA. This MA will not be presumptively construed for or against either party. Section titles are for convenience only. As used in this MA, "will" means "shall," and "include" means "includes without limitation." The parties may execute this MA in one or more counterparts, each of which will be deemed an original and one and the same instrument.

4.23 Conflict Between MA and Schedules. In the event of any conflict or inconsistency in the interpretation of this MA (including its Service Schedules and all Amendments executed hereunder), such conflict or inconsistency will be resolved by giving precedence according to the following order: (a) the Amendment, (b) the Service Schedule, (c) the MA Terms and Conditions and Exhibits, (d) documents incorporated by reference.

4.24 Section Headings. The Section headings used herein are for convenience only and shall not be used in the interpretation of this MA.

4.25 Authority. Service Provider and Client represent and warrant that they have the full power and authority to enter into this MA, that there are no restrictions or limitations on their ability to perform this MA, and that the person executing this MA has the full power and authority to do so.

4.26 Entire Agreement. This MA, including Service Schedules, Exhibits, Amendments, and documents incorporated by reference, is the complete and exclusive agreement between the parties with respect to the subject matter hereof, superseding and replacing all prior agreements, communications, and understandings (written and oral) regarding its subject matter.

EXHIBIT A
BUSINESS ASSOCIATE AGREEMENT ("BAA")

This Business Associate Agreement ("Agreement") is entered into by and between Service Provider ("Business Associate") and Client ("Covered Entity"). Business Associate and Covered Entity may be individually referred to as a "Party" and, collectively, the "Parties" in this Agreement. This Agreement shall be incorporated into and made part of the Underlying Agreement (as defined below).

STATEMENT OF PURPOSE

Pursuant to the Underlying Agreement, Business Associate provides services to Covered Entity and Covered Entity discloses certain information, including PHI (as defined below), to Business Associate. The purpose of this Agreement is to protect the privacy and provide for the security of such PHI in compliance with the Privacy Rule and Security Rule.

SECTION 1: DEFINITIONS

"Electronic Protected Health Information" or **"Electronic PHI"** will have the meaning given to such term under the Privacy Rule and the Security Rule, including, but not limited to, 45 C.F.R. § 160.103, as applied to the information that Business Associate creates, receives, maintains or transmits from or on behalf of Covered Entity.

"Privacy Rule" will mean the Standards for Privacy of Individually Identifiable Health Information at 45 C.F.R. Part 160 and Part 164, Subparts A and E.

"Protected Health Information" or **"PHI"** will have the same meaning as the term "protected health information" in 45 C.F.R. § 160.103, as applied to the information created, received, maintained or transmitted by Business Associate from or on behalf of Covered Entity.

"Security Rule" will mean the Security Standards at 45 C.F.R. Part 160 and Part 164, Subparts A and C

"Underlying Agreement" will mean the applicable written services agreement(s) between Covered Entity and Business Associate under which Covered Entity may disclose PHI to Business Associate.

Capitalized Terms. Capitalized terms used in this Agreement and not otherwise defined herein will have the meanings set forth in the Privacy Rule and the Security Rule which definitions are incorporated in this Agreement by reference.

SECTION 2: PERMITTED USES AND DISCLOSURES OF PHI

2.1 Uses and Disclosures of PHI Pursuant to the Underlying Agreement. Except as otherwise limited in this Agreement, Business Associate may use or disclose PHI to perform functions, activities or services for, or on behalf of, Covered Entity as specified in the Underlying Agreement, provided that such use or disclosure would not violate the Privacy Rule if done by Covered Entity.

2.2 Permitted Uses of PHI by Business Associate. Except as otherwise limited in this Agreement, Business Associate may use PHI for the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate.

2.3 Permitted Disclosures of PHI by Business Associate. Except as otherwise limited in this Agreement, Business Associate may disclose PHI for the proper management and administration of Business Associate, provided that the disclosures are Required by Law, or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and will be used or further disclosed only as Required by Law or for the purpose for which it was disclosed to the person (which purpose must be consistent with the limitations imposed upon Business Associate pursuant to this Agreement), and that the person agrees to notify Business Associate of any instances in which it is aware that the confidentiality of the information has been breached.

2.4 Data Aggregation. Except as otherwise limited in this Agreement, Business Associate may use PHI to provide Data Aggregation services for the Health Care Operations of the Covered Entity as permitted by 45 C.F.R. § 164.504(e)(2)(i)(B).

2.5 De-identified Data. Business Associate may de-identify PHI in accordance with the standards set forth in 45 C.F.R. § 164.514(b) and may use or disclose such de-identified data unless prohibited by applicable law.

SECTION 3: OBLIGATIONS OF BUSINESS ASSOCIATE

3.1 Appropriate Safeguards. Business Associate will use appropriate administrative, physical, and technical safeguards to comply with the Security Rule with respect to Electronic PHI, to prevent use or disclosure of such information other than as provided for by the Underlying Agreement and this Agreement. Except as expressly provided in the Underlying Agreement or this Agreement, Business Associate will not assume any obligations of Covered Entity under the Privacy Rule. To the extent that Business Associate is to carry out any of Covered Entity's obligations under the Privacy Rule, Business Associate will comply with the requirements of the Privacy Rule that apply to Covered Entity in the performance of such obligations.

3.2 Reporting of Improper Use or Disclosure, Security Incident or Breach. Business Associate will report to Covered Entity any use or disclosure of PHI not permitted under this Agreement, Breach of Unsecured PHI or any Security Incident, without unreasonable delay, and in any event no more than fourteen (14) days following discovery; provided, however, that the Parties acknowledge and agree that this Section constitutes notice by Business Associate to Covered Entity of the ongoing existence and occurrence of attempted but Unsuccessful Security Incidents (as defined below). "Unsuccessful Security Incidents" will include, but not be limited to, pings and other broadcast attacks on Business Associate's firewall, port scans, unsuccessful log-on attempts, denials of service and any combination of the above, so long as no such incident results in unauthorized access, use or disclosure of PHI. Business Associate's notification to Covered Entity of a Breach will comply with the requirements set forth in 45 C.F.R. § 164.404.

3.3 Business Associate's Agents. Business Associate will enter into a written agreement with any agent or subcontractor that creates, receives, maintains or transmits PHI on behalf of Business Associate for services provided to Covered Entity, providing that the agent agrees to restrictions and conditions that are no less restrictive than those that apply through this Agreement to Business Associate with respect to such PHI.

3.4 Access to PHI. To the extent Business Associate agrees in the Underlying Agreement to maintain any PHI in a Designated Record Set, Business Associate agrees to make such information available to Covered Entity pursuant to 45 C.F.R. § 164.524, within ten (10) business days of Business Associate's receipt of a written request from Covered Entity; provided, however, that Business Associate is not required to provide such access where the PHI contained in a Designated Record Set is duplicative of the PHI contained in a Designated Record Set possessed by Covered Entity.

3.5 Amendment of PHI. To the extent Business Associate agrees in the Underlying Agreement to maintain any PHI in a Designated Record Set, Business Associate agrees to make such information available to Covered Entity for amendment pursuant to 45 C.F.R. § 164.526 within ten (10) business days of Business Associate's receipt of a written request from Covered Entity.

3.6 Documentation of Disclosures. Business Associate will document disclosures of PHI and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 C.F.R. § 164.528.

3.7 Accounting of Disclosures. Business Associate will provide to Covered Entity, within twenty (20) business days of Business Associate's receipt of a written request from Covered Entity, information collected in accordance with Section 3.6 of this Agreement, to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 C.F.R. § 164.528.

3.8 Governmental Access to Records. Business Associate will make its internal practices, books and records relating to the use and disclosure of PHI received from, or created or received by Business

Associate on behalf of, Covered Entity available to the Secretary for purposes of the Secretary determining compliance with the Privacy Rule and the Security Rule.

3.9 Mitigation. To the extent practicable, Business Associate will cooperate with Covered Entity's efforts to mitigate a harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate that is not permitted by this Agreement.

3.10 Minimum Necessary. Business Associate will request, use and disclose the minimum amount of PHI necessary to accomplish the purpose of the request, use or disclosure, in accordance with 45 C.F.R. § 164.514(d), and any amendments thereto.

SECTION 4: CHANGES TO PHI AUTHORIZATIONS

Covered Entity will notify Business Associate fifteen (15) days, if practicable, prior to the effective date of (1) any limitation(s) in its notice of privacy practices in accordance with 45 C.F.R. § 164.520, (2) any changes in, or revocation of, permission by an Individual to use or disclose PHI, or (3) any restriction to the use or disclosure of PHI that Covered Entity has agreed to in accordance with 45 C.F.R. § 164.522. Covered Entity will make such notification to the extent that such limitation, restriction, or change may affect Business Associate's use or disclosure of PHI.

SECTION 5: TERM AND TERMINATION

5.1 Term. The term of this Agreement will commence as of the Effective Date, and will terminate when all of the PHI provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity.

5.2 Termination for Cause. Upon either Party's knowledge of a material breach by the other Party of this Agreement, such Party may terminate this Agreement immediately if cure is not possible. Otherwise, the non-breaching party will provide written notice to the breaching Party detailing the nature of the breach and providing an opportunity to cure the breach within thirty (30) business days. Upon the expiration of such thirty (30) day cure period, the non-breaching Party may terminate this Agreement and the affected underlying product or service if the breaching party does not cure the breach or if cure is not possible.

5.3 Effect of Termination.

5.3.1 Except as provided in Section 5.3.2, upon termination of the Underlying Agreement or this Agreement for any reason, Business Associate will return or destroy all PHI received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity, at Covered Entity's expense, and will retain no copies of the PHI. This provision will apply to PHI that is in the possession of subcontractors or agents of Business Associate.

5.3.2 If it is infeasible for Business Associate to return or destroy the PHI upon termination of the Underlying Agreement or this Agreement, Business Associate will: (a) extend the protections of this Agreement to such PHI and (b) limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such PHI.

5.3.3 The respective rights and obligations of Business Associate under Section 5.3 of this Agreement will survive the termination of this Agreement and the Underlying Agreement.

SECTION 6: COOPERATION IN INVESTIGATIONS

The Parties acknowledge that certain breaches or violations of this Agreement may result in litigation or investigations pursued by federal or state governmental authorities of the United States resulting in civil liability or criminal penalties. Each Party will cooperate in good faith in all respects with the other Party in connection with any request by a federal or state governmental authority for additional information and documents or any governmental investigation, complaint, action or other inquiry.

SECTION 7: COMPLIANCE WITH LAW

Business Associate will comply with all applicable federal privacy and security laws governing PHI, as they may be amended from time to time.

SECTION 8: AMENDMENT

This Agreement may be modified, or any rights under it waived, only by a written document executed by the authorized representatives of both Parties. In addition, if any relevant provision of the Privacy Rule or the Security Rule is amended in a manner that changes the obligations of Business Associate or Covered Entity that are embodied in terms of this Agreement, then the Parties agree to negotiate in good faith appropriate non-financial terms or amendments to this Agreement to give effect to such revised obligations.

SECTION 9: GENERAL

This Agreement is governed by, and will be construed in accordance with, the laws of the State that govern the Underlying Agreement. Covered Entity will not assign this Agreement without the prior written consent of Business Associate, which will not be unreasonably withheld. All notices relating to the Parties' legal rights and remedies under this Agreement will be provided in writing to a Party, will be sent to its address set forth in the Underlying Agreement, or to such other address as may be designated by that Party by notice to the sending Party, and will reference this Agreement. Nothing in this Agreement will confer any right, remedy, or obligation upon anyone other than Covered Entity and Business Associate.

EXHIBIT B
CONFIDENTIALITY AGREEMENT

Service Provider and ___ ***[insert name of Client]***___ ("Client") have entered into an agreement whereby Service Provider provides certain services (the "Services") to Client (the "Master Services Agreement"). Client has entered into a contractual relationship with _____[***insert name of person/entity performing the audit***]____ ("Recipient") and instructs Service Provider to allow Recipient to review certain information in Service Provider's possession regarding Client's business and accounts receivable billing and collections performed by Service Provider ("Client Proprietary Information"). Therefore, in consideration of the mutual covenants and conditions contained in this Confidentiality Agreement (the "Confidentiality Agreement"), Recipient and Client agree as follows:

A. During the course of Recipient's examination and review of Client Proprietary Information, Recipient may be exposed to or review certain proprietary information regarding Service Provider ("Service Provider Proprietary Information"). Service Provider Proprietary Information refers to any and all data and information relating to the business of Service Provider which has value to Service Provider and is not generally known by its competitors or the public, including, without limitation, financial information, inventions, methods, techniques, actual or potential customers and suppliers, the Master Services Agreement, Service Provider's business practices or other trade secrets or confidential information of Service Provider, all report formats, and existing and future products and computer systems and software. Recipient acknowledges and agrees that all Service Provider Proprietary Information and all physical embodiments thereof are confidential to Service Provider and are and will remain the sole and exclusive property of Service Provider. All Service Provider Proprietary Information acquired by Recipient will be kept strictly confidential and will not be disclosed to any other person or entity (including any entity affiliated with or any division of Recipient).

B. Service Provider Proprietary Information does not include information which (i) is publicly known or which becomes publicly known through no act or failure to act on the part of Recipient; (ii) is lawfully obtained by Recipient from any third party entitled to disclose such information; (iii) is in the lawful possession of Recipient prior to such information having been disclosed to Recipient by Service Provider; or (iv) is independently developed by Recipient.

C. Recipient further agrees that during Recipient's engagement by Client and for a period of one (1) year following any termination of Recipient's engagement for whatever reason, Recipient will not, directly or indirectly, on Recipient's own behalf or in the service of, or on behalf of any other individual or entity, divert, solicit or hire away, or attempt to divert, solicit or hire away, to or for any individual or entity, any person employed by Service Provider, whether or not such employee is a full-time employee, temporary employee, leased employee or independent contractor of Service Provider, whether or not such employee is employed pursuant to written agreement and whether or not such employee is employed for a determined period or at-will.

D. Recipient acknowledges that great loss and irreparable damage would be suffered by Service Provider if Recipient should breach or violate the terms of this Confidentiality Agreement. In the event Recipient breaches or violates this Confidentiality Agreement, Recipient agrees that Service Provider would not have an adequate remedy at law and, therefore, that Service Provider would be entitled to a temporary restraining order and permanent injunction to prevent a breach of any of the terms or provisions contained in this Confidentiality Agreement, in addition to any monetary damages that may be available at law or equity. Recipient's obligations under this Confidentiality Agreement will survive indefinitely.

E. Recipient represents and warrants that (i) it has the full power and authority to enter into this Confidentiality Agreement, and (ii) the person executing this Confidentiality Agreement has the full power and authority to do so.

IN WITNESS WHEREOF, Recipient has signed this Confidentiality Agreement as of the date below written.

RECIPIENT: _____

By: _____

Print Name: _____

Title: _____

Date: _____

SAMPLE
(No Signature Required)

CLIENT: *[INSERT CLIENT NAME]*

By: _____

Print Name: _____

Title: _____

Date: _____

SAMPLE
(No Signature Required)

EXHIBIT C

TRANSITION SPECIFICS

Upon termination or expiration of this MA, for any reason, Service Provider agrees to provide the following assistance to Client or Client's designated agent to transfer Service Provider's responsibilities under this MA and Service Schedule to Client or Client's designated agent ("Transitional Services"):

Data specifications	Patient information will be provided via a write-protected CD. Detailed specifications will be provided to Client or Client's designated agent.
Technical and Operational contacts	Service Provider Support contacts will be provided to answer questions regarding the specifications document and operational requirements. Questions may be presented by Client or its designee.
Test CD	A test CD will be provided containing 100 patient accounts and their associated transaction activity.
Final CD	A final CD will include all debit and credit balance accounts residing in the active AR. Zero balance accounts will be provided up to the age of two years (based on the date the account was placed on the system). Patient demographic and transaction information is included.
Utility file codes	Listings will be provided to Client or its designee for the following files: Charge codes, description and CPT Referring physician code, name and NPI (if available) Performing physician, code and name Location of service, code and description Transaction codes and description

SERVICE SCHEDULE 1
EMERGENCY (AMBULANCE) MEDICAL SERVICES

The MA Terms and Conditions and this Service Schedule apply to all services rendered by Service Provider under this Service Schedule.

1. Term

1.1 Initial Term of Schedule. The initial term of this Service Schedule is three years (the "Schedule 1 Term") beginning _____, 201___ (the "Schedule 1 Commencement Date").

1.2 Automatic Renewal. This Service Schedule will automatically renew for one year terms unless (i) either party delivers to the other written notice of termination at least 90 days prior to the expiration of the then-current term, or (ii) as otherwise set forth in the MA.

2 Scope of Services

2.1 Scope. Service Provider will provide the services related to the billing of Emergency Medical Services ("EMS") as specified below based on information provided by Client for professional ambulance services rendered by Client in accordance with the terms of the MA and this Service Schedule.

2.2 Responsibilities. Each party agrees to perform its respective responsibilities identified below in a timely and diligent manner. Client acknowledges and agrees that Service Provider's performance of the Services described herein is dependent upon Client's performance of its responsibilities as set forth in this Service Schedule.

2.2.1 Service Provider Responsibilities. Service Provider will have managerial responsibilities over all business support services as they relate to the billing of EMS provided by Client, subject to Client's ultimate control. In order for Service Provider to provide the necessary business support services on behalf of Client, the following operating policies will be used with respect to Client's EMS:

(a) Billing Responsibilities. Service Provider will be responsible for billing for all EMS provided by Client. Service Provider will:

(i) Process all demographic and charge information entered into the billing system based on the information provided by Client, including the schedule of EMS fees;

(ii) Process all required insurance forms whether submitted electronically or on hard copy. Insurance claims will be submitted at least weekly based on the availability of information received from the Client;

(iii) Provide all HCFA-1500 universal claim forms needed to submit claims for EMS provided by the Client;

(iv) Print and mail patient statements for accounts with patient balances greater than $5.00. Mail up to two statements and provide telecollect call according to the schedule set forth by the Client, to patients for fees not reimbursed by third-party payments including deductibles, co-payments and non-covered services for which the Client maintains appropriate waiver documentation. Client will specify if residents receive a balance due statement and if unpaid patient balance due amounts are written-off or forwarded to a collection agency for further activity;

(v) Receive from Client's lockbox, notification of payment and original remittance advices, and all other billing correspondence, as appropriate;

(vi) Enter all remittance information, including, contractual adjustments for third-party payers with which the Client participates (based

upon an approved list provided by the Client), and submit secondary insurance claims as necessary;

(vii) For a period of one year, maintain a paper or electronic copy of explanation of benefit statements ("EOBs") received from third-party payers. At the end of one year, all EOBs will be returned to Client when requested or may be destroyed by Service Provider;

(viii) Evaluate appropriate documentation of any request by a patient, third-partyfor an adjustment to a patient's bill, and coordinate findings with Client;

(ix) Code each patient chart, on the basis of the information provided by Client, including ICD and HCPCS codes, procedural modifiers and HCPCS Level II regulatory modifiers; and

(x) Assist with designing for the Client all necessary forms, fee slips, insurance authorizations, etc., for processing. Costs of actual forms, etc. will be the responsibility of Client.

(b) Collection Responsibilities. In undertaking these responsibilities, Service Provider will:

(i) Answer all patient and third-party payer inquiries. In some cases, additional data will be requested from Client. Responses to all patient inquiries will be made within one business day whenever possible;

(ii) Pay for all telephone costs for patient and third-party payer inquiries and follow-up;

(iii) Pursue balances with any third-party payer as follows:

1. Monitor the balances and follow-up either in writing or by telephone, as appropriate, when payments are overdue.
2. Monitor all payments received against anticipated payments. Discrepancies noted will be reviewed and, when appropriate, contact will be made by telephone, in writing, or in person with the third-party payer to request claim review.
3. Monitor payment patterns for each third-party payer at least monthly to identify any third-party payer with large amounts of pending open claims. Appropriate action will be taken with the third-party payer to expedite prompt payment.
4. In the event any claim is denied by any third-party payer for reasons other than a patient's insured status, Service Provider will use its commercially reasonable efforts to re-submit a clean claim in a timely manner. In the event a claim is denied as a result of improper coding or other act attributable to Service Provider, Service Provider will pursue a timely appeal of the denied claim.
5. Follow up with the third-party payer on assigned claims based upon the appropriate strategy for working with such third-party payer.

(iv) Pursue balances with patients by attaching notes on statements at pre-determined intervals using language approved by Client; and

(v) Amounts due from a third-party or patient, that have not been collected after the activities described above and that have aged greater than 120 days, will be considered uncollectable. Service Provider will provide pertinent demographic and transactional detail to the Client identifying uncollectable accounts monthly. Unless otherwise instructed by Client, Service Provider will write-off the identified accounts as bad debts and will cease collection efforts associated with those accounts.

(vi) Notify Client in writing of the Monthly Refund Amount owed by Client for the previous month. Upon Client's deposit of the Monthly Refund Amount in the Refund Account, prepare, sign and release the applicable individual patient and carrier refund checks.

(vii) Research, identify, and notify Client of overpayments through the refund register/refund checks prepared for Client or through a monthly management report. Overpayments that remain unresolved sixty (60) days after Client's receipt of notice will be removed from Service Provider's billing system.

(viii) Make reasonable efforts to identify the owners of unclaimed property. Notify Client of any unresolved refunds that Service Provider wrote off after ninety (90) days.

(c) Reporting Responsibilities. Service Provider will be responsible for making periodic reports to Client on the current status of all active patient accounts. In undertaking these responsibilities, Service Provider will:

(i) Produce monthly activity and summary reports as follows:

1. Fire/EMS Executive Summary - of the EMS for current month and year to date produced by:
    a. Number of transports and gross charges/receipts by level of service delivered;
    b. Drop off location; and
    c. Payer Category Analysis.
2. Financial Summary - of charges, write-offs and payments of the EMS for current month and year to date analyzed by:
    a. Current charges and payments received;
    b. Payer Category Analysis; and
    c. Summary aging of accounts receivable and adjustments and write-offs.

(ii) Provide off-site back up of all active data files; and

(iii) Provide additional reports reasonably requested by the Client.

(d) Implementation. Service Provider will be responsible for implementing the billing and collection services on behalf of Client. In undertaking such implementation, Service Provider will:

(i) Assign an account manager to Client who will be responsible for the following:

1. Act as primary contact with the personnel of Client;
2. Serve as the liaison with the Service Provider employees assigned to perform services for Client;
3. Communicate regularly with the key management of Client to review all activities with respect to the billing and collection services;
4. Work closely with Client to ensure a smooth transition and implementation; and

(ii) Review both its procedures and the procedures of Client and recommend and implement approved changes for improvements of collections.

2.2.2 Client Responsibilities. In order for Service Provider to undertake the billing and collection services, Client will:

(a) Cause the personnel of Client to timely submit to Service Provider the name of the patient when available, a paper copy of the Patient Care Report or an electronic extract when available, the date of service, a description of the nature, and the extent of services provided and any supporting medical information necessary to obtain payment or reimbursement, including the level of service provided, an address and zip code of where the patient was picked up from and a patient signature or other appropriate signature when a patient signature is not possible. Where a dispatch system is used, the dispatch code or description must be provided. Service Provider will rely on the truth and accuracy of such

information and will not in any event be required to verify medical treatment information submitted to Service Provider by the Client. Furthermore, Client will use its best efforts to procure all necessary consents to all assignments and obtain all other approvals, consents, and signatures necessary for Service Provider to collect payment for reimbursement on behalf of Client;

(b) Assist Service Provider with establishing dialog and a data interface with transport hospitals means to gather patient demographic and insurance data from transport hospitals when requested, or provide copies of the hospital face sheet if other means of capturing this data are not available.

(c) Be solely responsible for securing or causing to be secured from or on behalf of patients whose accounts are covered under this Service Schedule, any and all necessary consents for the release of information to third parties as contemplated by this Service Schedule, and any and all necessary assignments of insurance benefits and benefits due from and rights to payment or reimbursement by any other third party. Client will notify Service Provider in the event that assignment was not obtained;

(d) Supply complete and accurate patient charge information;

(e) Provide to Service Provider a schedule of professional fees charged for services rendered by Client's EMS. Service Provider will make revisions to the fee schedule from time to time upon at least 10 days prior written notice from Client to the effective date of any such revision. Service Provider will continue to bill at the rates then in effect until receipt of such notice. Fee schedule revisions must include an effective date for the new charges;

(f) Establish adequate controls to assure that all charges are captured, batched and reconciled with batch totals;

(g) Provide all input forms;

(h) Provide medical expertise regarding reimbursement of medically necessary services of Client arising from third-party payer disputes or patient inquiries;

(i) Be responsible for all medical decisions concerning patient care.

(j) Client will promptly review the refund register/refund checks prepared for Client or through a monthly management report that identifies current refunds that are due and will, within thirty (30) days of receipt of the refund register, refund checks prepared for Client or monthly management report will write a check to Service Provider's refund account for refunds to be sent to the patient or third-party payer based upon information provided by Service Provider; and

(k) Prepare and release Client's annual unclaimed property return.

3 SERVICE FEES

3.1 For Services rendered under this Service Schedule Service Provider will be paid a service fee equal to __% of the "Net Revenue" of Client. "Net Revenue" will mean cash receipts arising from the provision of patient services and related activities less refunds.

3.2 For Services rendered under the MA from this _____ day of _____, 20__ through this _____ day of _____, 20__. Client will pay Service Provider a service fee equal to ____% of the net revenue of Client, in accordance with Section 4 of the MA. In addition to the ____% service fee, Client will pay Service Provider a one-time initial fee of $_____ upon delivery of the computer **hardware and software** set forth on Schedule 1 attached hereto and made apart hereof (collectively, "Equipment") to Client's address set forth in the MA. With respect to the Equipment, Service Provider agrees it will be responsible for annual fees for **hardware and software** including the billing interface. Service Provider will also be responsible for the initial and monthly fees related to the air-cards on internet service fees for the duration of the MA. Net revenue will mean cash receipts arising from the provision of patient services and related activities less refunds. In the event that the total revenue for Service Provider in a month does not exceed $500.00, Service Provider will be paid a minimum service fee of $500.00 for that month.

3.3 For Supplemental Payment Recovery Assistance Services rendered under Exhibit A-1, Client will pay Service Provider a service fee equal to __% of the Supplemental Payments recovered by Service Provider on behalf of Client, in accordance with Section 4 of the MA. Supplemental Payments will include any payments for ambulance services, including all nonemergency and emergency patient transports that are reimbursed by Texas Medicaid to Client. In addition to the ____% service fee due by Client to Service Provider under this Sales Order, Client will pay Service Provider a one-time, upfront fee of $3,900.00 ("Setup Fee") for completion of the pre-cost report submittal requirements necessary for Client's participation in the Texas Ambulance Supplemental Payment Program. The Setup Fee will be due upon Client's execution of this Service Schedule. Client acknowledges and agrees that Service Provider will be entitled to receive the service fee describer in this sub-section even after expiration or earlier termination of this Service Schedule, provided that Service Provider provided such services on or before the date of expiration or termination.

3.4 All service fees are exclusive of all federal, state and local taxes, including sales taxes, assessed on or due in respect of any Services performed by Service Provider under the MA, for which taxes Client will be solely responsible. Client will reimburse Service Provider for all those costs and expenses of Client paid by Service Provider or any subsidiary or affiliate of Service Provider Group on behalf of Client in connection with the provision of Services hereunder.

3.5 There will be a charge to the Client for requests, including but not limited to, requests for special programming and non-standard reports. The cost for such requests will be determined on an individual basis and will be reimbursed in accordance with Section _____.

3.6 Equipment. Client acknowledges that the Equipment and any services related thereto are provided strictly "as is," and Service Provider makes no additional warranties, express, implied, arising from course of dealing or usage of trade, or statutory, as to the Equipment, any associated services or any matter whatsoever. In particular, any and all warranties of merchantability, fitness for a particular purpose, title and non-infringement are expressly excluded.

EXHIBIT A-1

SUPPLEMENTAL PAYMENT RECOVERY ASSISTANCE SERVICES

1. Description of Services.

As part of the Service Provider's Supplemental Payment Assistance Services, Service Provider's responsibilities under this Service Schedule will include:

(a) Advising and assisting Client with enrolling in the Texas Medicaid Supplemental Payment Program;
(b) Assisting Client with enrolling in the Texas Ambulance Supplemental Payment Program ("ASPP");
(c) Managing the program applications and required cost reports for Client in accordance with the ASPP;
(d) Managing the ASPP pre-cost report submittal process for Client, which may also include:

- Developing and submitting the Provider Approval materials to the Texas Health and Human Services Commission (HHSC) on behalf of Client;
- Receiving the Provider Approval from HHSC for Client's participation in the ASPP,
- Developing and submitting the Cost Allocation Model and Report to HHSC on behalf of Client for review as part of the ASPP;
- Changing and finalizing the Cost Allocation Model during HHSC's review of the Cost Allocation Model and Report, to meet HHSC's requirements to move forward with the cost report submittal.

(e) Assisting Client in developing cost models for EMS transports for submission to ASPP;
(f) Assisting Client with submitting other annual reports as my required by the ASPP.
(g) Ensuring that cost report preparer(s) engaged on behalf of Client by Service Provider are certified in accordance with all applicable rules, laws and regulations.
(h) Ensuring that it utilizes separate staff for all billing and cost report preparation services provided to Client.

2. Client Responsibilities.

Client acknowledges and understands that inaccurate or false data submissions, even advertent ones, can lead to a false claim charge or Medicaid program exclusion. Therefore, Client agrees that it will use best efforts to:

(a) Ensure the accuracy of all cost report data provided by Client to Service Provider and provide written certification of the accuracy of such data to Service Provider and all applicable governmental agencies;
(b) Make its internal practices, books and records relating to all cost report data provided to Service Provider by Client available to Service Provider to ensure the accuracy of all such data;

(c) Comply with Service Provider policies and procedures for the documentation of all cost report data as established and provided to Client by Service Provider from time to time; and

(d) Provide Service Provider with the following as part of Client's request for Supplemental Payment:

- An organizational chart of Client's agency;
- An organizational chart of Client's ambulance department;
- Identification of the specific geographic service area covered by Client's ambulance department;
- Copies of job descriptions for all staff employed within Client's ambulance department and an estimated percentage of time spent working for Client's ambulance department and for other departments of Client's agency;
- Primary contact person for Client's agency; and

- A signed letter documenting the governmental provider's voluntary contribution of non-federal funds.

3. Indemnification.

Client will indemnify and hold harmless Service Provider and its affiliates, employees and agents from and against, and at the option of Service Provider (or any of its affiliates, employees or agents) defend against, at Client's sole expense, all claims, liabilities, damages, losses and expenses as they are accrued, including court costs and fees and expenses of attorneys, expert witnesses and other professionals, arising out of, relating to or resulting from:

(a) any breach or alleged breach of any representation, warranty, covenant or obligation of Client pertaining to the Supplemental Payment Recovery Assistance Services; and

(b) any alleged negligent act or omission or intentional misconduct of Client or Client's employees or agents or subcontractors related to any of Client's obligations pertaining to the Supplemental Payment Recovery Assistance Services.

Equipment Quote for _____

ePCR
(List the product) Patient Care Reporting software:

Service Provider agrees to provide (List the Client's DBA Name) the following listed software and hardware for EMS patient care reporting based on the conditions listed below.

Software:

- Example: ESO Patient Care Reporting Software including cardiac monitor interface for 4000 runs per year for 3 years (12,000 runs).
- Example: CAD Interface from ESO

Hardware:

- Example: 4 Panasonic toughbook (PF-19) or (H2) computers
- Example: 3 year factory warranties for the 4 computers
- Example: 4 Verizon or AT&T air-cards
- Example: Monthly fee for 4 Verizon or AT&T air-cards

Conditions:

1. Terms of agreement will be for x year period.

2. If the MA terminates prior to the ___ term, than Client will reimburse Contractor for the remaining costs as outlined in the attached Amortization Schedule. Client is not responsible for interest on the Equipment, calculated at eleven percent (11%), in the amount of _____ ($_____).

3. Hardware set-up installation and maintenance (other than warranty) are not a part of this MA.

4. Support services for (hard/software) are provided by (Vendor supplying hard/software) through on-line and phone support.

Equipment Amortization Chart for _____

Service Provider will deliver to Client Equipment to be utilized by Client. Client acknowledges it is responsible for installation of the Equipment.

Amortization Chart

Month	Balance Due
1	x
2	x
3	x
4	x
5	x
6	x
7	x
8	x
9	x
10	x
11	x
12	x
13	x
14	x
15	x
16	x
17	x
18	x
19	x
20	x
21	x
22	x
23	x
24	x
25	x
26	x
27	x
28	x
29	x
30	x
31	x
32	x
33	x
34	x
35	x
36	x
	0.00

SERVICE SCHEDULE 2
BUSINESS PERFORMANCE INSIGHT SERVICES

The MA Terms and Conditions and this Service Schedule apply to the Business Performance Insight Services rendered by Service Provider under this Service Schedule.

1. Term

1.1 Initial Term of Schedule. The initial term of this Service Schedule is three years (the "Schedule 2 Term") beginning _____, 201___ (the "Schedule 2 Commencement Date").

1.2 Automatic Renewal. This Service Schedule will automatically renew for one year terms unless (i) either party delivers to the other written notice of termination at least 90 days prior to the expiration of the then-current term, or (ii) as otherwise set forth in the MA.

2 Scope of Services

2.1 Responsibilities. Each party agrees to perform its respective responsibilities identified below in a timely and diligent manner. Client acknowledges and agrees that Service Provider's performance of the Business Performance Insight Services is dependent upon Client's performance of its responsibilities as set forth in this Service Schedule.

2.1.1 Service Provider Responsibilities.

(a) Basic User Access.

- **(i)** Provide 24 hour access, less scheduled or unscheduled downtime for maintenance or repair, from any Internet access point to the Client reporting portal.
- **(ii)** Provide access to all current and future standard level reports generated by Service Provider.
- **(iii)** Provide ability to review reports as HTML and PDF documents.
- **(iv)** Provide the ability to save report documents as PDF, Excel or CSV file formatted documents.
- **(v)** Provide access to the Dashboard folder and associated current and future Dashboard based deliverables.

(b) Intermediate User Access.

- **(i)** Includes all activities defined in the Basic User Access.
- **(ii)** Provide access to all current and future public reports generated by Service Provider.
- **(iii)** Provide online analysis functionality which allows Client the ability to drill down, filter and group data as well as apply simple updates such as adding/removing fields, re-sorting, calculations, etc.
- **(iv)** Provide a personal reporting mail box which enables Client to send/receive reports to/from other users within Client group.
- **(v)** Provide ability to save in a personal folder a copy of an altered report for future data refresh or editing.
- **(vi)** Provide the ability to schedule saved reports as needed.

(c) Advanced User Access.

- **(i)** Includes all activities as defined in the Basic and Intermediate User Access.
- **(ii)** Provide ability to create, edit and save document structures and formats.
- **(iii)** Provide ability to manipulate report query, prompts, filters and scope of analysis.
- **(iv)** Provide ability to modify/create formulas and report variables.
- **(v)** Provide access to Service Provider's complete ad-hoc reporting development framework.
- **(vi)** Provide the ability to customize reporting queries.

(vii) Provide the ability to set personal user reporting preferences.

(viii) Upon Client request, provide a Client named folder to be utilized by Client appointed Advanced User(s) to store reports for Client use.

(d) Support Services. Service Provider will provide telephone and e-mail support to answer questions and address issues related to the Practice Focus Web Based Reporting product at no cost to Client. Normal support hours and response time are as follow:

Monday through Friday: 8:00 a.m. until 8:00 p.m. eastern time

(e) Training Services. Service Provider will provide Client with one 1-hour webinar for Basic Users on the Practice Focus Web Based Reporting Product at no cost to Client. Recommended training for Intermediate Users is either a 2-day on-site Intermediate training session or attendance at a public Intermediate training session. Recommended training for Advanced Users is attendance at an Intermediate training session and additional attendance at either a 2-day on-site Advanced training session or attendance of a public Advanced training session. Service Provider can provide Client training classes for a specific Client environment or as specifically requested by Client.

(f) eLearning Training For Intermediate User Access. If requested by Client's "Manager," Service Provider will provide a one year subscription for Intermediate User(s) at the fees set forth in this Service Schedule.

(g) Mobile Electronic Authorized User Access. If requested by Client's "Manager," Service Provider will provide Client an Authorized User and allow such Authorized User to access Business Performance Insight Services by means of an I-Pad or other mobile electronic device authorized by Service Provider at the fees set forth in this Service Schedule.

(h) Consulting Services. If requested by Client's "Manager," Service Provider's staff of resources can design, build and generate customized Client specific Practice Focus deliverables, including but not limited to customized reports, graphs and dashboards at the fees set forth in this Service Schedule.

2.1.2 Client Responsibilities. Client will:

(a) Establish Client's broadband access to the Internet for use of the Practice Focus Web Based Reporting product.

(b) Allow access to such Practice Focus Web Based Reporting Product only to user(s) authorized by Service Provider to access and use such Practice Focus Web Based Reporting Product ("Authorized User").

(c) Provide a competent member of Client's staff ("Manager") to be trained by Service Provider on use of the Practice Focus Web Based Reporting product to serve as a liaison to Service Provider on Practice Focus Web Based Reporting matters.

(d) After Service Provider has provided training to the Client's Manager, Client agrees to train only other Authorized Users on use of the Practice Focus Web Based Reporting product.

(e) Client's Manager may change Authorized Users level of use or add or subtract Authorized Users on no less than 15 days' prior written notice to Service Provider (e-mail requests are acceptable). Client will pay Service Provider the applicable pro-rated Authorized User fee for any Authorized User added or subtracted during any month.

(f) Client acknowledges and agrees that it shall not: (i) transmit or share identification and/or password codes to persons other than the Authorized Users for whom such codes were generated; (ii) permit Authorized Users

to share identification and/or password codes with others; (iii) permit the identification and/or password codes from being cached in proxy servers and accessed by individuals who are not Authorized Users; (iv) permit access to the Business Performance Insight Services through a single identification and/or password code being made available to multiple users on a network; or (v) attempt or permit any person without valid identification and/or password codes to attempt to access the Business Performance Insight Services.

(g) Client acknowledges (i) that certain services or obligations of Service Provider hereunder may be dependent on Client providing access to certain data, information, or assistance to Service Provider from time to time (collectively, "Cooperation"); and (ii) that such Cooperation may be essential to the performance of services by Service Provider. The parties agree that any delay or failure by Service Provider to provide Services hereunder which is caused by Client's failure to provide timely Cooperation reasonably requested by Service Provider shall not be deemed to be a breach of Service Provider's performance obligations under this MA.

(h) Client acknowledges that (i) the Business Performance Insight Services embodies valuable and proprietary trade secrets of Service Provider, (ii) the identification and password codes issued by Service Provider hereunder constitute valuable confidential information, which is proprietary to Service Provider, (iii) the Business Performance Insight Services may be utilized by Client only to facilitate its use of the Services hereunder in accordance with the terms of this MA, (iv) any reports, report formats, documents, ideas or other discoveries made or developed by Client during its use of the Business Performance Insight Services may be utilized by Client only to facilitate its use of the Services hereunder in accordance with the terms of this MA and shall not be given or sold to or used on behalf of any third-party and shall remain the sole and exclusive property of Service Provider, and (v) Client agrees, and will cause its employees, agents, subcontractors and representatives to agree, that it/they shall not copy, modify, change, disassemble, or reverse engineer any part or aspect of the Business Performance Insight Services. Client shall safeguard the right to access the Business Performance Insight Services and confidentiality of such identification and password codes, using the same standard of care which Client uses for its similar confidential materials, but in no event less than reasonable care.

(i) Client acknowledges and agrees that it is solely responsible for the security of any information received through Business Performance Insight Services on any device or in any printed format.

(j) Client acknowledges and agrees that it shall (1) immediately notify Service Provider of any Authorized User Client no longer wishes to have access to the Software, and (2) indemnify and hold Service Provider harmless from and against any losses (including fines or penalties and interest) incurred by Service Provider as a result of Client's failure to so notify Service Provider.

3 SERVICE FEES

3.1 Beginning on the Schedule 2 Commencement Date listed in Section 1 above, Client agrees to pay Service Provider the fees as set forth below:

3.1.1 User Access. Authorized Users may obtain Basic, Intermediate or Advanced User Access at an amount equal to $100.00 per Authorized User per month; and

3.1.2 Training Services. If Client's Manager request private classes at a Service Provider facility or at Client's site, the Client will pay an amount equal to $1,250.00 per day for each day spent by a Service Provider employee or agent in the provision of such Training Services for Client's Authorized Users, or $500.00 per day per Authorized User for public classes at a Service Provider facility; and

3.1.3 Consulting Services. If Client's Manager request Consulting Services, the Client will pay an amount equal to $150.00 per hour for each hour spent by a Service Provider employee or agent in the provision of such Consulting Services during the previous month, such Consulting Services to be set forth in a separate *Practice Focus Web Based Reporting Product Service Form*; and

3.1.4 eLearning Training for Intermediate User Access. If Client's Manager request eLearning Training for Intermediate User Access, then Service Provider will provide a 1 year subscription at an amount equal to $250.00 per year per Authorized User. If Client has signed up for Live Intermediate Training (either on-site or off-site), eLearning Training will be provided at no cost to Client; and

3.1.5 Travel Expense. Client will pay an amount equal to the out-of-pocket travel and travel related expenses incurred by Service Provider employees and/or agents involved in the initial implementation and general product overview sessions, Training Services or Consulting Services during the previous month; and

3.1.6 Implementation Fees. Service Provider and the Client's Manager will mutually agree-upon the number of Authorized Users, and Training if applicable, and the Client's Manager will complete the *Practice Focus Web Based Reporting Product Service Form*. The Client's Manager and Service Provider will mutually agree upon a revised *Practice Focus Web Based Reporting Product Service Form* any time the Client's Manager requests a change in Client's use of the Practice Focus Web Based Reporting Product; and

3.1.7 Mobile Electronic Authorized User Access. If Client's Manager request Service Provider will provide Client an Authorized User to access the Business Performance Insight Services by means of an I-Pad or other mobile electronic device at a fee of $50.00 per Authorized User per month

0001P Executive Summary Reports (ESR) Package

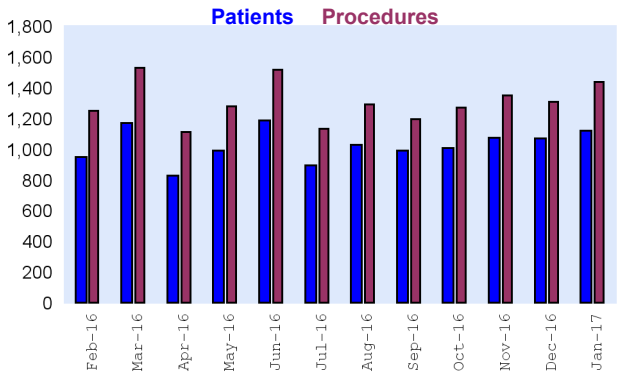
SAMPLE PRACTICE

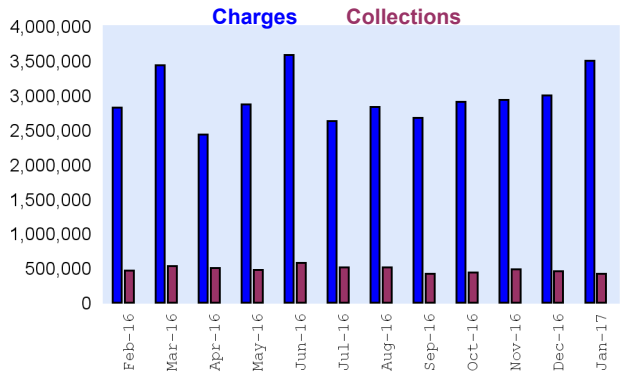
January 2017

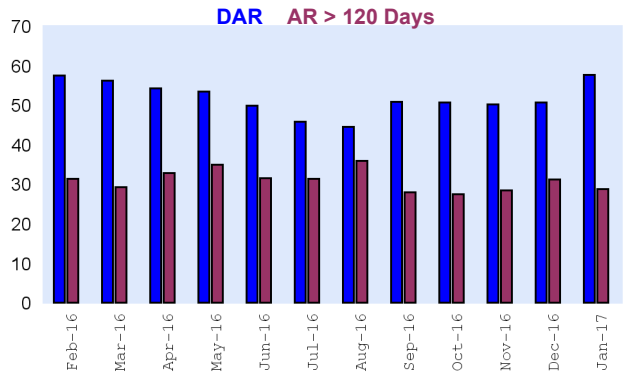
The 0001P Executive Summary Reports (ESR) Package presents a comprehensive monthly view of the practice through a series of 7 reports. View major production measures and performance metrics. Track month to month over 12 months and compare metrics year to year.

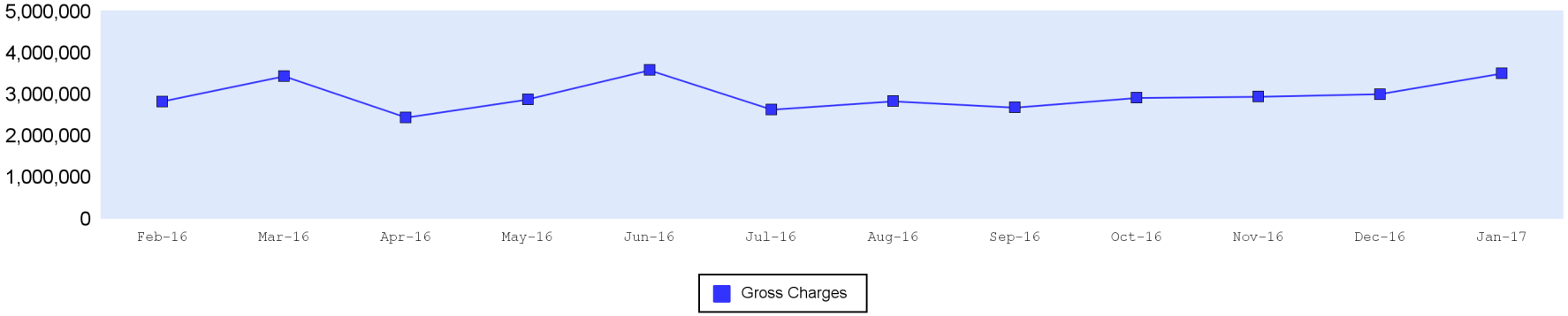
	Volume		Charges			Collections			Collection Rates			Accounts Receivable				Net Bad Debt	
Account Period	Patients	Procedures	Gross	Adjustments	Net	Gross	Adjustments	Net	GCR*	NCR*	Net GCR Lag*	Ending AR	Days in AR	%AR >120	Credit Balance	Amount	% *
Feb-16	948	1,252	2,824,598	(1,846,758)	977,840	(463,198)	4,695	(458,503)	14.7%	42.5%	19.2%	5,048,477	57.6	31.3%	(134,659)	0	0.0%
Mar-16	1,169	1,529	3,437,959	(2,400,352)	1,037,606	(529,752)	3,081	(526,671)	14.8%	43.4%	19.6%	5,441,808	56.3	29.3%	(134,522)	(117,604)	0.7%
Apr-16	828	1,111	2,434,145	(2,168,940)	265,204	(500,808)	331	(500,477)	15.3%	47.2%	16.9%	5,188,902	54.3	32.8%	(166,773)	(17,633)	0.8%
May-16	989	1,279	2,875,257	(2,375,705)	499,552	(475,892)	3,136	(472,756)	16.3%	61.3%	17.2%	5,135,441	53.4	35.0%	(239,077)	(80,256)	1.3%
Jun-16	1,189	1,517	3,583,057	(3,211,699)	371,358	(580,749)	2,451	(578,298)	17.2%	81.6%	17.7%	4,879,462	49.9	31.6%	(274,865)	(49,039)	1.5%
Jul-16	895	1,134	2,626,609	(2,377,916)	248,693	(509,376)	3,413	(505,963)	18.2%	114.3%	17.5%	4,574,747	45.8	31.4%	(305,474)	(47,445)	1.8%
Aug-16	1,028	1,290	2,829,362	(2,456,994)	372,368	(516,232)	2,633	(513,599)	18.5%	130.0%	17.6%	4,418,431	44.5	35.9%	(214,962)	(15,085)	1.8%
Sep-16	990	1,197	2,676,553	(2,118,008)	558,545	(421,432)	9,466	(411,966)	18.0%	99.7%	15.8%	4,551,763	50.9	27.9%	(242,113)	(13,247)	1.3%
Oct-16	1,006	1,272	2,911,486	(2,322,069)	589,417	(441,581)	30,765	(410,815)	17.7%	96.3%	16.4%	4,698,199	50.8	27.4%	(235,964)	(32,165)	1.4%
Nov-16	1,075	1,350	2,939,214	(2,442,909)	496,305	(483,836)	44,744	(439,092)	17.4%	90.3%	15.0%	4,712,728	50.3	28.5%	(218,326)	(42,684)	1.1%
Dec-16	1,072	1,309	3,002,950	(2,332,258)	670,692	(455,126)	644	(454,481)	17.2%	90.2%	15.3%	4,927,309	50.6	31.2%	(207,131)	(1,630)	0.9%
Jan-17	1,122	1,436	3,504,933	(2,004,121)	1,500,813	(417,048)	18,720	(398,328)	16.3%	74.7%	14.6%	5,997,560	57.8	28.8%	(208,845)	(32,233)	0.8%
12 Mth Total	12,311	15,676	35,646,123	(28,057,730)	7,588,393	(5,795,029)	124,078	(5,670,951)	-	-	-	-	-	-	-	(449,022)	1.1%
Current FYTD	1,122	1,436	3,504,933	(2,004,121)	1,500,813	(417,048)	18,720	(398,328)	-	-	-	-	-	-	(208,845)	(32,233)	0.8%
Previous FYTD	881	1,136	2,531,346	(2,131,727)	399,620	(581,040)	2,936	(578,104)	-	-	-	-	-	-	(131,606)	0	0.0%
Current 12 Mth Avg	1,026	1,306	2,970,510	(2,338,144)	632,366	(482,919)	10,340	(472,579)	16.3%	74.7%	16.4%	4,964,569	51.8	30.9%	(215,226)	(37,419)	1.1%
Prev 12 Mth Avg	863	1,161	2,513,360	(1,646,228)	867,132	(364,690)	796	(363,894)	14.5%	42.0%	16.3%	4,572,303	62.2	18.6%	(38,149)	0	0.0%
Variance%	18.9%	12.5%	18.2%	42.0%	(27.1%)	32.4%	1,199.6%	29.9%	12.0%	78.1%	0.3%	8.6%	(16.7%)	65.7%	464.2%	0.0%	0.0%

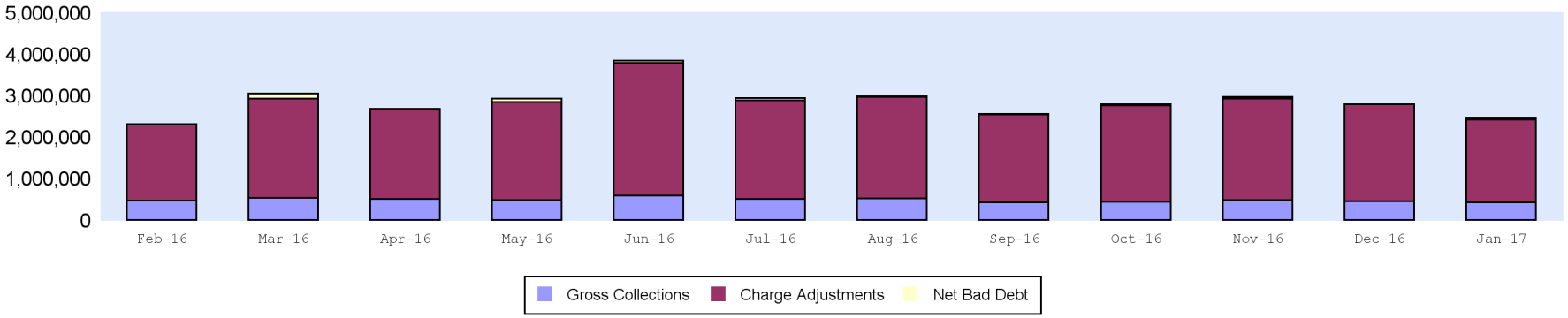
* GCR (Gross Collections / Gross Charges) and NCR (Net Collections / Net Charges) calculations are based on a maximum of 12 months of data. The Net GCR Lag (Net Collections / Gross Charges) is based on a maximum of 3 months of data with a 1 month Gross Charge Lag. Net Bad Debt % is based on a 6 month average.







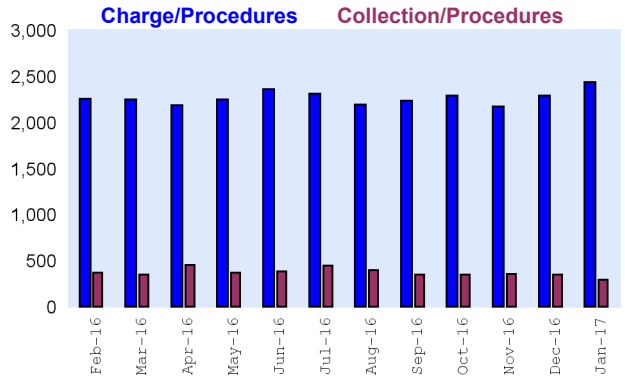


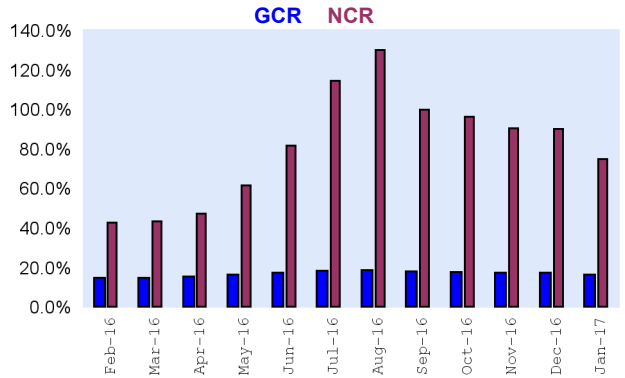


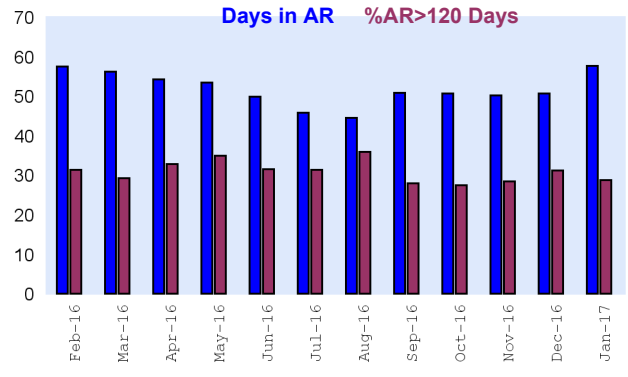
	Feb-16	Mar-16	Apr-16	May-16	Jun-16	Jul-16	Aug-16	Sep-16	Oct-16	Nov-16	Dec-16	Jan-17	Curr 12 Mth Avg	Prev 12 Mth Avg
Gross Charges	2,824,598	3,437,959	2,434,145	2,875,257	3,583,057	2,626,609	2,829,362	2,676,553	2,911,486	2,939,214	3,002,950	3,504,933	2,970,510	2,513,360
Charge Adjustments	(1,846,758)	(2,400,352)	(2,168,940)	(2,375,705)	(3,211,699)	(2,377,916)	(2,456,994)	(2,118,008)	(2,322,069)	(2,442,909)	(2,332,258)	(2,004,121)	(2,338,144)	(1,646,228)
Gross Collections	(463,198)	(529,752)	(500,808)	(475,892)	(580,749)	(509,376)	(516,232)	(421,432)	(441,581)	(483,836)	(455,126)	(417,048)	(482,919)	(364,690)
Net Bad Debt	0	(117,604)	(17,633)	(80,256)	(49,039)	(47,445)	(15,085)	(13,247)	(32,165)	(42,684)	(1,630)	(32,233)	(37,419)	0

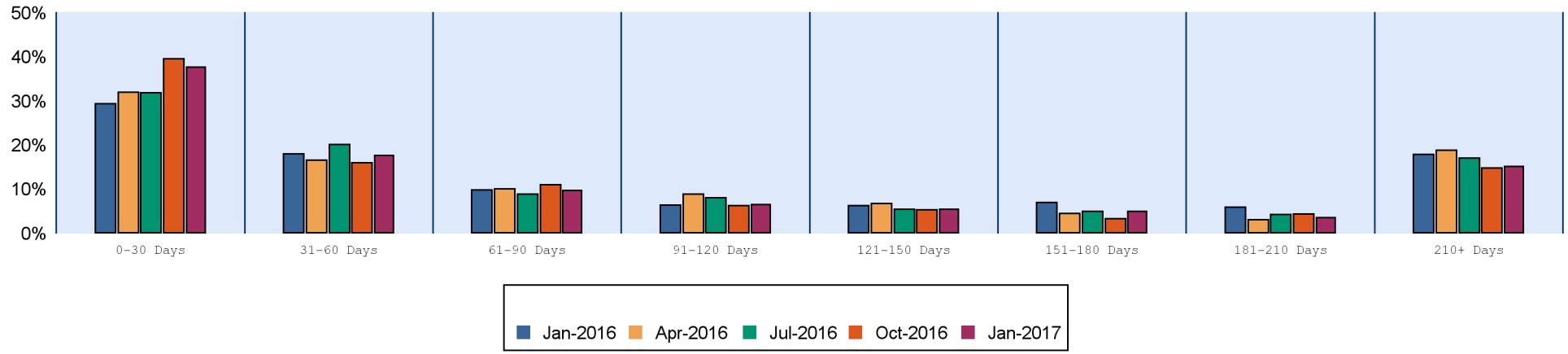
	Current Month			Comparative Rolling Qtr					FYTD			Fiscal Year over Year			Fiscal Year	
Key Performance Measurements	Jan-2017	6 month Average	% var	Prev Year Nov-15 to Jan-16	Previous Aug-16 to Oct-16	Current Nov-16 to Jan-17	% Var Curr vs Prev Year	% Var Curr vs Prev	Previous Jan-16 to Jan-16	Current Jan-17 to Jan-17	% Var	Jan-15 to Dec-15	Jan-16 to Dec-16	% Var	Run Rate Jan-17 to Dec-17	% Var Run Rate vs Prev FY
Procedures	1,436	1,309	9.7%	3,600	3,759	4,095	13.8%	8.9%	1,136	1,436	26.4%	9,316	15,376	65.0%	17,232	12.1%
Total RVU	20,587	18,384	12.0%	52,102	52,670	57,634	10.6%	9.4%	16,770	20,587	22.8%	132,836	217,241	63.5%	247,042	13.7%
Gross Charges	3,504,933	2,977,417	17.7%	7,732,489	8,417,401	9,447,098	22.2%	12.2%	2,531,346	3,504,933	38.5%	20,088,894	34,672,536	72.6%	42,059,201	21.3%
Gross Charges per Procedure	2,441	2,275	7.3%	2,148	2,239	2,307	7.4%	3.0%	2,228	2,441	9.5%	2,156	2,255	4.6%	2,441	8.2%
Gross Collections	(417,048)	(455,876)	(8.5%)	(1,552,398)	(1,379,245)	(1,356,010)	(12.7%)	(1.7%)	(581,040)	(417,048)	(28.2%)	(2,701,169)	(5,959,020)	120.6%	(5,004,581)	(16.0%)
Gross Collection per Procedure	(290)	(348)	(16.6%)	(431)	(367)	(331)	(23.2%)	(9.8%)	(511)	(290)	(43.2%)	(290)	(388)	33.7%	(290)	(25.1%)
Gross Collection per RVU	(20)	(25)	(18.3%)	(30)	(26)	(24)	(21.0%)	(10.2%)	(35)	(20)	(41.5%)	(20)	(27)	34.9%	(20)	(26.1%)
Net Collections	(398,328)	(438,047)	(9.1%)	(1,546,636)	(1,336,381)	(1,291,901)	(16.5%)	(3.3%)	(578,104)	(398,328)	(31.1%)	(2,696,945)	(5,850,726)	116.9%	(4,779,936)	(18.3%)
Net Collection per Procedure	(277)	(335)	(17.1%)	(430)	(356)	(315)	(26.6%)	(11.3%)	(509)	(277)	(45.5%)	(289)	(381)	31.4%	(277)	(27.1%)
Net Collection per RVU	(19)	(24)	(18.8%)	(30)	(25)	(22)	(24.5%)	(11.7%)	(34)	(19)	(43.9%)	(20)	(27)	32.7%	(19)	(28.2%)
GCR*	16.3%	15.3%	6.2%	20.1%	16.4%	14.4%	(28.5%)	(12.4%)	23.0%	11.9%	(48.2%)	13.4%	17.2%	27.8%	11.9%	(30.8%)
NCR*	74.7%	62.8%	19.1%	125.2%	87.9%	48.4%	(61.3%)	(44.9%)	144.7%	26.5%	(81.7%)	36.4%	90.2%	147.6%	26.5%	(70.6%)
Contractual Adjustments	(2,004,121)	(2,279,393)	(12.1%)	(6,497,356)	(6,897,071)	(6,779,289)	4.3%	(1.7%)	(2,131,727)	(2,004,121)	(6.0%)	(12,684,325)	(28,185,336)	122.2%	(24,049,450)	(14.7%)
Net Bad Debt	(32,233)	(22,841)	41.1%	0	(60,498)	(76,547)	0.0%	26.5%	0	(32,233)	0.0%	0	(416,789)	0.0%	(386,797)	(7.2%)
Days in AR	57.8	50.9	13.6%	53.3	50.8	57.8	8.4%	13.7%	53.3	57.8	8.4%	55.0	50.6	(7.9%)	57.8	14.1%
% AR > 120 Days	28.8%	29.9%	(3.6%)	36.7%	27.4%	28.8%	(21.6%)	5.0%	36.7%	28.8%	(21.6%)	35.9%	31.2%	(13.3%)	28.8%	(7.6%)

* GCR and NCR calculations are based on a maximum of 12 months of data unless otherwise specified by the time period defined in the column.

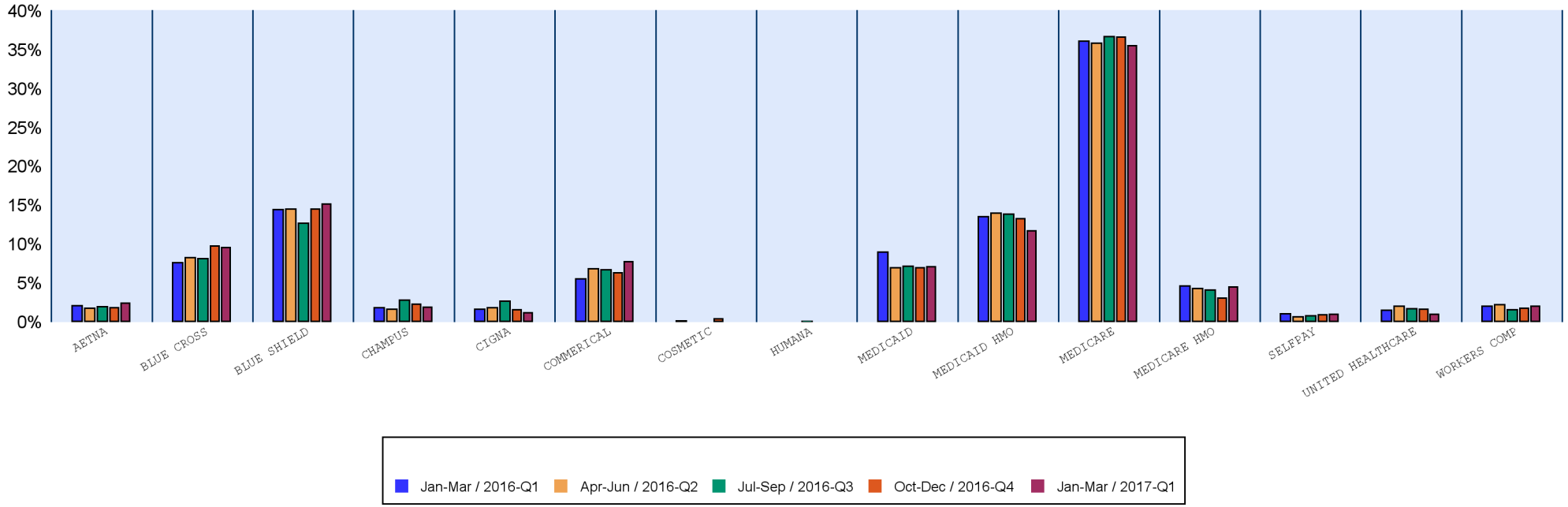








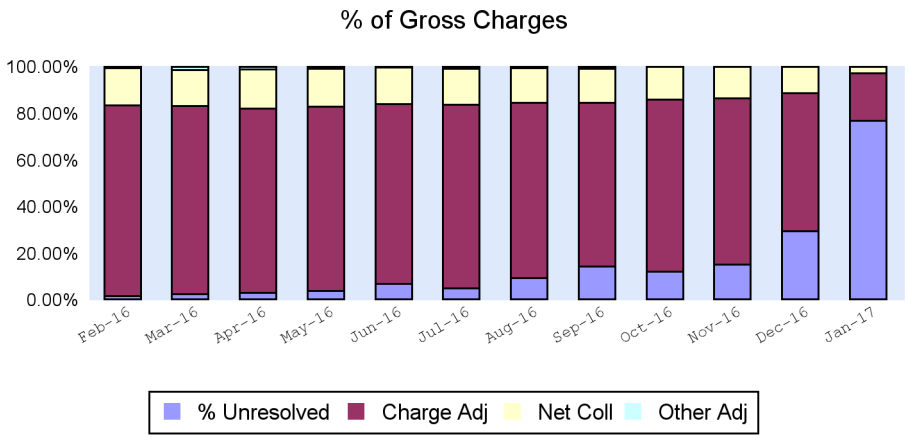
	Feb-16	Mar-16	Apr-16	May-16	Jun-16	Jul-16	Aug-16	Sep-16	Oct-16	Nov-16	Dec-16	Jan-17	12 Mth Avg	% Var Jan-17 to Oct-16
0-30 Days	1,821,698	2,203,173	1,654,901	1,497,645	1,833,020	1,452,726	1,529,721	1,981,389	1,857,846	1,930,968	1,808,738	2,253,688	1,818,793	21.3%
31-60 Days	868,763	697,242	856,893	895,677	693,782	918,303	522,450	698,413	748,712	600,905	787,565	1,055,230	778,661	40.9%
61-90 Days	482,326	531,513	518,069	514,082	466,867	403,040	503,080	298,720	512,189	433,360	426,700	577,649	472,299	12.8%
91-120 Days	294,256	414,312	455,821	432,293	342,645	364,941	275,373	301,998	291,858	404,849	369,315	385,430	361,091	32.1%
121-150 Days	261,792	282,325	347,906	407,541	278,752	242,725	342,419	182,459	243,835	231,066	315,594	324,288	288,392	33.0%
151-180 Days	209,404	177,970	230,089	306,102	224,477	225,052	214,328	212,830	152,202	200,026	216,291	289,589	221,530	90.3%
181-210 Days	275,625	164,862	154,443	184,296	155,101	190,366	210,024	157,985	199,107	133,382	178,722	208,384	184,358	4.7%
210+ Days	834,614	970,411	970,780	897,806	884,818	777,593	821,036	717,970	692,451	778,172	824,382	903,301	839,445	30.4%
Total	5,048,477	5,441,808	5,188,902	5,135,441	4,879,462	4,574,747	4,418,431	4,551,763	4,698,199	4,712,728	4,927,309	5,997,560	4,964,569	27.7%
Days in AR	57.6	56.3	54.3	53.4	49.9	45.8	44.5	50.9	50.8	50.3	50.6	57.8	51.8	13.7%
% AR > 120	31.3%	29.3%	32.8%	35.0%	31.6%	31.4%	35.9%	27.9%	27.4%	28.5%	31.2%	28.8%	30.9%	5.0%
$ AR > 120	1,581,435	1,595,569	1,703,218	1,795,745	1,543,148	1,435,736	1,587,808	1,271,243	1,287,594	1,342,646	1,534,990	1,725,563	1,533,725	34.0%

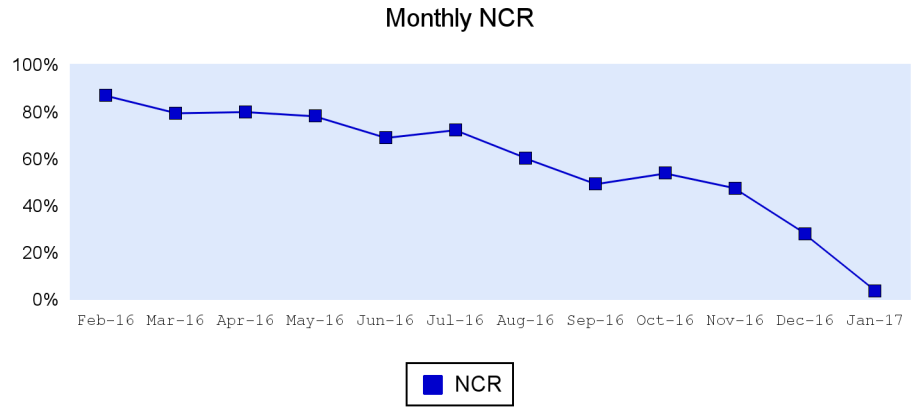


Payor Group	Jan-Mar2016	Apr-Jun2016	Jul-Sep2016	Oct-Dec2016	Jan-Mar2017
AETNA	2%	2%	2%	2%	2%
BLUE CROSS	8%	8%	8%	10%	10%
BLUE SHIELD	14%	14%	13%	14%	15%
CHAMPUS	2%	2%	3%	2%	2%
CIGNA	2%	2%	3%	1%	1%
COMMERICAL	5%	7%	7%	6%	8%
COSMETIC	0%	0%	0%	0%	0%
HUMANA	0%	0%	0%	0%	0%
MEDICAID	9%	7%	7%	7%	7%
MEDICAID HMO	13%	14%	14%	13%	12%
MEDICARE	36%	36%	37%	37%	35%
MEDICARE HMO	5%	4%	4%	3%	4%
SELFPAY	1%	1%	1%	1%	1%
UNITED HEALTHCARE	1%	2%	2%	2%	1%
WORKERS COMP	2%	2%	2%	2%	2%
Total	100%	100%	100%	100%	100%

		Charges			Collections					NCR		% of Gross Charges			
Charge Month	Patients	Gross (a)	Adjustments (b)	Net (c=a+b)	Gross (d)	Adjustments (e)	Net (f=d+e)	Other Adjustments	AR Balance	Monthly (g=f/c)	Coll/ Patients	% Unresolved	Charge Adj	Net Coll	Other Adj
Prior 12 Mths	8,392	22,624,402	(18,031,023)	4,593,379	(4,129,435)	71,158	(4,058,277)	(230,741)	304,361	88.4%	483.59	1.35%	79.70%	17.94%	1.02%
Feb-16	950	2,819,492	(2,303,599)	515,893	(452,876)	4,060	(448,816)	(21,364)	45,713	87.0%	472.44	1.62%	81.70%	15.92%	0.76%
Mar-16	1,169	3,404,400	(2,748,081)	656,319	(533,097)	11,620	(521,477)	(54,338)	80,504	79.5%	446.09	2.36%	80.72%	15.32%	1.60%
Apr-16	822	2,382,669	(1,881,478)	501,192	(404,843)	3,924	(400,919)	(30,584)	69,689	80.0%	487.74	2.92%	78.97%	16.83%	1.28%
May-16	991	2,878,243	(2,276,173)	602,071	(489,056)	18,647	(470,408)	(27,536)	104,126	78.1%	474.68	3.62%	79.08%	16.34%	0.96%
Jun-16	1,187	3,570,537	(2,751,058)	819,479	(572,502)	7,849	(564,653)	(9,968)	244,858	68.9%	475.70	6.86%	77.05%	15.81%	0.28%
Jul-16	894	2,618,045	(2,060,046)	557,999	(409,797)	6,380	(403,417)	(25,114)	129,467	72.3%	451.25	4.95%	78.69%	15.41%	0.96%
Aug-16	1,023	2,809,431	(2,118,541)	690,890	(419,687)	3,215	(416,471)	(17,009)	257,409	60.3%	407.11	9.16%	75.41%	14.82%	0.61%
Sep-16	1,005	2,789,768	(1,956,149)	833,619	(411,919)	2,000	(409,919)	(27,579)	396,120	49.2%	407.88	14.20%	70.12%	14.69%	0.99%
Oct-16	1,015	2,916,603	(2,151,147)	765,455	(413,102)	1,007	(412,095)	(4,752)	348,609	53.8%	406.00	11.95%	73.76%	14.13%	0.16%
Nov-16	1,077	2,942,739	(2,097,422)	845,317	(401,822)	1,378	(400,444)	(62)	444,811	47.4%	371.81	15.12%	71.27%	13.61%	0.00%
Dec-16	1,075	3,006,310	(1,783,057)	1,223,253	(341,223)	0	(341,223)	0	882,030	27.9%	317.42	29.34%	59.31%	11.35%	0.00%
Jan-17	1,118	3,503,722	(715,980)	2,787,743	(97,879)	0	(97,879)	0	2,689,864	3.5%	87.55	76.77%	20.43%	2.79%	0.00%
24 Mth Total	20,718	58,266,363	(42,873,756)	15,392,608	(9,077,238)	131,238	(8,945,999)	(449,048)	5,997,560	-	431.80	10.29%	73.58%	15.35%	0.77%

* All activity has been summarized at the encounter accounting period level. Amounts displayed in each column may not reconcile to deliverables generated using posting period. The 24 Mth Total row is the sum of data represented on this report which is a maximum of 24 months. The total amount displayed in the AR Balance column may or may not equal the client's ending AR balance depending on how many months of data are available. The Charge Adjustments on tab are not impacted by "Select: Include Misc Debit/Credit in Net Charges?" prompt.





McKESSON
Empowering Healthcare

0203 Management Summary

SAMPLE CLIENT

April 2017

Management Report Summary

I.	NET CHARGES BILLED FOR MONTH	2,602,072.81
II.	NET COLLECTIONS RECEIVED FOR MONTH	(2,096,749.63)
III.	NET COLLECTIONS PERCENTAGE	80.6%
IV.	ACCOUNTS RECEIVABLE * Includes In-House AR	20,440,494.93
V.	DAYS CHARGES CARRIED AS BILLED OPEN ACCOUNTS RECEIVABLE	111.4
VI.	PERCENTAGE OF ACCOUNTS RECEIVABLE OVER 90 DAYS	60.3%
VII.	TOTAL PROCEDURES PERFORMED	10,047
VIII.	AVERAGE GROSS CHARGE PER PROCEDURE	443.16
IX.	NUMBER OF PATIENTS	5,082
X.	AVERAGE GROSS CHARGES PER PATIENT	876.12

Management Report Detail and Analysis of Charges and Collections

	Current Month	Same Month Prior Year	12 Month Average
GROSS CHARGES	4,452,440.40	4,493,037.20	4,148,365.83
LESS: CURRENT UNBILLABLES	(5,473.56)	(9,962.16)	(8,316.40)
LESS: LIMIT OF ALLOWANCE	(1,844,894.03)	(2,436,430.91)	(1,529,968.64)
N E T C H A R G E S	**2,602,072.81**	**2,046,644.13**	**2,610,080.79**
GROSS COLLECTIONS	(2,115,488.98)	(2,698,873.10)	(1,742,951.43)
LESS: REFUNDS	18,354.79	16,595.47	31,358.08
LESS: RETURNED CHECKS	384.56	401.53	32.05
N E T C O L L E C T I O N S	**(2,096,749.63)**	**(2,681,876.10)**	**(1,711,561.31)**
NET COLLECTION PERCENTAGE	80.6%	131.0%	65.6%

Accounts Receivable

Analysis by Age

		Gross Charges	Current A/R	Variance	Percent of Change	Prior Month A/R
0-30	April	4,452,440.40	4,327,561.69	124,878.71	2.8%	4,570,407.33
31-60	March	5,405,490.20	2,165,237.21	3,240,252.99	59.9%	2,280,469.79
61-90	February	6,843,381.60	1,628,065.23	5,215,316.37	76.2%	1,691,152.08
91-120	January	3,825,708.00	1,326,101.75	2,499,606.25	65.3%	1,119,423.81
121-150	December	3,191,163.00	1,023,331.49	2,167,831.51	67.9%	1,077,459.32
151-180	November	4,177,716.40	925,810.07	3,251,906.33	77.8%	887,958.49
181-210	October	3,505,453.20	607,785.28	2,897,667.92	82.7%	551,100.81
OVER 210		N/A	8,436,602.21	N/A	N/A	8,301,415.50
TOTAL ACCOUNTS RECEIVABLE			**20,440,494.93**			**20,479,387.13**
CREDIT BALANCES			**(161,595.35)**			**(106,123.45)**
DAYS CARRIED AS OPEN A/R			**111.4**			**115.9**

Gross Charges / Gross Collections Analysis – Current and Year to Date
Financial Classification

Financial Class Group	Current Gross Charges	Current Gross Receipts	Current Active Net A/R	% Of Active A/R
AETNA	45,612.40	(25,772.21)	200,742.07	0.98%
AUTO INS	112,722.80	(82,100.50)	847,392.61	4.15%
BCBS	304,797.80	(196,857.20)	1,888,117.22	9.24%
CIGNA	28,059.80	(16,919.37)	133,498.19	0.65%
COMMERCIAL	154,970.40	(111,925.00)	1,200,630.12	5.87%
HMO MEDICARE	85,437.60	(54,428.86)	601,137.28	2.94%
HUMANA	76,805.20	(32,083.47)	228,585.77	1.12%
MEDICAID	392,590.40	(75,477.58)	1,600,862.7	7.83%
MEDICARE	1,712,853.60	(1,165,314.41)	3,621,826.8	17.72%
SELFPAY	1,056,406.60	(16,465.34)	6,066,833.17	29.68%
TRICARE/CHAMPUS	118,705.60	(119,710.79)	1,819,031.62	8.90%
UNITED HEALTHCARE	349,753.00	(203,046.24)	2,068,385.9	10.12%
WORKERS COMP	13,725.20	(15,388.01)	163,451.48	0.80%
MTD TOTAL	**4,452,440.40**	**(2,115,488.98)**	**20,440,494.93**	100.0%

Financial Class Group	FYTD Gross Charges	% of Total	FYTD Gross Receipts	% of Total
AETNA	388,503.60	1.2%	(186,207.61)	1.5%
AUTO INS	894,804.80	2.8%	(476,712.05)	3.9%
BCBS	2,602,853.80	8.3%	(1,327,042.58)	10.8%
CIGNA	235,826.80	0.8%	(146,693.84)	1.2%
COMMERCIAL	1,552,475.00	4.9%	(828,137.43)	6.7%
HMO MEDICARE	735,080.40	2.3%	(318,196.24)	2.6%
HUMANA	462,789.00	1.5%	(161,452.09)	1.3%
MEDICAID	2,942,631.60	9.4%	(517,307.81)	4.2%
MEDICARE	13,342,228.60	42.5%	(6,386,506.39)	51.9%
SELFPAY	4,681,049.00	14.9%	(95,897.74)	0.8%
TRICARE/CHAMPUS	917,337.40	2.9%	(718,220.69)	5.8%
UNITED HEALTHCARE	2,531,890.20	8.1%	(1,052,547.88)	8.6%
WORKERS COMP	113,882.60	0.4%	(92,202.26)	0.7%
FYTD TOTAL	**31,401,352.80**		**(12,307,124.61)**	

Sites Report
Gross Charges / Gross Collections Analysis - Current Month

Location	Current Gross Charges	% of Total	Current Gross Collections	% of Total	Percent Received
[redacted]	8,554.00	0.2%	(5,418.90)	0.3%	63.3%
[redacted]	1,114,959.80	25.0%	(598,611.92)	28.3%	53.7%
[redacted]	0.00	0.0%	(522.30)	0.0%	0.0%
[redacted]	14,084.80	0.3%	(5,665.16)	0.3%	40.2%
[redacted]	2,057.80	0.0%	(1,150.02)	0.1%	55.9%
[redacted]	1,015,471.00	22.8%	(487,822.15)	23.1%	48.0%
[redacted]	792,631.20	17.8%	(370,392.92)	17.5%	46.7%
[redacted]	0.00	0.0%	0.00	0.0%	0.0%
[redacted]E	0.00	0.0%	0.00	0.0%	0.0%
[redacted]	0.00	0.0%	(587.49)	0.0%	0.0%
[redacted]	1,052,703.20	23.6%	(401,511.35)	19.0%	38.1%
[redacted]	25,168.00	0.6%	(7,325.81)	0.3%	29.1%
[redacted]	29,987.20	0.7%	(13,640.13)	0.6%	45.5%
[redacted]	9,413.20	0.2%	(7,622.18)	0.4%	81.0%
[redacted]	270,251.00	6.1%	(130,581.15)	6.2%	48.3%
[redacted]	17,250.00	0.4%	(8,875.64)	0.4%	51.5%
[redacted]	980.60	0.0%	0.00	0.0%	0.0%
[redacted]	91,558.20	2.1%	(71,739.84)	3.4%	78.4%
[redacted]	5,895.40	0.1%	(4,022.02)	0.2%	68.2%
[redacted]	0.00	0.0%	0.00	0.0%	0.0%
[redacted]	0.00	0.0%	0.00	0.0%	0.0%
[redacted]	1,475.00	0.0%	0.00	0.0%	0.0%
	4,452,440.40	**100.0%**	**(2,115,488.98)**	**100.0%**	**47.5%**
TOTAL	**4,452,440.40**		**(2,115,488.98)**		

Sites Report
Gross Charges / Gross Collections Analysis - Year to Date

Location	Fiscal Year to Date Gross Charges	% of Total	Fiscal Year to Date Gross Collections	% of Total	Percent Received
[redacted]	71,832.20	0.2%	(35,361.45)	0.3%	49.2%
[redacted]	7,899,979.80	25.2%	(3,293,327.88)	26.8%	41.7%
[redacted]	2,808.60	0.0%	(712.30)	0.0%	25.4%
[redacted]	76,345.60	0.2%	(30,546.91)	0.2%	40.0%
[redacted]	22,592.40	0.1%	(13,961.17)	0.1%	61.8%
[redacted]	6,791,229.40	21.6%	(2,962,673.93)	24.1%	43.6%
[redacted]	0.00	0.0%	0.00	0.0%	0.0%
[redacted]	90,094.40	0.3%	(22,535.05)	0.2%	25.0%
[redacted]	5,684,454.80	18.1%	(2,151,034.99)	17.5%	37.8%
[redacted]	0.00	0.0%	(7,842.11)	0.1%	0.0%
[redacted]	170,135.80	0.5%	(36,303.02)	0.3%	21.3%
[redacted]	7,557,494.80	24.1%	(2,642,997.76)	21.5%	35.0%
[redacted]	5,702.40	0.0%	(2,661.74)	0.0%	46.7%
[redacted]	1,965,653.20	6.3%	(732,567.47)	6.0%	37.3%
[redacted]	222,191.00	0.7%	(81,794.81)	0.7%	36.8%
[redacted]	129,909.80	0.4%	(50,572.01)	0.4%	38.9%
[redacted]	4,160.60	0.0%	(1,846.56)	0.0%	44.4%
[redacted]	672,513.40	2.1%	(225,344.10)	1.8%	33.5%
[redacted]	0.00	0.0%	0.00	0.0%	0.0%
[redacted]	0.00	0.0%	(142.15)	0.0%	0.0%
[redacted]	29,074.60	0.1%	(13,592.25)	0.1%	46.7%
[redacted]	5,180.00	0.0%	(1,306.95)	0.0%	25.2%
	31,401,352.80	**100.0%**	**(12,307,124.61)**	**100.0%**	**39.2%**
TOTAL	**31,401,352.80**		**(12,307,124.61)**		

Procedure Report

Average Charge Per Procedure

Description	Month Count	Current Total Amount	Current Average Charge	FYTD Count	FYTD Total Amount	FYTD Average Charge
ALS1	3,434	3,004,750.00	875.00	20,294	17,757,250.00	875.00
ALS2	56	49,000.00	875.00	572	500,500.00	875.00
BLS	1,475	958,750.00	650.00	15,187	9,871,550.00	650.00
BLS NON EMERGENCY	0	0.00	0.00	7	4,550.00	650.00
MILEAGE ALS	3,491	308,191.20	88.28	20,877	1,941,922.80	93.02
MILEAGE BLS	1,474	114,199.20	77.48	15,182	1,196,430.00	78.81
TREAT-NO TRANSPORT	117	17,550.00	150.00	861	129,150.00	150.00
TOTAL	**10,047**	**4,452,440.40**	**443.16**	**72,980**	**31,401,352.80**	**430.27**
PATIENT COUNT	**5,082**	**4,452,440.40**	**876.12**	**36,915**	**31,401,352.80**	**850.64**
PROCEDURES/PATIENT		**1.98**		**1.98**		

Accounts Receivable Reconciliation

	MTD Amount	FYTD Amount
BEGINNING ACCOUNTS RECEIVABLE	**20,479,387.13**	**16,751,803.38**
PLUS: GROSS CHARGES	4,452,440.40	31,401,352.80
LESS: GROSS COLLECTIONS	(2,115,488.98)	(12,307,124.61)
LESS: TOTAL ADJUSTMENTS		
1. LIMIT OF ALLOWANCE	(1,844,894.03)	(10,879,649.98)
2. REFUNDS	18,354.79	217,699.99
3. RETURNED CHECKS	384.56	384.56
5. UNBILLABLES	(5,473.56)	(48,440.91)
6. BAD DEBT WRITE-OFFS	(547,186.15)	(4,714,937.24)
7. BAD DEBT RECOVERY	2,970.77	19,406.94
8. MISC DEBITS	0.00	0.00
9. MISC CREDITS	0.00	0.00
ENDING ACCOUNTS RECEIVABLE	**20,440,494.93**	**20,440,494.93**

Financial Adjustment Activity

Unbillables

UNBILLABLES	MTD BALANCE	FYTD BALANCE
ADMINISTRATIVE ADJUSTMENT	(1,775.56)	(11,370.31)
CR TRANSFER ADJUSTMENT	(4,904.64)	(37,085.03)
DATA ENTRY ERROR	(3,560.60)	(29,494.40)
DB TRANSFER ADJUSTMENT	4,904.64	35,853.35
NON TRANSPORT	(203.55)	(1,684.00)
REVERSE ADMINISTRATIVE ADJT	0.00	263.75
REVERSE INTEREST DEBIT ADJT	66.15	651.53
W/O DUPLICATE CHARGE	0.00	(5,575.80)
TOTAL	**(5,473.56)**	**(48,440.91)**

Limit Of Allowance - Current Month and Year to Date

LIMIT OF ALLOWANCE CURRENT MONTH	CURRENT PROCESSED	CURRENT PAYMENTS	CURRENT LOA	CURRENT %
AETNA	(50,622.47)	(25,772.21)	(24,850.26)	49.1%
AUTO INS	(98,165.24)	(82,100.50)	(16,064.74)	16.4%
BCBS	(286,890.94)	(196,857.20)	(90,033.74)	31.4%
CIGNA	(23,776.26)	(16,919.37)	(6,856.89)	28.8%
COMMERCIAL	(165,764.35)	(111,925.00)	(53,839.35)	32.5%
HMO MEDICARE	(107,039.98)	(54,428.86)	(52,611.12)	49.2%
HUMANA	(66,394.69)	(32,083.47)	(34,311.22)	51.7%
MEDICAID	(382,286.68)	(75,477.58)	(306,809.10)	80.3%
MEDICARE	(2,213,112.58)	(1,165,314.41)	(1,047,798.17)	47.3%
SELFPAY	(16,465.34)	(16,465.34)	0.00	0.0%
TRICARE/CHAMPUS	(130,397.83)	(119,710.79)	(10,687.04)	8.2%
UNITED HEALTHCARE	(401,403.85)	(203,046.24)	(198,357.61)	49.4%
WORKERS COMP	(18,062.80)	(15,388.01)	(2,674.79)	14.8%
TOTAL	**(3,960,383.01)**	**(2,115,488.98)**	**(1,844,894.03)**	**46.6%**

LIMIT OF ALLOWANCE YEAR TO DATE	FYTD PROCESSED	FYTD PAYMENTS	FYTD LOA	FYTD %
AETNA	(310,743.17)	(186,207.61)	(124,535.56)	40.1%
AUTO INS	(559,230.28)	(476,712.05)	(82,518.23)	14.8%
BCBS	(1,908,629.66)	(1,327,042.58)	(581,587.08)	30.5%
CIGNA	(189,424.41)	(146,693.84)	(42,730.57)	22.6%
COMMERCIAL	(1,271,007.26)	(828,137.43)	(442,869.83)	34.8%
HMO MEDICARE	(641,088.78)	(318,196.24)	(322,892.54)	50.4%
HUMANA	(345,471.69)	(161,452.09)	(184,019.60)	53.3%
MEDICAID	(2,586,258.25)	(517,307.81)	(2,068,950.44)	80.0%
MEDICARE	(12,407,329.35)	(6,386,506.39)	(6,020,822.96)	48.5%
SELFPAY	(95,765.74)	(95,897.74)	132.00	(0.1%)
TRICARE/CHAMPUS	(780,207.88)	(718,220.69)	(61,987.19)	7.9%
UNITED HEALTHCARE	(1,988,385.04)	(1,052,547.88)	(935,837.16)	47.1%
WORKERS COMP	(103,233.08)	(92,202.26)	(11,030.82)	10.7%
TOTAL	**(23,186,774.59)**	**(12,307,124.61)**	**(10,879,649.98)**	**46.9%**

Financial Adjustment Activity

REFUNDS	MTD BALANCE	FYTD BALANCE
REFUND TO PATIENT	5,813.39	77,405.08
REFUND TO INSURANCE COMPANY	10,195.33	38,020.95
REFUND TO FREE FORM	2,346.07	100,552.15
REFUND TO RESPONSIBLE PARTY	0.00	1,721.81
TOTAL	**18,354.79**	**217,699.99**

RETURN CHECKS	MTD BALANCE	FYTD BALANCE
RETURNED CHECK DEBIT	384.56	384.56
TOTAL	**384.56**	**384.56**
TOTAL - NET REFUNDS	**18,739.35**	**218,084.55**

BAD DEBT WRITE OFF	MTD BALANCE	FYTD BALANCE
BANKRUPTCY WRITE-OFF	(205.00)	(7,945.60)
DECEASED WRITE-OFF	(175.00)	(185,902.15)
CHARITY/INDIGENT W/O	0.00	(3,069.18)
SMALL BALANCE WRITEOFF - CREDIT	(46.16)	(272.50)
BAD ADDRESS WRITEOFF - CREDIT	0.00	(650.00)
COLLECTOR WRITEOFF - CREDIT	(546,759.99)	(4,517,097.81)
TOTAL	**(547,186.15)**	**(4,714,937.24)**

BAD DEBT RECOVERY	MTD BALANCE	FYTD BALANCE
REVERSE DECEASED WRITE-OFF	0.00	1,660.16
COLL W/O PMTS	2,677.62	2,677.62
SMALL BALANCE WRITEOFF - DEBIT	5.55	569.89
COLLECTOR WRITEOFF - DEBIT	287.60	14,499.27
TOTAL	**2,970.77**	**19,406.94**

Financial Adjustment Activity

TOTAL - NET BAD DEBT	**(544,215.38)**	**(4,695,530.30)**
NET BAD DEBT PERCENT OF GROSS CHARGES	**(12.2%)**	**(15.0%)**

List of Unbillable, LOA, and Adjustment Codes Used in Report

Transaction Code	Description	SKEY	Amount
7300	SMALL BALANCE WRITEOFF - CREDIT		(46.16)
		005 - TOTAL	**(46.16)**
9300	SMALL BALANCE WRITEOFF - DEBIT		5.55
		008 - TOTAL	**5.55**
0123	REVERSE INTEREST DEBIT ADJT		66.15
0146	DATA ENTRY ERROR		(3,560.60)
0155	CR TRANSFER ADJUSTMENT		(4,904.64)
0156	DB TRANSFER ADJUSTMENT		4,904.64
0187	ADMINISTRATIVE ADJUSTMENT		(1,775.56)
0188	NON TRANSPORT		(203.55)
		970 - TOTAL	**(5,473.56)**
0164	BANKRUPTCY WRITE-OFF		(205.00)
0169	DECEASED WRITE-OFF		(175.00)
7700	COLLECTOR WRITEOFF - CREDIT		(546,759.99)
		975 - TOTAL	**(547,139.99)**
0150	RETURNED CHECK DEBIT		384.56
		976 - TOTAL	**384.56**
0170	REFUND TO PATIENT		5,813.39
0171	REFUND TO INSURANCE COMPANY		10,195.33
0172	REFUND TO FREE FORM		2,346.07
		977 - TOTAL	**18,354.79**
7144	COLL W/O PMTS		2,677.62
9700	COLLECTOR WRITEOFF - DEBIT		287.60
		978 - TOTAL	**2,965.22**

List of Unbillable, LOA, and Adjustment Codes Used in Report

Transaction Code	Description	SKEY	Amount
0398	REVERSE BLUE SHIELD LOA		0.00
0399	BLUE SHIELD LOA		(85,744.40)
1198	REVERSE MEDICARE LOA		5,031.58
1199	MEDICARE LOA		(1,060,316.06)
1598	REVERSE MEDICAID LOA		2,943.13
1599	MEDICAID LOA		(51,781.03)
2299	CHAMPUS LOA		(2,866.32)
4096	HMO/OTHER CONTRACTUAL W/O		(2,417.62)
4098	LOA DEBIT ADJUSTMENT		236.22
4099	LIMIT OF ALLOWANCE WRITEOFF		(100,833.89)
4198	HMO/PPO DEBIT ADJUSTMENT		270.56
4199	LIMIT OF ALLOWANCE WRITEOFF		(11,184.95)
5099	WORKMANS COMP LOA		(2,674.79)
9198	LIMIT OF ALLOWANCE DEBIT		4,629.78
9199	LIMIT OF ALLOWANCE WRITEOFF		(278,641.84)
9498	LIMIT OF ALLOWANCE DEBIT		2,788.00
9499	LIMIT OF ALLOWANCE WRITEOFF		(264,332.40)
		979 - TOTAL	**(1,844,894.03)**

[redacted] County EMS - Monthly Financial Summary

April 2017

Client ID(s) Selected: [redacted]

[redacted] County Emergency Medical Services
Schedule of Transports and Collections by Date of Service

Reporting Period: April 2017

Year-Month	Transports	Gross Charges	Contractual Adjustments	Net Charges	Net Collections	Writeoffs	Refunds	Balance	Gross Charge/Trip	Net Charge/ Trip	Net Coll/ Trip	Net Coll %
2016-10	6,157	$4,146,255.06	$1,096,852.77	$3,049,402.29	$1,554,405.63	$765,768.22	($17,124.79)	$729,228.44	$673.42	$495.27	$252.46	51.0%
2016-11	5,718	$3,898,404.45	$1,056,885.13	$2,841,519.32	$1,465,245.01	$177,586.83	($11,826.95)	$1,198,687.48	$681.78	$496.94	$256.25	51.6%
2016-12	6,088	$4,148,458.16	$1,036,195.64	$3,112,262.52	$1,521,877.57	$107,335.47	($10,863.89)	$1,483,049.48	$681.42	$511.21	$249.98	48.9%
2017-01	6,248	$4,275,258.61	$1,041,107.94	$3,234,150.67	$1,416,887.03	$68,443.86	($5,508.94)	$1,748,078.98	$684.26	$517.63	$226.77	43.8%
2017-02	5,883	$4,034,242.53	$947,247.33	$3,086,995.20	$1,218,455.47	$25,166.11	($3,060.67)	$1,843,031.60	$685.75	$524.73	$207.11	39.5%
2017-03	6,594	$4,525,258.00	$884,466.87	$3,640,791.13	$1,028,855.45	$11,841.17	$0.00	$2,601,177.33	$686.27	$552.14	$156.03	28.3%
2017-04	3,898	$2,683,220.30	$182,096.50	$2,501,123.80	$116,333.16	$200.00	$0.00	$2,384,590.64	$688.36	$641.64	$29.84	4.7%
	40,586	**$27,711,097.11**	**$6,244,852.18**	**$21,466,244.93**	**$8,322,059.32**	**$1,156,341.66**	**($48,385.24)**	**$11,987,843.95**	**$682.77**	**$528.91**	**$205.05**	**38.8%**

April 2017

[redacted] County Emergency Medical Services
Schedule of Transports and Collections by Date of Service

Reporting Period: April 2017

Year-Month	Transports	Gross Charges	Contractual Adjustments	Net Charges	Net Collections	Writeoffs	Refunds	Balance	Gross Charge/Trip	Net Charge/Trip	Net Coll/Trip	Net Coll %
2016-10	2,491	$1,691,598.25	$552,154.62	$1,139,443.63	$896,132.82	$20,489.46	($7,310.39)	$222,821.35	$679.08	$457.42	$359.75	78.6%
2016-11	2,350	$1,621,720.11	$529,684.84	$1,092,035.27	$861,054.66	$8,311.84	($8,434.46)	$222,668.77	$690.09	$464.70	$366.41	78.8%
2016-12	2,659	$1,827,756.04	$561,996.02	$1,265,760.02	$943,612.10	$3,668.41	($7,746.09)	$318,479.51	$687.38	$476.03	$354.87	74.5%
2017-01	2,792	$1,923,474.70	$559,544.81	$1,363,929.89	$901,724.62	$3,753.34	($4,521.34)	$458,451.93	$688.92	$488.51	$322.97	66.1%
2017-02	2,620	$1,807,720.62	$496,008.84	$1,311,711.78	$802,107.16	$2,260.67	($1,329.56)	$506,261.13	$689.97	$500.65	$306.15	61.1%
2017-03	2,793	$1,932,281.03	$455,720.46	$1,476,560.57	$698,371.17	$565.00	$0.00	$778,707.22	$691.83	$528.66	$250.04	47.3%
2017-04	1,937	$1,343,272.74	$36,883.67	$1,306,389.07	$40,809.75	$0.00	$0.00	$1,265,579.32	$693.48	$674.44	$21.07	3.1%
	17,642	**$12,147,823.49**	**$3,191,993.26**	**$8,955,830.23**	**$5,143,812.28**	**$39,048.72**	**($29,341.84)**	**$3,772,969.23**	**$688.57**	**$507.64**	**$291.57**	**57.4%**

April 2017

[redacted] County Emergency Medical Services
Schedule of Transports and Collections by Date of Service

Reporting Period: April 2017

Year-Month	Transports	Gross Charges	Contractual Adjustments	Net Charges	Net Collections	Writeoffs	Refunds	Balance	Gross Charge/Trip	Net Charge/ Trip	Net Coll/ Trip	Net Coll %
2016-10	786	$518,294.47	$354,801.39	$163,493.08	$89,229.76	$2,720.87	$0.00	$71,542.45	$659.41	$208.01	$113.52	54.6%
2016-11	860	$574,235.24	$365,112.82	$209,122.42	$91,255.19	$0.00	$0.00	$117,867.23	$667.72	$243.17	$106.11	43.6%
2016-12	719	$477,935.54	$325,752.20	$152,183.34	$81,145.12	$0.00	$0.00	$71,038.22	$664.72	$211.66	$112.86	53.3%
2017-01	772	$513,771.44	$341,413.10	$172,358.34	$82,232.38	$557.27	$0.00	$89,568.69	$665.51	$223.26	$106.52	47.7%
2017-02	739	$496,484.04	$319,357.14	$177,126.90	$78,225.73	$0.00	$0.00	$98,901.17	$671.83	$239.68	$105.85	44.2%
2017-03	847	$564,686.70	$317,178.66	$247,508.04	$75,643.76	$0.00	$0.00	$171,864.28	$666.69	$292.22	$89.31	30.6%
2017-04	587	$388,902.89	$118,222.05	$270,680.84	$27,796.02	$0.00	$0.00	$242,884.82	$662.53	$461.13	$47.35	10.3%
	5,310	**$3,534,310.32**	**$2,141,837.36**	**$1,392,472.96**	**$525,527.96**	**$3,278.14**	**$0.00**	**$863,666.86**	**$665.60**	**$262.24**	**$98.97**	**37.7%**

April 2017

[redacted]County Emergency Medical Services
Schedule of Transports and Collections by Date of Service

Reporting Period: April 2017

Year-Month	Transports	Gross Charges	Contractual Adjustments	Net Charges	Net Collections	Writeoffs	Refunds	Balance	Gross Charge/Trip	Net Charge/ Trip	Net Coll/ Trip	Net Coll %
2016-10	1,402	$952,217.17	$155,513.61	$796,703.56	$539,262.91	$41,974.88	($9,814.40)	$215,465.77	$679.18	$568.26	$384.64	67.7%
2016-11	1,335	$918,646.14	$140,915.68	$777,730.46	$493,883.39	$16,227.00	($3,392.49)	$267,620.07	$688.12	$582.57	$369.95	63.5%
2016-12	1,419	$973,667.89	$135,482.72	$838,185.17	$478,996.83	$4,641.28	($3,117.80)	$354,547.06	$686.16	$590.69	$337.56	57.1%
2017-01	1,521	$1,056,945.21	$140,150.03	$916,795.18	$426,301.54	$3,223.01	($987.60)	$486,529.83	$694.90	$602.76	$280.28	46.5%
2017-02	1,287	$897,118.32	$131,881.35	$765,236.97	$333,236.69	$2,667.27	($1,731.11)	$430,073.81	$697.06	$594.59	$258.93	43.5%
2017-03	1,408	$983,655.34	$111,567.75	$872,087.59	$254,790.52	$5,006.05	$0.00	$612,291.02	$698.62	$619.38	$180.96	29.2%
2017-04	891	$620,361.75	$26,990.78	$593,370.97	$47,727.39	$0.00	$0.00	$545,643.58	$696.25	$665.96	$53.57	8.0%
	9,263	**$6,402,611.82**	**$842,501.92**	**$5,560,109.90**	**$2,574,199.27**	**$73,739.49**	**($19,043.40)**	**$2,912,171.14**	**$691.20**	**$600.25**	**$277.90**	**46.3%**

April 2017

[redacted] County Emergency Medical Services
Schedule of Transports and Collections by Date of Service

Reporting Period: April 2017

Year-Month	Transports	Gross Charges	Contractual Adjustments	Net Charges	Net Collections	Writeoffs	Refunds	Balance	Gross Charge/Trip	Net Charge/ Trip	Net Coll/ Trip	Net Coll %
0001-01		$0.00	$0.00	$0.00	$8,134.67	($74.31)	($265.00)	($8,060.36)				0.0%
2016-09		$0.00	$0.00	$0.00	$0.00	$0.00	$0.00					0.0%
2016-10	1,478	$984,145.17	$34,383.15	$949,762.02	$29,780.14	$700,583.01	$0.00	$219,398.87	$665.86	$642.60	$20.15	3.1%
2016-11	1,173	$783,802.96	$21,171.79	$762,631.17	$19,051.77	$153,047.99	$0.00	$590,531.41	$668.20	$650.15	$16.24	2.5%
2016-12	1,291	$869,098.69	$12,964.70	$856,133.99	$18,123.52	$99,025.78	$0.00	$738,984.69	$673.20	$663.16	$14.04	2.1%
2017-01	1,163	$781,067.26	$0.00	$781,067.26	$6,628.49	$60,910.24	$0.00	$713,528.53	$671.60	$671.60	$5.70	0.8%
2017-02	1,237	$832,919.55	$0.00	$832,919.55	$4,885.89	$20,238.17	$0.00	$807,795.49	$673.34	$673.34	$3.95	0.6%
2017-03	1,546	$1,044,634.93	$0.00	$1,044,634.93	$50.00	$6,270.12	$0.00	$1,038,314.81	$675.70	$675.70	$0.03	0.0%
2017-04	483	$330,682.92	$0.00	$330,682.92	$0.00	$200.00	$0.00	$330,482.92	$684.64	$684.64	$0.00	0.0%
	8,371	**$5,626,351.48**	**$68,519.64**	**$5,557,831.84**	**$86,654.48**	**$1,040,201.00**	**($265.00)**	**$4,430,976.36**	**$672.12**	**$663.94**	**$10.35**	**1.6%**

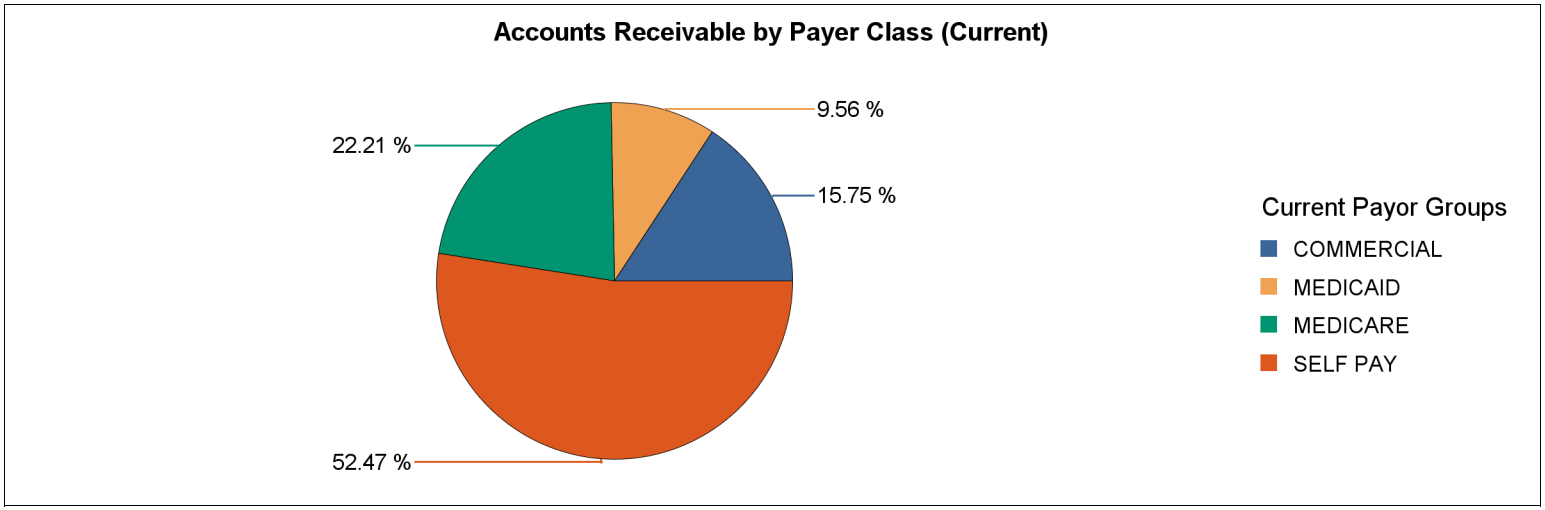
[redacted]County Emergency Medical Services
Accounts Receivable Aging by Current Payor

Reporting Period: April 2017

Payor Class	Current	30 Days	60 Days	90 Days	120 Days	150 Days	180 Days	210 Days	AR
COMMERCIAL	$519,149	$416,517	$276,610	$278,915	$178,266	$116,173	$106,998	($5,446)	**$1,887,183**
MEDICAID	$256,912	$204,120	$151,317	$138,771	$116,663	$154,025	$120,481	$3,284	**$1,145,573**
MEDICARE	$1,275,558	$548,304	$335,885	$198,615	$133,397	$88,827	$79,185	$1,003	**$2,660,775**
SELF PAY	$451,146	$1,314,063	$1,185,870	$1,080,168	$999,681	$839,663	$406,081	$9,581	**$6,286,253**
	$2,502,765	**$2,483,003**	**$1,949,682**	**$1,696,470**	**$1,428,008**	**$1,198,687**	**$712,746**	**$8,422**	**$11,979,784**

Accounts Receivable Aging Balance %

Payor Class	Current	30 Days	60 Days	90 Days	120 Days	150 Days	180 Days	210 Days	% of Total AR
COMMERCIAL	**20.7%**	**16.8%**	**14.2%**	**16.4%**	**12.5%**	**9.7%**	**15.0%**	**-64.7%**	**15.8%**
MEDICAID	**10.3%**	**8.2%**	**7.8%**	**8.2%**	**8.2%**	**12.8%**	**16.9%**	**39.0%**	**9.6%**
MEDICARE	**51.0%**	**22.1%**	**17.2%**	**11.7%**	**9.3%**	**7.4%**	**11.1%**	**11.9%**	**22.2%**
SELF PAY	**18.0%**	**52.9%**	**60.8%**	**63.7%**	**70.0%**	**70.0%**	**57.0%**	**113.8%**	**52.5%**



April 2017

	Oct-16	Nov-16	Dec-16	Jan-17	Feb-17	Mar-17	Apr-17
Management Summary							
Billing Activity	$2,061,916	$4,795,304	$3,412,397	$4,609,344	$4,093,062	$4,575,459	$4,163,616
Net Collections	$200	$328,164	$1,727,655	$1,059,702	$1,603,522	$2,341,039	$1,269,911
Write Offs	$0	$0	$0	$2,687	$22,053	$213,286	$918,241
Adjustments	$0	$153,075	$918,888	$518,376	$847,491	$2,865,387	$892,985
AR Ending Balance	$2,061,716	$6,375,780	$7,141,304	$10,163,157	$11,772,585	$10,912,958	$11,979,784
Transport Activity							
Total Transports	3,036	7,083	5,003	6,748	5,949	6,662	6,105
BLS	28.7%	32.9%	34.2%	33.0%	30.0%	31.7%	31.6%
ALS	69.2%	64.5%	62.7%	64.1%	67.9%	65.8%	66.1%
ALS2	2.1%	2.6%	3.1%	2.9%	2.1%	2.5%	2.3%
Avg Charge / Transport	$679.16	$677.02	$682.07	$683.07	$688.03	$686.80	$682.00
Collection Activity							
Medicaid	$0	$0	$953	$0	$1,893	$449,812	$72,870
Medicare	$200	$123,639	$1,262,232	$643,274	$1,076,291	$1,299,557	$738,619
Private Insurance	$0	$203,694	$458,733	$403,443	$503,971	$571,728	$432,631
Self Pay	$0	$831	$5,737	$12,986	$21,367	$19,943	$25,791
Medicaid	0.0%	0.0%	0.1%	0.0%	0.1%	19.2%	5.7%
Medicare	100.0%	37.7%	73.1%	60.7%	67.1%	55.5%	58.2%
Private Insurance	0.0%	62.1%	26.6%	37.9%	31.0%	24.0%	33.2%
Self Pay	0.0%	0.3%	0.3%	1.2%	1.3%	0.9%	2.0%
Accounts Receivable - Aging							
Current	$2,060,382	$2,832,868	$2,040,252	$2,631,361	$2,583,763	$2,303,635	$2,502,765
30 Days	$687	$3,542,912	$2,595,440	$2,873,565	$2,722,291	$2,213,083	$2,483,003
60 Days	$646	$0	$2,444,738	$2,233,226	$2,244,780	$1,885,538	$1,949,682
90 Days	$0	$0	$60,873	$2,300,490	$2,100,535	$1,659,042	$1,688,435
120 Days	$0	$0	$0	$124,390	$2,121,042	$1,433,977	$1,428,008
150 Days	$0	$0	$0	$0	$0	$1,396,785	$1,198,687
180 Days	$0	$0	$0	$0	$0	$20,924	$712,746
210 Days	$0	$0	$0	$126	$175	($25)	$16,458
Collection Adjustments							
Refunds	$0.00	$0.00	$0.00	$4,460.26	$9,122.69	$8,478.16	$8,473.49
Recoups	$0.00	$0.00	$330.30	$2,265.50	$1,444.65	$6,895.34	$7,179.85
Total	$0.00	$0.00	$330.30	$6,725.76	$10,567.34	$15,373.50	$15,653.34

[redacted] County Emergency Medical Services
Billing Activity Summary Report

Reporting Period: April 2017

		Current Month			Fiscal YTD		
Financial Class		**Count**	**Charges**		**Count**	**Charges**	
Commercial		1,324	$912,282.91	21.8%	9,425	$6,402,611.82	23.1%
Medicaid		874	$576,282.08	13.8%	5,401	$3,534,310.32	12.8%
Medicare		2,636	$1,818,767.81	43.4%	17,842	$12,147,823.49	43.8%
Self Pay		1,343	$881,588.29	21.0%	8,719	$5,626,351.48	20.3%
TOTAL BILLABLE		**6,177**	**$4,188,921.09**		**41,387**	**$27,711,097.11**	
Billable Transports							
Emergency	ALS1	4,027	$2,480,226.23	68.8%	26,579	$16,290,925.27	68.2%
	Assessment	*359*	*$220,771.93*		*3,224*	*$1,975,650.94*	
	ALS2	141	$126,397.04	3.5%	1,032	$915,148.23	3.8%
	BLS	1,746	$988,126.12	27.4%	12,784	$6,597,477.76	27.6%
	RME	22	$11,765.81	0.3%	191	$99,953.09	0.4%
	Mileage	*51,921*	*$568,005.89*		*337,494*	*$3,647,392.76*	
		6,105	**$4,174,521.09**		**40,586**	**$27,550,897.11**	

[redacted] County Emergency Medical Services
Collection Report Summary - By Financial Class

Reporting Period: April 2017

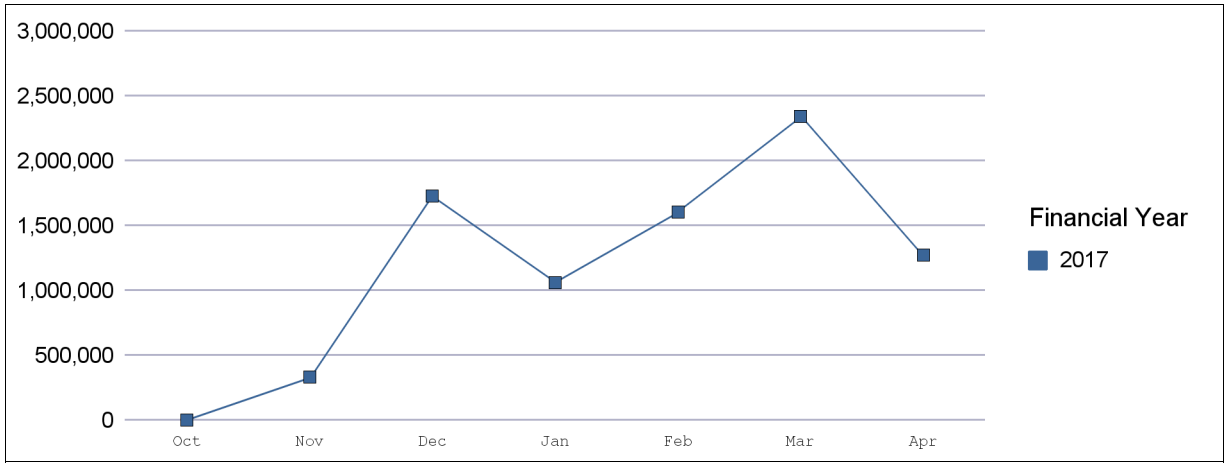
Primary Payor	Current Month		Fiscal YTD	
Commercial	$432,631.22	34.1%	$2,574,199.27	30.9%
Medicaid	$72,869.98	5.7%	$525,527.96	6.3%
Medicare	$738,618.84	58.2%	$5,143,812.28	45.4%
Self Pay	$25,790.80	2.0%	$86,654.48	1.0%
[redacted]	[redacted]		[redacted]	
Net Collections	**$1,269,910.84**		**$8,330,193.99**	
Unidentified Payments	$8,022.32		$8,134.67	
Total	$1,270,884.84		$9,528,501.59	

April 2017

[redacted]County Emergency Medical Services
Fiscal Year Revenue Summary by Posting Date

Reporting Period: April 2017

Financial Year	Oct	Nov	Dec	Jan	Feb	Mar	Apr
2017	$200	$328,164	$1,727,655	$1,059,702	$1,603,522	$2,341,039	$1,269,911

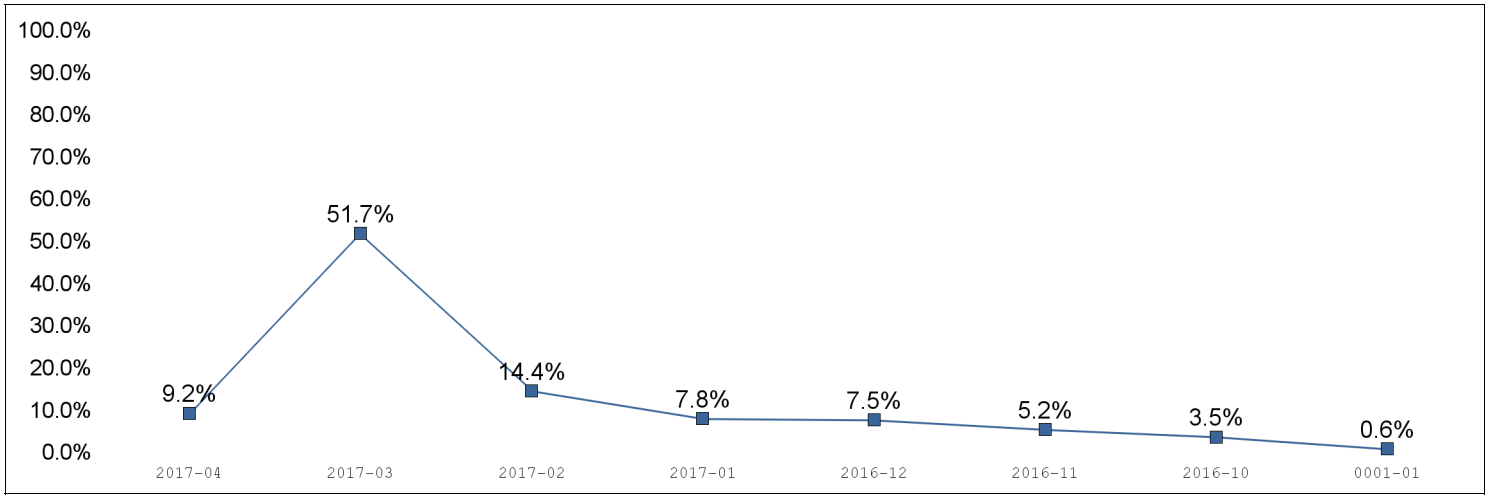


April 2017

[redacted] County Emergency Medical Services
Collections by Transport Month

Reporting Period: April 2017

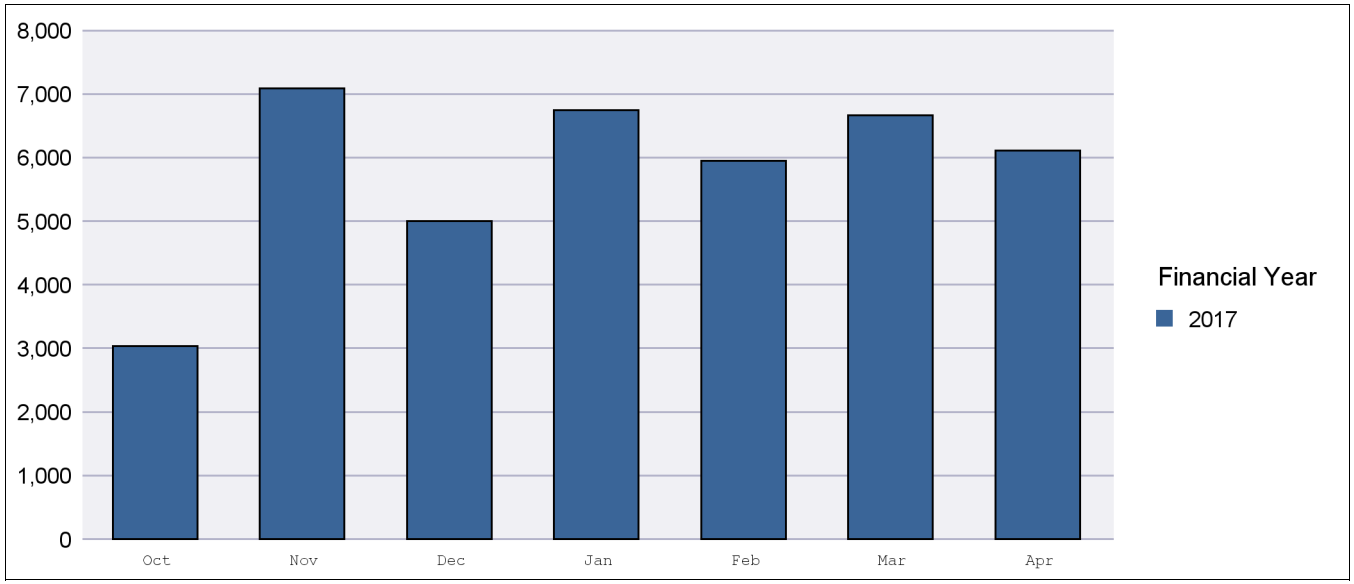
MOS	Net Collections	%
2017-04	$116,333.16	9.2%
2017-03	$656,666.67	51.7%
2017-02	$183,163.07	14.4%
2017-01	$99,390.46	7.8%
2016-12	$95,336.84	7.5%
2016-11	$66,593.40	5.2%
2016-10	$44,404.92	3.5%
0001-01	$8,022.32	0.6%
	$1,269,910.84	



[redacted]County Emergency Medical Services
Transport Historical Comparison by AcctPer

Reporting Period: April 2017

Financial Year	Oct	Nov	Dec	Jan	Feb	Mar	Apr	Total
2017	3,036	7,083	5,003	6,748	5,949	6,662	6,105	40,586



April 2017

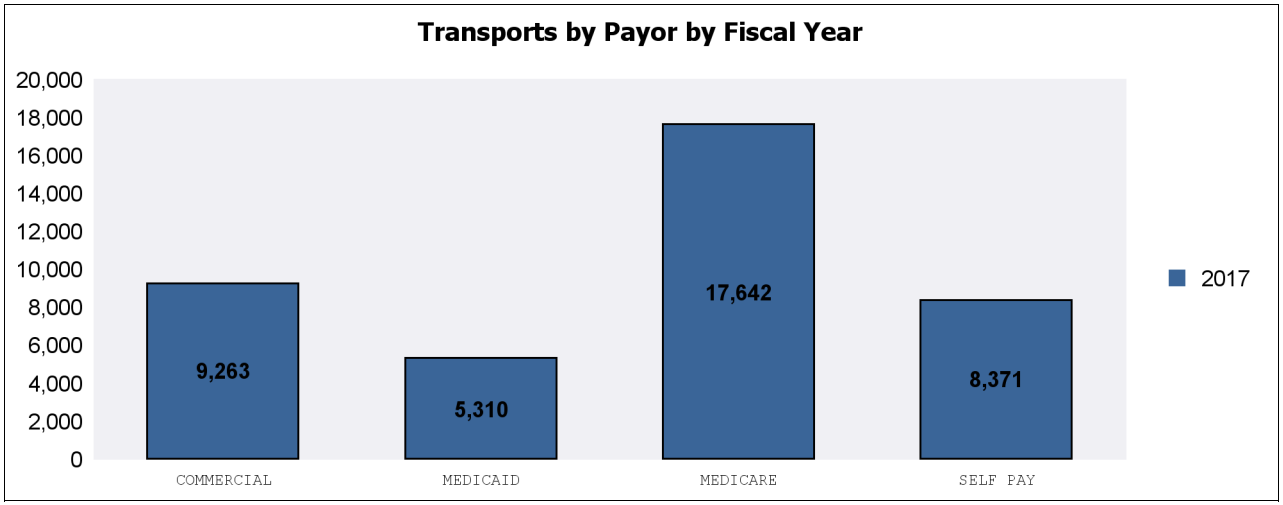
[redacted] County Emergency Medical Services
Transport Historical Level of Service Comparison

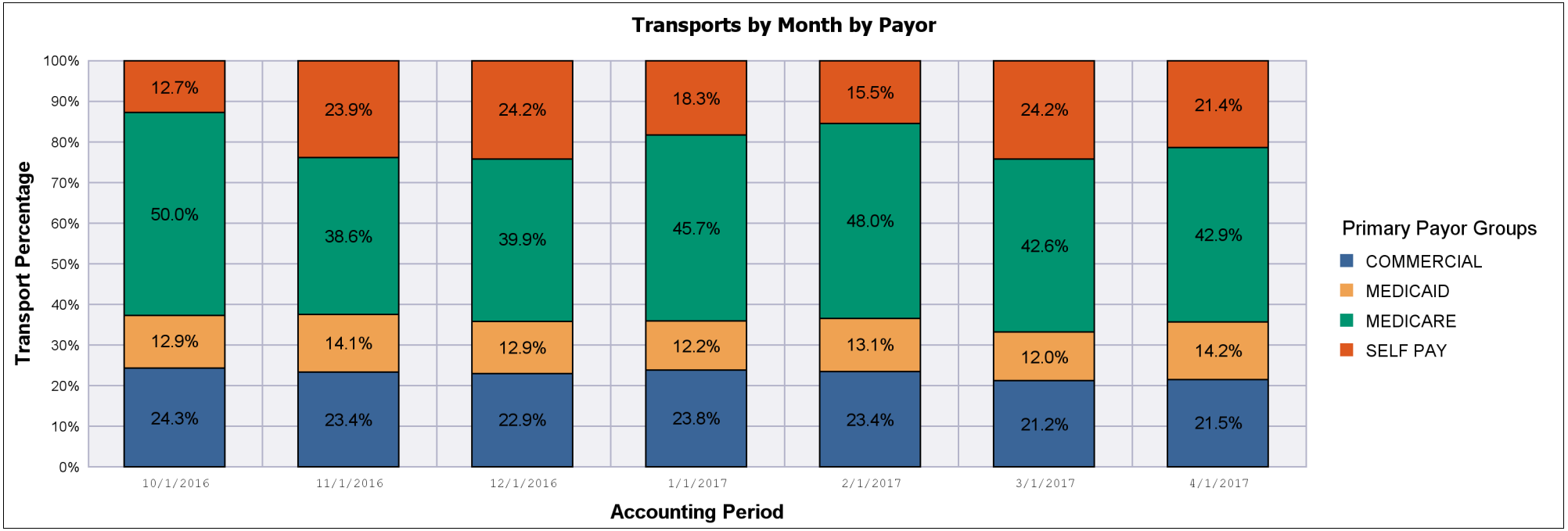
Reporting Period: April 2017

Financial Year	Level of Service	Oct	Nov	Dec	Jan	Feb	Mar	Apr	%	Total
2017	**ALS1**	2,100	4,567	3,138	4,326	4,040	4,381	4,033	65.5%	**26,585**
	ALS2	64	186	155	197	123	166	143	2.5%	**1,034**
	BLS	872	2,330	1,710	2,225	1,786	2,115	1,929	31.9%	**12,967**
	Total	3,036	7,083	5,003	6,748	5,949	6,662	6,105		**40,586**

April 2017

	COMMERCIAL	MEDICAID	MEDICARE	SELF PAY	Total
2016-10	737	393	1,519	387	3,036
2016-11	1,656	1,002	2,731	1,694	7,083
2016-12	1,147	646	1,997	1,213	5,003
2017-01	1,604	823	3,084	1,237	6,748
2017-02	1,393	781	2,853	922	5,949
2017-03	1,414	798	2,837	1,613	6,662
2017-04	1,312	867	2,621	1,305	6,105
	9,263	**5,310**	**17,642**	**8,371**	**40,586**
	22.8%	**13.1%**	**43.5%**	**20.6%**	





[redacted]County Emergency Medical Services
Fiscal Year Revenue Summary by Posting Date

Reporting Period: April 2017

MOS	Charges	2016-10	2016-11	2016-12	2017-01	2017-02	2017-03	2017-04	
2016-10	$4,146,255	$200	$308,003	$774,228	$135,239	$79,817	$212,514	$44,405	$1,554,406
2016-11	$3,898,404		$20,162	$824,779	$256,350	$111,832	$185,530	$66,593	$1,465,245
2016-12	$4,148,458			$128,648	$633,362	$454,240	$210,291	$95,337	$1,521,878
2017-01	$4,275,259				$34,675	$824,997	$457,824	$99,390	$1,416,887
2017-02	$4,034,243					$132,608	$902,684	$183,163	$1,218,455
2017-03	$4,525,258						$372,189	$656,667	$1,028,855
2017-04	$2,683,220							$116,333	$116,333
	$27,711,097	$200	$328,164	$1,727,655	$1,059,626	$1,603,494	$2,341,031	$1,261,889	$8,322,059

MOS	Charges	2016-10	2016-11	2016-12	2017-01	2017-02	2017-03	2017-04
2016-10	$4,146,255	100.00%	93.86%	44.81%	12.76%	4.98%	9.08%	3.52%
2016-11	$3,898,404		6.14%	47.74%	24.19%	6.97%	7.93%	5.28%
2016-12	$4,148,458			7.45%	59.77%	28.33%	8.98%	7.56%
2017-01	$4,275,259				3.27%	51.45%	19.56%	7.88%
2017-02	$4,034,243					8.27%	38.56%	14.51%
2017-03	$4,525,258						15.90%	52.04%
2017-04	$2,683,220							9.22%

CHANGE HEALTHCARE

Mauricio Chavez, Specialty Vice President – EMS

Sample Client Experience	1996 – 2004 Miami-Dade County Fire Rescue
	1990 – Present City of Miami Fire Rescue
	2014 – Present Lee County EMS 2001 – Present Indian River County Fire Rescue
Education	1987 – 1989 Miami-Dade Community College Miami, FL AA – Business Administration 1990-1992 Florida International University Miami, FL Management Information Systems – BA – Business Administration
Additional Experience	Worked as a Computer Operator, Computer Programmer, Client Manager, Director of Operations and Specialty VP all within the EMS billing umbrella including direct client contacts since 1989.

CHANGE HEALTHCARE

Mary J. Lopez, Director of Operations

Sample Client Experience	1996 – 2004 Miami-Dade County Fire Rescue
	1990 – Present City of Miami Fire Rescue
	2014 – Present Lee County EMS 2001 – Present Indian River County Fire Rescue
Education	1972 – 1974 Miami-Dade Community College Miami, FL AA – School of Health Florida International University Miami, FL BA – School of Health
Additional Experience	Experience with medical billing systems and procedures, including billing EMS transports, radiology, pathology, and anesthesia since 1973. Expert in governmental and private payers' rules and issues.

Getac

V110

FULLY RUGGED 11.6" CONVERTIBLE

Large 11.6" IPS LumiBond® 2.0 sunlight display
6th generation Intel® Core™ processor
Dual hot-swappable battery design
Intel HD graphics 520
Full-size 88 key backlit keyboard
Optional integrated 4G LTE broadband wireless
802.11ac next generation WiFi
MIL-STD 810G and IP65 certified
Industry-leading bumper-to-bumper warranty

6th Gen Intel Core Processor.

With the latest Intel Core i5 or Intel Core i7 processor, the V110 rugged convertible was designed for speed and efficiency. Clocking in at up to 2.6GHz and with Turbo Boost speeds up to 3.4GHz, the V110 has the power needed for the most demanding tasks.

Multi-Level Security

V110 provides TPM 2.0 for powerful anti-tampering protection. Combined with fingerprint scanner, smart card reader, RFID, optional Absolute™ DDS and support for the latest Windows 10 security features, the F110 delivers industry-leading protection for your data and device.

Large 11.6" IPS Display.

The V110 features a large 11.6" IPS display that utilizes our revolutionary LumiBond 2.0 technology to achieve a display that is more readable, and offers better contrast and more crisp colors than any other rugged laptop display. The 11.6" widescreen display is ideally suited providing plenty of real estate to run Windows and your apps on.

Dual Hot-Swappable Batteries.

The V110's unique, hot-swappable dual-battery design allows for potentially infinite, uninterrupted battery life. This enables you to remove one of the two rechargeable batteries and replace it with a fresh battery without ever shutting down apps or your Windows OS.

Full-Size 88 Key Backlit Keyboard.

Unlike our competitors' products that have small keyboards with small keys, the V110 features a full-sized 88-key waterproof membrane backlit keyboard with standard-sized keys. The V110 lets you type the way you're used to typing.

Bumper-to-Bumper Warranty.

Accidents happen. Only Getac offers bumper-to-bumper coverage standard on every V110 rugged convertible.

GETAC V110

Specifications

Getac

GetacSales_US@getac.com
www.getac.com
949.681.2900

Getac, Inc.
400 Exchange, Ste 100
Irvine, CA 92602

Ruggedness
MIL-STD 810G and IP65 certified
MIL-STD 461F ready[2]
Optional ANSI/ISA 12.12.01
Vibration, drop, temperature & humidity resistant
Optional salt fog feature

Operating System
Windows® 10 Professional
(available Windows 7 Professional downgrade option)

CPU
Intel® Core™ i7-6600U vPro™ 2.6GHz processor with Turbo Boost Technology up to 3.4GHz
4MB Intel Smart Cache

Intel Core i7-6500U 2.5GHz processor with Turbo Boost Technology up to 3.1GHz
4MB Intel Smart Cache

Intel Core i5-6300U vPro™ 2.4GHz processor with Turbo Boost Technology up to 3.0GHz
3MB Intel Smart Cache

Intel Core i5-6200U 2.3GHz processor with Turbo Boost Technology up to 2.8GHz
3MB Intel Smart Cache

Memory
4GB DDR4 expandable to 16GB[3]

Storage
Solid State OPAL 2.0 128GB / 256GB / 512GB / 1TB[†]

VGA Controller
Intel HD Graphics 520

Display
11.6" IPS HD (1366x768) 800 NITs
LumiBond® 2.0 sunlight readable display with multi-touch technology
Optional digitizer

Keyboard
Waterproof backlit mechanical membrane keyboard
Optional waterproof rubber keyboard

Expansion
Smart card reader x 1
Express Card 54 x 1

Communications
Intel Dual Band Wireless-AC 8260, 802.11ac
10/100/1000 base-T Ethernet
Bluetooth (v4.2)
Optional discrete GPS
Optional 4G LTE multi-carrier mobile broadband; XLTE Ready[1]

Security
Intel vPro™ Technology (per CPU options)
TPM 2.0
Cable lock slot
NIST BIOS compliant
Optional 13.56MHz RFID/NFC contactless smart card reader
Optional fingerprint reader
Optional Absolute™ DDS software

Pointing Device
Touchscreen:
Capacitive multi-touch screen
Optional dual mode touchscreen (multi-touch and digitizer)
Touchpad:
Glide touchpad with scroll bar

Webcam
FHD webcam x 1
Optional 8MP rear camera x1

Power
AC Adapter (65W, 100-240VAC, 50/60Hz)
Hot swappable Dual Li-Ion battery (2100mAh) x 2 (up to 13 hours of battery life)[4]

Dimensions and Weight
11.77" x 8.78" x 1.34" (299 x 223 x 34mm)
4.36lbs (1.98Kg)[††]

Temperature
Operating Temp:
-5.8° F to 140° F / -21°C to 60°C
Storage Temp:
-40°F to 160°F / -40°C to 71°C
Humidity: 95% RH, non-condensing

I/O Interfaces
DC in x 1
USB 3.0 x 2
USB 2.0 x 1
Network (RJ-45) x 1
Headphone out/Mic-in Combo x 1
HDMI x 1
Serial port (RS-232) x 1
Docking connector (24-pin) x 1
Optional RF antenna pass-through for GPS, WLAN and WWAN

Warranty
3 Year bumper-to-bumper warranty standard[‡]

Specification subject to change without notice.
[1] Data plan required. Cellular data is available in the US on Verizon Wireless and AT&T networks. LTE is available in select markets. Check with your carrier for details. 4G LTE configuration must be ordered at time of purchase.
[2] Requires MIL-STD 461F 90W AC Adapter sold separately.
[3] Computers configured with a 32-bit operating system can address up to 3GB of system memory. Only computers configured with a 64-bit operating system can address 4 GB or more of system memory.
[4] Battery life testing conducted under BatteryMark 4.0.1. Battery performance will vary based on software applications, wireless settings, power management settings, LCD brightness, customized modules and environmental conditions. As with all batteries, maximum capacity decreases with time and use and may eventually need to be replaced by a Getac service provider. Battery life and charge cycles vary by use and settings.
[†] For storage, 1GB = 1 billion bytes; actual formatted capacity less.
[††] Weight varies by configuration and manufacturing process.
[‡] 3 year bumper-to-bumper limited warranty standard. For warranty terms and conditions visit www.getac.com

V1M01Y17

CONFIDENTIAL

January 26, 2017

Dear McKesson Client,

As you may know, McKesson Corporation – Enterprise Technology & Services completed a SOC1 Type 2 examination in the October-November 2016 timeframe. The reporting period reviewed for that examination was October 1, 2015 to September 30, 2016. The scope of the report included two data centers and related general computing controls.

The objective of this letter is to provide our clients and our clients' external financial statement auditors with an update regarding our services and the related controls included in the scope of the SOC 1 report for the period of time that has elapsed since the end of the review period.

In light of this, please be advised that the following statements are true to the best of our knowledge for the period of time between the conclusion of the review period and the date of this letter:

- ☐ There have been no events subsequent to the review period of the report that would have a significant effect on our assertion contained within the report.
- ☐ There have been no significant changes to our services or the underlying processes and/or systems since the conclusion of the review period.
- ☐ There have been no significant changes to our control objectives or the related control activities described in the SOC 1 report since the conclusion of the review period.
- ☐ Excluding the exceptions noted in the report, the control activities that govern our services have operated as described in the SOC 1 report since the conclusion of the review period.
- ☐ There have been no significant changes to the complementary user entity controls necessary to achieve the control objectives as described in the SOC 1 report.
- ☐ We are not aware of any significant operating or design deficiencies specific to the control activities described in the SOC 1 report that have occurred since the conclusion of the review period.
- ☐ We are making significant progress regarding the remediation of the exceptions defined in the report.
- ☐ Going forward, our reporting period will remain October 1 – September 30.

For additional questions, please contact your McKesson Customer Contact Representative.

Sincerely,

Kenneth Hogan
Manager ISRM Compliance – McKesson ETS

McKesson Corporation
One Post Street
San Francisco, CA 94104

www.mckesson.com

SOC 1 REPORT

FOR

MCKESSON ETS

A TYPE 2 INDEPENDENT SERVICE AUDITOR'S REPORT ON A DESCRIPTION OF A SERVICE ORGANIZATION'S SYSTEM AND THE SUITABILITY OF THE DESIGN AND OPERATING EFFECTIVENESS OF CONTROLS

FOR THE PERIOD OCTOBER 1, 2015, TO SEPTEMBER 30, 2016

PREPARED IN ACCORDANCE WITH THE
AICPA SSAE NO. 16 STANDARD

Attestation and Compliance Services

schellman
formerly BrightLine

Table of Contents

Section 1 Independent Service Auditor's Report 1

Section 2 Management's Assertion 4

Section 3 Description of the System 7

Section 4 Testing Matrices 28

Section 5 Other Information Provided by Management 49

SECTION I

INDEPENDENT SERVICE AUDITOR'S REPORT

schellman

INDEPENDENT SERVICE AUDITOR'S REPORT

To McKesson Corporation:

Scope

We have examined McKesson Corporation's ("McKesson" or the "service organization") description of its Enterprise Technology Services (ETS) system at the San Francisco, California, Rancho Cordova, California, and Atlanta, Georgia, facilities throughout the period October 1, 2015, to September 30, 2016, (the "description") and the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the description. The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls contemplated in the design of McKesson's controls are suitably designed and operating effectively, along with related controls at the service organization. We have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

In Section 5, McKesson has provided additional information that is not a part of McKesson's description. Such information has not been subjected to the procedures applied in our examination of the description and of the suitability of design of controls to achieve the related control objectives stated in the description, and accordingly, we express no opinion on it.

Service organization's responsibilities

In Section 2, McKesson has provided an assertion about the fairness of the presentation of the description and suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description. McKesson is responsible for preparing the description and for the assertion, including the completeness, accuracy, and method of presentation of the description and the assertion, providing the services covered by the description, specifying the control objectives and stating them in the description, identifying the risks that threaten the achievement of the control objectives, selecting the criteria, and designing, implementing, and documenting controls to achieve the related control objectives stated in the description.

Service auditor's responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on our examination. We conducted our examination in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is fairly presented and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description throughout the period October 1, 2015, to September 30, 2016.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of the service organization's controls to achieve the related control objectives stated in the description involves performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of those controls to achieve the related control objectives stated in the description. Our procedures included assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the description. Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the related control objectives stated in the description were achieved. An examination engagement of this type also includes evaluating the overall presentation of the description and the suitability of the control objectives stated therein, and the suitability of the criteria specified by the service organization and described in Section 2. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Inherent limitations

Because of their nature, controls at a service organization may not prevent, or detect and correct, all errors or omissions in processing or reporting transactions. Also, the projection to the future of any evaluation of the fairness

of the presentation of the description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives is subject to the risk that controls at a service organization may become inadequate or fail.

Opinion

In our opinion, in all material respects, based on the criteria described in McKesson's assertion in Section 2,

a. the description fairly presents the McKesson system that was designed and implemented throughout the period October 1, 2015, to September 30, 2016;

b. the controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period October 1, 2015, to September 30, 2016, and user entities applied the complementary user entity controls contemplated in the design of McKesson's controls throughout the period October 1, 2015, to September 30, 2016; and

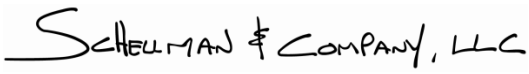
c. the controls tested, which together with the complementary user entity controls referred to in the scope paragraph of this report, if operating effectively, were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved, operated effectively throughout the period October 1, 2015, to September 30, 2016.

Description of tests of controls

The specific controls tested and the nature, timing, and results of those tests are listed in Section 4 (the "Testing Matrices").

Restricted use

This report, including the description of the tests of controls and results thereof in the Testing Matrices, is intended solely for the information and use of McKesson, user entities of McKesson's system during some or all of the period October 1, 2015, to September 30, 2016, and the independent auditors of such user entities, who have a sufficient understanding to consider it, along with other information including information about controls implemented by user entities themselves, when assessing the risks of material misstatements of user entities' financial statements. This report is not intended to be and should not be used by anyone other than these specified parties.



Tampa, Florida
January 18, 2017

SECTION 2

MANAGEMENT'S ASSERTION

MANAGEMENT'S ASSERTION

We have prepared the description of McKesson Corporation's system (the "description") for user entities of the ETS system during some or all of the period October 1, 2015, to September 30, 2016, and their user auditors who have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities of the system themselves, when assessing the risks of material misstatements of user entities' financial statements.

We confirm, to the best of our knowledge and belief, that

a. the description fairly presents the McKesson ETS system made available to user entities of the system during some or all of the period October 1, 2015, to September 30, 2016, for processing their transactions. The criteria we used in making our assertion were that the description

   i. presents how the system made available to user entities of the system was designed and implemented to process relevant transactions, including, as applicable:

      (1) the types of services provided including, as appropriate, the classes of transactions processed;

      (2) the procedures, within both automated and manual systems, by which services are provided, including, as appropriate, procedures by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to reports and other information presented to user entities of the system;

      (3) the related accounting records, supporting information, and specific accounts that are used to initiate, authorize, record, process, and report transactions; this includes the correction of incorrect information and how information is transferred to the reports and other information prepared for user entities of the system;

      (4) how the system captures and addresses significant events and conditions, other than transactions;

      (5) the process used to prepare reports or other information provided for entities of the system;

      (6) specified control objectives and controls designed to achieve those objectives, including as applicable, complementary user entity controls contemplated in the design of our controls; and

      (7) other aspects of our control environment, risk assessment process, information and communication systems (including the related business processes), control activities, and monitoring controls that are relevant to processing and reporting transactions of user entities of the system.

   ii. does not omit or distort information relevant to the scope of the McKesson ETS system, while acknowledging that the description is presented to meet the common needs of a broad range of user entities of the system and their user auditors, and may not, therefore, include every aspect of the McKesson ETS system that each individual user entity of the system and its user auditor may consider important in its own particular environment; and

   iii. includes relevant details of changes to the McKesson ETS system during the period October 1, 2015, to September 30, 2016.

b. the controls related to the control objectives stated in the description were suitably designed and operated effectively throughout the period October 1, 2015, to September 30, 2016, to achieve those control objectives. The criteria we used in making this assertion were that

   i. the risks that threaten the achievement of the control objectives stated in the description have been identified by management;

ii. the controls identified in the description would, if operating as described, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved; and

iii. the controls were consistently applied as designed, and manual controls were applied by individuals who have the appropriate competence and authority.

SECTION 3

DESCRIPTION OF THE SYSTEM

OVERVIEW OF OPERATIONS

Company Background

McKesson Corporation ("McKesson") delivers pharmaceuticals, medical supplies and healthcare information technology designed to make healthcare safer and reduce costs.

McKesson, founded in 1833 and headquartered in San Francisco, California, plays an integral role in healthcare and has a unique vision for its future. McKesson serves American hospitals, U.S. physicians and health plans, delivering medications used daily in North America.

Distribution Solutions

McKesson Distribution Solutions (MDS) delivers pharmaceutical and medical products and business services to retail pharmacies and institutional providers like hospitals and health systems throughout North America and internationally. MDS also provides specialty pharmaceutical solutions for biotech and pharmaceutical manufacturers, as well as practice management, technology, and clinical support to oncology and other specialty practices. Additionally, MDS delivers a suite of healthcare products, technology, equipment, and related services to the non-hospital market, including physician offices, surgery centers, long-term care facilities, and home healthcare businesses.

MDS consists of the US Pharmaceutical, McKesson Canada, McKesson Medical-Surgical, McKesson Specialty Health, McKesson Pharmacy Technology and Services, and Celesio business units.

Technology Solutions

McKesson Technology Solutions (MTS) provides software solutions, services and consulting to hospitals, physician offices, imaging centers, home health care agencies, and payers. MTS also provides connectivity services that streamline clinical, financial, and administrative communication between patients, providers, payers, pharmacies, and financial institutions. MTS solutions are designed to improve patient safety, reduce the cost and variability of care, improve health care efficiency, and better manage revenue streams and resources.

MTS consists of the McKesson Health Solutions, Imaging and Workflow Solutions, Connected Care and Analytics, Business Performance Solutions, and Enterprise Information Solutions business units.

[Intentionally Blank]

McKesson Enterprise Structure

Description of Services Provided

McKesson ETS provides end-to-end information technology (IT) services and solutions to McKesson business units and employees, including support and infrastructure for technology solutions the business units deliver to McKesson customers.

For employees, McKesson ETS supports McKesson's IT and services, including the McKesson's technology infrastructure, IT support desk, Internet access, and e-mail, as well as business systems like SAP and human resource information system (HRIS).

McKesson ETS' portfolio is composed of a range of solutions, such as data center, network, security, server (operating system), and application (e.g., web) services. Customers can choose from a variety of solutions depending on their technical requirements (i.e., reliability, performance, security, and support) and the cost associated with the selected services. This approach allows customers to subscribe to solutions that reflect their business and technical requirements while providing the flexibility of managing risk against cost.

The services provided by McKesson ETS are supported by personnel located in various locations, including San Francisco, California (Corporate Headquarters); Rancho Cordova, California (Drohan Data Center (Drohan)); and Atlanta, Georgia (North Druid Hills 1 Data Center (NDH1)). Drohan and NDH1 are the primary McKesson ETS data centers that are managed and operated by McKesson ETS personnel. The aforementioned locations are in scope for the purposes of this report.

The following are the services and capabilities that are available and provided to customers by the McKesson ETS organization:

- **Colocation —** Facility services for systems installed within one of McKesson ETS' enterprise data centers. Services provided include space, power, cooling, physical security, fire suppression, outbound network firewalls, environmental controls, and facility plan operations.
- **Data Center —** Provides customers with server hosting and administration services. These services include maintaining the computing environment to be compliant with relevant security, compliance, and audit standards.
- **Hosting Services —** Provides server hosting to customers or access to hosted Application Service Provider applications. Services by the Hosting Services team include the ongoing engineering, administration, management, and certification of hardware infrastructure for applications and solutions.
- **Infrastructure as a Service (IaaS) —** Provides IaaS at a simple cost structure for managing customer applications and servers.
- **Network —** Provides network services (including local area network (LAN)/wide area network service offerings, corporate virtual private network (VPN), and Econolink) to McKesson customers

Boundaries of the System

Subservice Organizations

No subservice organizations were included in the scope of this assessment.

Significant Changes During the Review Period

No significant changes to the McKesson ETS system occurred during the review period.

Functional Areas of Operations

- Executive management – responsible for overseeing company-wide activities, establishing and accomplishing goals, and overseeing objectives
- IT Department – manages, monitors and supports user entities' information and systems from unauthorized access and use while maintaining integrity and availability

Infrastructure

The production information systems are located the Drohan and NDH1 data centers used to by McKesson ETS to support McKesson business units. The ETS environment consists of various operating systems, including Microsoft Windows Server, CentOS Linux, and databases, including Oracle and Microsoft SQL. The environment is composed of virtual servers, with Citrix and VMWare hypervisors managing the virtualized environments. External connections to the environment are only permitted through the use of the McKesson access portal, which requires the use of a password and an RSA token that is installed on an individual's machine. IPSoft is used for enterprise monitoring and alerting.

CONTROL ENVIRONMENT

The control environment at McKesson is the foundation for the other areas of internal control. It sets the tone of the organization and influences the control consciousness of its personnel. The components of the control environment factors include the integrity and ethical values, management's commitment to competence; its organizational structure; the assignment of authority and responsibility; and the oversight and direction provided by the board of directors and operations management.

Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of McKesson's control environment, affecting the design, administration, and monitoring of other components. McKesson management delivers consistent and periodic messages to its employees regarding the value of teamwork, collective versus individual success, the importance of client service versus self-service, and that success for the organization and the individual will not occur as the result of any unethical or deceptive behavior.

Specific control activities that McKesson has implemented in this area include the following:

- Management's commitment to integrity and ethical behavior is demonstrated through the application of the "integrity, customer first, accountability, respect, excellence" (ICARE) principles. ICARE training has been provided to employees and is included as part of new-hire orientation.
- Personnel who violate McKesson's *Code of Business Conduct and Ethics* (the "Code") are subject to disciplinary actions, up to and including immediate termination. The Code is located on the corporate intranet and McKesson's public website. Employees are required to acknowledge that they have read and understand The Code upon hire and annually thereafter.
- A third party service provider administers a company-wide telephone hotline service. The hotline called the McKesson Global Compliance and Ethics Line has a toll-free number in operation 24 hours day, seven days a week, through which employees and others who have suspicions of wrongdoing, illegal or unethical acts, breaches of Company policy, or any form of loss relating to the Company's operations, property, or employees, may file a report.
- Employees participate in ongoing training and certification regarding internal controls and processes.

McKesson business units have a Chief Compliance Officer who oversees the unit's compliance program and helps to ensure compliance with governing laws, contractual obligations, and company ethics.

Board of Directors and Audit Committee Oversight

McKesson control consciousness is influenced significantly by the Board of Directors and Audit Committee.

Specific control activities that McKesson has implemented in this area include the following:

- The board of directors makes an annual determination as to the independence of each of its members. Each year, members are asked by the corporate secretary's office to complete a questionnaire that explores respective histories, stock ownership, and relationships with McKesson. Answers to the questionnaires are reviewed by the corporate secretary's office and relationships or transactions are analyzed by McKesson's lawyers and disclosed, as required, to the board of directors, and to the Company's stockholders in the proxy statement.
- The board of directors has adopted a related-party transactions policy, which establishes standards and a process for evaluating transactions with entities in which directors have involvement.
- The audit committee has a written charter, which is posted on McKesson's website under "Corporate Governance."

Organizational Structure and Assignment of Authority and Responsibility

McKesson's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. McKesson's management believes that establishing a relevant organizational structure includes considering key areas of authority and responsibility and appropriate lines of reporting. McKesson has, therefore, developed an organizational structure that is suited to its needs and is based, in part, on its size and the nature of its activities.

McKesson's assignment of authority and responsibility activities includes factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies

are established. It also includes policies relating to business practices, knowledge and experience of key personnel, and resources provided for carrying out duties.

In addition, it includes policies and communications directed at ensuring that personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and what they will be held accountable for. Organizational charts are in place to communicate key areas of authority, responsibility, and appropriate lines of reporting to personnel. These charts are communicated to employees and updated as needed.

Commitment to Competence

McKesson's management defines competence as the knowledge and skills necessary to accomplish tasks that define an employee's roles and responsibilities. Among McKesson's stated values are performance, excellence, and continuous improvement; thus, a fundamental aspect of performance measurement is the extent to which McKesson employees pursue and demonstrate a commitment to competence.

Specific control activities that McKesson has implemented in this area include the following:

- Hiring decisions are approved by the human resources department, and personnel are qualified through the hiring process for their assigned level or responsibility.
- Ongoing training is offered through courses in professional and technical development.
- A formal performance management process is in place that includes assessment of performance twice a year based on performance objectives and competencies defined at the beginning of each fiscal year.
- HR personnel perform criminal, credit, educational, and employment background checks on applications as a component of the hiring process.
- Drug testing is performed as a component of the hiring process.

Accountability

McKesson's management philosophy and operating style encompasses a broad range of characteristics. Such characteristics may include the following: management's approach to taking and monitoring business risks; management's attitudes and actions toward financial reporting (conservative or aggressive selection from available alternative accounting principles, and conscientiousness and conservatism with which accounting estimates are developed); and management's attitudes toward information processing, accounting functions, and personnel.

Additionally, McKesson's human resources policies and practices relate to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities.

Specific control activities that McKesson has implemented in these areas include the following:

- Management receives regulatory updates affecting services provided and industry correspondence on an ongoing basis. Management conducts periodic independent internal audits to ensure compliance to internal processes.
- Meetings are conducted on a regular basis to discuss operational issues related to McKesson services.
- A new hire checklist is completed for new employees.
- Termination checklists are completed as a component of the termination process.

RISK ASSESSMENT

McKesson has placed into operation a risk-assessment process to identify and manage risks that could affect the organization's ability to provide reliable general IT control activities and infrastructure services for customers. This process requires management to identify significant risks in their areas of responsibility and to implement appropriate measures to address those risks. Key stakeholders, including service owners, ETS management, information security and risk management personnel, and executive management, meet on an annual basis to identify and review risks applicable to the services provided. These risks are documented in various means, including spreadsheets and the corporate GRC tool.

The risk assessment process has three components: identifying risks; establishing a risk level by determining the likelihood of occurrence and impact; and finally, identifying controls and safeguards that reduce the impact of the risk to an acceptable level. To gather relevant information, the risk management team utilizes a number of techniques, including brainstorming, questionnaires, on-site interviews, and documentation reviews.

Risk Factors

Risks that are considered during management's risk assessment activities include consideration of the following events:

External Factors

- Technological developments
- Changing customer needs or expectations
- New legislation and regulation that could force changes in policies and strategies
- Natural catastrophes that could lead to changes in operations or information systems
- Economic changes that could have an impact on management decisions

Internal Factors

- Significant changes in policies, processes or personnel
- Types of fraud
- Fraud incentives and pressures for employees
- Fraud opportunities
- Employee attitudes and rationalizations for fraud
- A disruption in information systems processing
- The quality of personnel hired and methods of training utilized
- Changes in management responsibilities
- Expanded operations
- Corporate restructurings

Risk Analysis

Risk analysis is an essential process to McKesson ETS' success. It includes identification of key business processes where potential exposures of some consequence exist, as well as significant changes to those processes. Management has implemented a process whereby the likelihood and impact of identified risks are assessed. Once the likelihood and impact of each identified risk have been assessed, management determine a control rating for the risk, based on the type and level of controls and/or management activities that are currently

in place to manage the risk. These factors are evaluated to determine the residual risk, which is the exposure to the business after consideration of management and control activities designed and implemented to specifically mitigate a risk. Management then considers how the residual risk should be managed using four risk mitigation strategies:

- Risk Acceptance: management accepts the potential risk and continues operating after performing due diligence of examining the risks and determining the risk level.
- Risk Mitigation: management approves the implementation of controls that lower the risk to an acceptable level. These control activities are documented in the Related Control Activities section below.
- Risk Avoidance: management avoids the risks by eliminating the function or process that could cause the risk.
- Risk Transference: management transfers the risk by using other options to compensate for a loss such as purchasing an insurance policy.

In addition to the above process, the McKesson Internal Audit department performs an annual risk assessment, which covers business units within the McKesson enterprise. Interviews are held with corporate and business unit leadership to identify and determine key objectives, initiatives, challenges, and risks that are being experienced at the business unit and/or enterprise-wide level. Once these interviews have been conducted, the Internal Audit management team compiles a register of the key risks identified (i.e., financial, operational, reputation, compliance, strategic, fraud) and assigns a risk score based on impact, likelihood, and management preparedness. The information compiled within the risk register is subsequently presented and confirmed with business unit leadership (business unit president/general manager and chief financial officer (CFO)/controller) and corporate executives. The Internal Audit management team develops its annual audit plan based on the highest risks identified during this process. The ranking of each risk is internally reevaluated and, if required, recalibrated on a quarterly basis. Additionally, the Vice President of internal audit presents the results of each audit during the quarterly audit committee meetings.

Integration with Control Objectives

Along with assessing risks, management has identified and put into effect actions needed to address those risks. In order to address risks, control objectives have been defined for each significant risk area. Control activities are then defined to serve as mechanisms for managing the achievement of those objectives and help ensure that the actions associated with those risks are carried out properly and efficiently.

CONTROL OBJECTIVES AND RELATED CONTROL ACTIVITIES

Selection and Development of Control Activities

Control activities are a part of the process by which McKesson strives to achieve its business objectives. McKesson has applied a risk management approach to the organization in order to select and develop control activities. After relevant risks have been identified and evaluated, control activities are established to meet the overall objectives of the organization.

The establishment of control activities is inclusive of general control activities over technology. The management personnel of McKesson evaluate the relationships between business processes and the use technology to perform those processes to determine the dependencies on technology. The security management processes for the technology, along with other factors, are analyzed to define and establish the necessary control activities to achieve control objectives that include technology.

The establishment of the control activities is enforced by defined policies and procedures that specifically state management's directives for McKesson personnel. The policies serve as the rules that personnel must follow when implementing certain control activities. The procedures are the series of steps the personnel should follow

when performing business or technology processes and the control activities that are components of those processes. After the policies, procedures and control activities are established, each are implemented, monitored, reviewed and improved when necessary.

McKesson's control objectives and related control activities are included below and also in Section 4 (the "Testing Matrices") of this report.

The description of the service auditor's tests of operating effectiveness and the results of those tests are also presented in the Testing Matrices, adjacent to the service organization's description of control activities. The description of the tests of operating effectiveness and the results of those tests are the responsibility of the service auditor and should be considered information provided by the service auditor.

Physical Access and Environmental Safeguards

Control Objective: Control activities provide reasonable assurance that information resources are protected against environmental hazards and related damage and physical access to information resources is appropriately restricted.

The McKesson ETS environment is housed in two primary data center facilities, which are geographically separated to protect against natural disasters. The data centers are manned 24 hours a day, seven days a week, by the Data Center team, which includes dedicated security personnel. In addition, the data centers are located in unmarked buildings to protect their identity and help reduce the risk of intentional attacks.

Formal access procedures exist for controlling physical access to the data centers. Entrants to the data center, whether McKesson ETS employees, visitors, or contractors, must identify themselves and show proof of identity. Valid proof of identity is a photo identification (ID) issued by McKesson or a governmental entity. Only escorted visitors, McKesson ETS employees, and authorized contractors are allowed admittance into the data centers. In addition to a valid proof of identify, visitors are required to provide a written record containing the date, time in, time out, and purpose of the visit. Visitors are also required to review the Data Center Access Policy prior to accessing the data center. Evidence of review is captured via a signature in the visitor's log. Once a visitor has signed in, the visitor is provided with a temporary badge and is escorted by a McKesson ETS employee throughout the duration of the visit.

Access to the data center, including restricted and secured areas (e.g., raised floor), requires approval from an authorized Data Center employee. Only McKesson ETS employees and authorized contractors who permanently work at the data center are granted access to the raised-floor area.

An electronic key card access control system that is linked to card readers, and a system alarm (for restricted or secured areas) is in place at the Drohan and NDH1 data center facilities. The access control system monitors and records each individual's access to the perimeter doors and secured areas. Unauthorized activity and failed access attempts are logged by the access control system and investigated by the Data Center Security and Incident Management teams. The security manager reviews access log reports on a daily basis and the Data Center Manager reviews access log reports on a monthly basis. The key card access logs are retained for a minimum of three months. Access throughout the business operations and data center areas is restricted based on the individual's job responsibilities. System access logs are generated and retained for a minimum of three months. Additionally, a periodic review over individuals with permanent access to the data center (including sensitive work areas) is performed by data center management on a monthly basis to confirm that access is still required based on their job responsibilities.

The primary entrance to the Drohan or NDH1 data centers is through the manned reception area. Other doors or entryways, such as fire doors, exist within the data centers and are controlled or secured through an access card reader, alarm system, or are made inaccessible from the outside. Digital Video Recorder Internet Protocol (DVR IP) cameras are located inside and outside the data center facilities and within the raised floor area. The cameras are monitored 24 hours a day, seven days a week, by the Data Center Security team. Camera footage is recorded and retained for a minimum of 120 days based on the amount of activity.

<u>Redundancy</u>

The data center is designed with resiliency and redundancy. The redundancy is intended to minimize the impact of common equipment failures and environmental risks. Infrastructure systems have been designed to eliminate

single points of failure. Dual circuits, switches, networks, or other necessary devices are utilized to provide this redundancy. Critical facilities infrastructure at the data centers have been designed to be robust, fault tolerant, and concurrently maintainable. Preventative and corrective maintenance is performed without interruption of services.

The environmental equipment has documented preventative maintenance procedures that detail the procedure and frequency of maintenance in accordance with either the manufacturer's or internal specifications. Preventative and corrective maintenance is performed to support the operability of the Drohan and NDH1 data centers. The preventative maintenance schedule is managed at an enterprise level and is designed so that equipment is working properly and sustaining the quality and capacity outlined in customer service level agreements (SLAs). Scheduled maintenance is performed according to documented procedures once a service request has been created and approved by the Data Center Facilities team.

Power

The data centers electrical power systems are designed to be fully redundant and maintainable without impact to continuous operations, 24 hours a day, seven days a week. A primary as well as an alternate power source, each with equal capacity, is provided for critical infrastructure components in the data center. This redundancy begins with dual utility power feeds, primary and alternate, to parallel utility switchboards sized so that anyone can provide power to the entire facility. The output power is then routed to supply building loads, including uninterruptible power supplies (UPS), building and mechanical services, and heating, ventilation, and air conditioning systems.

Backup battery power is provided by UPS batteries and diesel generators. UPS batteries supply power protection during utility brownouts, blackouts, over voltage, under voltage, and out-of-tolerance frequency conditions. During normal operations, the utility power charges the battery modules, as well as supplies power to the raised-floor area. If utility power is interrupted, the UPS batteries provide backup support until the diesel generator systems take over power service.

Emergency electrical power at the Drohan data center is provided by five diesel backup generators. These generators automatically start up and provide power within 10 seconds of a power outage. There are 30,000 gallons of fuel storage, enough for at least six days of operation at full load.

Emergency electrical power at the NDH1 data center is provided by two diesel backup generators. The primary generator will automatically start up and provide power within 10 seconds of a power outage. The other generator remains in standby mode and will automatically start up in the event that the primary generator fails to come online. There are 21,000 gallons of fuel storage, enough for at least six days of operation at full load.

Climate and Temperature

Air-cooling is required to maintain a constant operating temperature for servers and other computing hardware, which prevents overheating and reduces the possibility of a service outage. The Drohan and NDH1 data centers have ambient temperature sensors located within the server racks as well as on each computer room air conditioner (CRAC). There are currently multiple CRAC units that cool the raised-floor area and maintain constant temperature and humidity conditions.

The CRAC units utilized within the Drohan and NDH1 data centers are powered by both normal and emergency electrical systems. These units are monitored by the Data Center Facilities team.

Fire Detection and Suppression

Automatic fire detection and suppression equipment have been installed to prevent damage to computing hardware. The fire detection system utilizes smoke and/or heat detection sensors that are located in the data center ceiling plenum, main room, and below the raised floor, as well as in critical support areas. These sensors are tied to a pre-acting gaseous suppression system. In the event that smoke is detected, the system will generate visible alarms in the raised floor, at the security console, and at the remote monitoring desk of the local fire department.

The fire sprinkler system is a dry pipe system. Pipes are equipped with heat-activated heads that allow water flow to occur if the temperature at the head exceeds a set limit. This time delay is to prevent false alarms from discharging water over the computer hardware. The fire sprinkler system utilizes city water pressure to extinguish

the fire within the data centers and is a completely automatic system, which requires no operator intervention to activate.

In addition, there are fire extinguishers located at each of the raised-floor entrances, which are to be used as the first line of fire fighting. All hand-held fire extinguishers are inspected annually.

Backup and Recovery

Control Objective: Control activities provide reasonable assurance that programs, files, and datasets are routinely backed up and archived in a secure location and that measures have been taken to reduce the risk of a business interruption.

McKesson ETS utilizes a combination of disk and tape backups to protect internal and customer data. Backups of customer data take place using dedicated backup servers and tape libraries. Backups of databases and file systems are performed according to formal procedures and/or the requirements and guidelines established within a customer's SLA. The standard backup schedule is daily for production servers. Any failures that occur during a database or file system backup are reviewed and resolved by the Operations team immediately or during the next business day. A Remedy ticket is opened for each backup failure to document and track the identified issues to resolution.

A contracted third party service provider performs secure transportation of the backups between the data center location and the tape storage location each day, in addition to providing off-site data storage services. Backup tapes transported by the third party, utilize dedicated transport containers and have scheduled times for pick-up and delivery.

Before tapes are picked up by the third party, operations personnel scan the bar code label of each tape to produce a shipping list that is sent to the third party electronically. A hard copy of the shipping list is also included in the shipment. When the third party receives the physical tape shipment, the tape bar code labels are scanned and compared to the shipping list that was sent electronically by the Drohan or NDH1 data centers. A notification is sent to operations personnel if any expected tapes were missing or if any unexpected tapes were included in the shipment.

Before tapes are shipped back to the data centers, the above process is repeated with the third party organization performing the preliminary scan of the tapes and providing the operations team with both electronic and hard-copy formats of the shipping list. Upon receipt at the data centers, the tape bar code labels are scanned and reconciled to the shipping list. If any expected tapes are missing or if any unexpected tapes are received, the third party is subsequently notified. The off-site rotation period is 14 days for daily backup tapes, three years for monthly backup tapes, and seven years for yearly backup tapes.

Computer Operations

Control Objective: Controls provide reasonable assurance that the implementation of new equipment and services (i.e., servers, storage, and network equipment) is tracked, reviewed, and authorized.

McKesson ETS has developed formal policies and procedures for confirming the production readiness of new services. The purpose of the production acceptance (PA) process is to verify compliance with current engineering standards and operational requirements for services being promoted into the production environment. Deployment is the event of moving the services/devices into the production environment. Go-Live is the date when the deployed services are "fit for purpose" and ready for use by the business.

Services include storage (backups), Linux/Unix and Wintel servers, and network and telephony equipment.

Servers and Storage

If a new service is required, a ticket is created within the Remedy system by the project manager ten days prior to Go-Live with a change type of "project". Additionally, for a new equipment deployment, a ticket is created within the Remedy system by the build team with a change type of "change".

Once a Remedy ticket has been created, the project manager sends the e-mail notification to the Run and Build teams. The notification details the Go-Live date or start date (confirmed against the internal McKesson SLA

date), a link to the project folder in SharePoint, an attached copy of the completed internal McKesson SLA, and the Remedy ticket number.

After the e-mail notification, the project manager contacts the build engineering team, who downloads and completes the various automated and manual steps detailed within their applicable PA checklist.

There are separate PA checklists for the various technical groups within the build engineering teams (i.e., Linux/Unix, Windows, and storage). The PA checklist is a series of steps that are performed to determine the service meets engineering and security standards and operational requirements.

Once the server engineering team has completed the PA checklist, the project manager contacts the run team, who performs and completes a similar PA checklist. The completed checklists signal the completion of the PA process, and the new service is implemented in the production environment on the established go-live date. Any issues that were identified and unresolved at the time the PA process was completed are documented as an incident within the Remedy system.

Mainframe and AS400 PA processes are handled by standard IVP (Initial Verification Programs) jobs and manual checks performed by the mainframe team and customer. Customer PA checklists for application verification are also developed and maintained by the customer. At the completion of both checklists, a go/no-go decision is made by the mainframe team and customer.

Once the new service has been implemented, the project manager notifies the operations and hardware asset management teams, who remove the servers from maintenance mode or in the case of mainframe and AS400, operations standard monitoring is resumed, and update the Hewlett Packard asset management (HPAM) database from “build” to “in service” status, respectively.

The Remedy ticket is then closed by the project manager within 30 calendar days of the go-live date.

Network

If a new network service is required, the implementation engineer responsible for the change completes a PA request form and submits it to the PA team via e-mail. Upon receipt of PA request form, the PA team creates a PA Remedy ticket with the project manager and or data center engineering team manager as the owner. PA requestor contacts the assigned PA engineer, who performs a peer review to confirm that the network configurations meet established design standards. Within the PA process, the data center network (DCN) team, and other operations personnel complete a PA checklist. Once the PA checklist is completed, the new service is accepted into the production environment. Any issues that were identified through the PA process are documented and completed as an incident within the Remedy system assigned to the implementation engineer. Once issues have been remediated the PA process is documented as complete.

Once the new service has been implemented, the project manager closes out the Remedy ticket within 30 calendar days of the go-live.

Database

The McKesson Oracle database team is divided into the database operations team and database application team. The primary function of the database operations team is to provide Tier 1/Level 1 database support for the SQL and Oracle databases managed by McKesson ETS. The database application team provides dedicated application database administration services for their respective business units. This includes supporting application development, database upgrades, application enhancements, usage trend analysis, performance tuning of databases for optimal application performance, backup recovery strategies, and new database provisioning.

New database servers including operating system and system software installations are performed by server build teams and follow the PA process.

Incident Management

Control Objective: Control activities provide reasonable assurance that processing incidents impacting infrastructure are identified, assigned, and resolved in a timely manner.

McKesson ETS has developed and implemented a formal incident management and resolution process, which is used to manage various types of incidents, such as connectivity problems, account lockouts, PC or laptop issues, and security events (e.g., intrusion and privilege abuse, malicious code, denial of service, unauthorized access, theft, or electronic information).

If an incident is identified, a ticket is automatically generated within the Remedy system or is manually opened by the McKesson SupportNow Help Desk ("Help Desk") or Operations personnel (system alerts). Once generated, the Help Desk reviews the ticket summary and determines the impact and priority level of the incident. Depending on the impact or severity rating of the incident associated with the ticket, the incident is internally resolved by the Help Desk or assigned to the designated technical or support group for resolution. Remedy is systematically configured to route an incident ticket to a designated group based on the type of incident reported. If the impact level of the incident is high or catastrophic, multiple departmental teams (e.g., Corporate Legal Team), as well as senior and executive-level personnel, are involved with the management, resolution, and communication of the incident.

Once the Remedy ticket has been assigned or routed to the designated group, an analysis or investigation is performed to determine the root cause of the incident. Based on the results of the analysis or investigation, the recovery or resolution plan is created and implemented to resolve the incident. The analysis and decisions, including the summary of the incident, actions taken by the incident responders, contact information of involved parties, and incident resolution date, are documented within or are attached to the Remedy ticket for reference purposes.

For non-security related incidents, a Daily Operations Meeting (DOM) is held with the Incident Management and Operations team to review and determine the risk and criticality associated with incident tickets with a high-impact level. As part of the meeting, the root cause and impact of each incident is discussed and the next steps are determined to resolve the incident. In addition to the DOM, the Security Incident Response Team generates monthly and quarterly reports that detail past and current security incidents. The reports are provided to the chief information security officer, who determines whether any security related threats or trends exist within the Company's environment.

Logical Access

Control Objective: Controls provide reasonable assurance that logical security tools and techniques are configured, administered and monitored to restrict access to programs, data, and other information resources.

McKesson ETS's Information Security and Risk Management group has developed formal policies and procedures specific to logical security to ensure access to sensitive system resources and data are properly restricted and monitored. Access and authentication control technologies, such as unique user accounts, two-factor authentication, access profiles, and passwords, as well as logically restricted access to hosts, data, and configuration information, restricts unauthorized access to internal and customer systems and data.

Multiple layers of authentication are required to access customer systems within the McKesson ETS environment. The first level of authentication requires a user account and token password to access the McKesson VPN. The second level of access requires a user account and password to authenticate to the McKesson internal network. The third layer of access requires a user account and password to authenticate to a customer server.

Provisioning of General and Privileged Access

The granting or modification of system access rights is requested through the shared service catalog tool. If access is requested by the new or existing user's manager, the request is automatically approved through the McKesson ETS shared service catalog. The McKesson ETS security operations team manages the requests sent through the shared service catalog and provides general access for the various technical teams within the organization (e.g., Windows, Unix, ASP, Mainframe). Specific access to local servers or other system resources may be provisioned by the individual technical teams, but is performed on a limited basis and is accompanied by a ticket documenting the implementation. Once the request has been submitted, the McKesson ETS shared service catalog automatically notifies and sends the access request to the requestor's manager for review and approval. After management approval is obtained, the database administration (DBA) team creates a change ticket to implement access, and then subsequently provisions the specified access rights. User IDs and one-time unique passwords are randomly generated and provided to the user via e-mail using workflow tools. First time passwords are generated leveraging known data elements from the user's profile so they are not transmitted in

clear text (e.g., assignment of the first five numbers in a supplied password from a user's home zip code and the last four numbers from the user's Social Security Number (SSN)).

If super user or privileged access to a specific platform (e.g., Unix "root" access) is required, the user's manager completes the "Super User — System Access Request" form in the service catalog and submits it to the security operations team. Once the form has been received with the manager's approval, the respective system administrator creates a super user ID (SID) for the user. Access to sensitive system utilities and resources are restricted to authorized individuals based on their job responsibilities.

Unix root access is provisioned by the Unix system administration (USA) team. Elevated rights in Unix leverage the sudo functionality. Sudoer access is managed and provisioned by the USA team. For users who require administrative (local or domain) access to a Windows production server, the user's manager completes the "Super User — System Access Request" form in the service catalog and submits it to the security operations team. Once the form has been received with the manager's approval, a system administrator creates a SID for the user. If a user requires temporary access to a production server, a change request is initiated through the ticketing system. The user or requestor is required to detail the reason for the access, the affected servers, and the timeline of the project that requires administrative capabilities. The approval process follows the standard McKesson ETS change management process. If a user requires permanent access, an incident ticket is created within the ticketing system and assigned to the Windows systems administration (WSA) group through the general McKesson ETS incident management process.

Documentation of the requestor's SID and an approved "Policy Exception Request Form" is included within the incident ticket.

Termination of General and Privileged Access

When an employee is terminated from the company, HR or the terminated employee's manager enters the termination date within the HRMS system, which automatically disables the employee's domain or network account and remote access the evening of the entered date via an automated process. Access to single-sign-on enabled applications such as shared services catalog, Remedy ticketing system, PeopleSoft HRMS, and McKesson intranet (internal employee portal) is also disabled. A daily termination report is also sent by PeopleSoft to the McKesson ETS security operations team and the various technical teams. Furthermore, the terminated employee's manager is prompted to review a termination checklist to ensure that any physical or informational assets (e.g., PDA, CDs, and badges) are collected from the employee. Once the termination checklist has been completed, the terminated employee's manager returns it to the HR team for retention purposes.

Password Settings

Access and administration of logical security for systems under McKesson ETS administrative authority rely upon user IDs and passwords to authenticate users to systems and devices, as well as to authorize the level of access for the user. As this control is a primary component of the McKesson ETS security strategy, McKesson ETS has developed and implemented explicit password policies.

Where possible, security controls built into system, such as specified characteristics and expiration, are used to enforce the password standards. In other cases, McKesson ETS employees are responsible for implementing the appropriate standards on passwords for which they have responsibility. For users with sensitive or privileged access, such as system or security administration functions, stronger password standards have been designed and implemented. Key standards within the McKesson ETS password policy are:

- Passwords must be a minimum of eight alpha-numeric characters using both upper and lowercase letters.
- Passwords must be changed every three months to a new and unique password.
- When possible, passwords should include numbers and/or symbols/special characters.
- Passwords must not be coded into login scripts, dial-in communications programs, browsers, or any executable program or file.

- When an account is created, it must be assigned a random and secure password that must be preset to expire upon login. The password can be generated by the system or by the creator of the account. The password assignments must be unique to each user, and the user must be forced to change the password upon login.
- After five consecutive incorrect password attempts are entered, the system will lock out the user's account.
- Users must not be able to construct passwords that are identical passwords they have previously employed in the last five times they have changed their password. User selections for new passwords must be checked against the history and rejected if there is a match.

Periodic User Access Review

In accordance with frequency defined in established McKesson ETS policies and procedures, sensitive and privileged access rights associated with system users are reviewed for appropriateness on a periodic basis for each technical area within the McKesson ETS organization. The user access review is performed separately by each technical team (usually management-level personnel). The review process for the McKesson ETS technical teams is described in detail below:

Windows

A review of privileged users is performed on a quarterly basis by the system manager and system administrator for Windows-based systems and servers. Privileged access is restricted to the appropriate individuals within the windows implementation engineering, WSA, and storage administration (USS) teams. Once the user access review is completed, any required changes are formally documented and sent to the McKesson ETS system operations team for immediate disabling or removal of the requested access. A completion notification is subsequently sent to the reviewers once the access has been disabled or removed.

Unix/Linux

A review of privileged users is performed on a quarterly basis by the Unix manager and Unix technical lead for Unix-based systems and servers. Privileged access is restricted to appropriate individuals within the storage implementation engineering, Unix DBA, enterprise systems management, information security administration, middleware, OPS, USA, and USS teams. Once the user access review has been completed, any required changes are formally documented and sent to the McKesson ETS system operations team for immediate disabling or removal of the requested access. A completion notification is subsequently sent to the reviewers once the access has been disabled or removed.

Mainframe

A review of privileged users is performed on a monthly basis by the RACF group owners. Privileged access is restricted to appropriate individuals within the system administration, OPS, and information security teams. Once the user access review has been completed, any required changes are formally documented and sent to the McKesson ETS system operations team for immediate disabling or removal of the requested access. A completion notification is subsequently sent to the reviewers once the access has been disabled or removed. In addition to the aforementioned, manual monthly reports are generated for the security and operations users' groups. Members of these groups must respond to e-mails providing notification of current status.

Network Security

A review of users with privileged access to network devices is performed on a biannual basis during SOX self-assessment process. Privileged access should be restricted to appropriate individuals within the network engineering team. Once the user access review has been completed, any required changes are formally documented and reflected within the Opsware configuration management tool by the appropriate network administrator.

Antivirus

McKesson ETS has licensed and implemented a third party antivirus product to scan network-attached Windows systems. At a minimum, daily updates of antivirus signature files are pushed to the managed systems to ensure the maximum effectiveness of the antivirus software and solution.

Network Security

Control Objective: Control activities provide reasonable assurance that the network is secured, managed, and maintained.

Network Architecture and Management

The Drohan and NDH1 data centers have fully redundant local area network (LAN) infrastructures. Border routers that provide the connection point between the data center infrastructure and any Internet service provider are deployed in a fully redundant, fault-tolerant configuration. Multiprotocol label switching is used for McKesson backbone connections. Business-to-Business (B2B) VPNs are configured over the company's internet circuits. Firewalls are also connected in a fully redundant fault-tolerant configuration, as required. Servers that require redundancy are configured with two separate switches, which are connected to separate network interface cards on each server.

McKesson IT has documented procedures and checklists for configuring and installing new routers, switches, and firewalls, as well as documented procedures to add a new server to the network. If a new firewall or router is being set up or a configuration or rule requires modification, a change control ticket is created within the Remedy system and the general McKesson IT change management process is followed. Access to set up or modify a firewall or router configuration is provided on a temporary basis and is removed once the associating project has been completed. The network is documented in detailed network diagrams and configuration documents, including customers' unique specifications.

Various tools, such as IPCenter and Smarts, are installed and used to monitor the status and load of each managed network device and, where possible, the connection to the customer's network. The monitoring tools are configured to generate alerts when specified thresholds are reached or exceeded. When triggered, the predefined group of alerts will generate an automatic notification to designated McKesson IT personnel or create an incident ticket, which is routed to the network control center. The network control center, which is manned 24 hours a day, seven days a week, will then take action on the alert depending on the severity of the problem where appropriate levels of triage and escalation are applied. In addition, the Opsware tool is used to maintain backups of the network device configurations. Upon reaching or exceeding specified thresholds, Orion or Smarts network monitoring tools generate alerts that systematically create Remedy tickets. The network control center tracks Remedy tickets from inception through to resolution. The Opsware tool maintains copies of the current and previous network device configurations. Upon modification of a network device configuration, the Opsware tool systematically captures the prior configuration and the new configuration.

Firewalls

Access into the McKesson IT environments must traverse firewalls. The firewalls perform these validations through recognition protocols as well as the acceptability of ranges of source and destination IP addresses.

McKesson IT has a formal firewall configuration policy that defines acceptable ports that may be used on a firewall. Only required ports are open. Access to change firewall configurations is restricted by terminal access controller access-control system (TACACS) to authorized network security personnel. Firewall configurations are versioned using tools such as Network Management System or Opsware that tracks changes to firewall configurations whenever a change is made.

Change Management

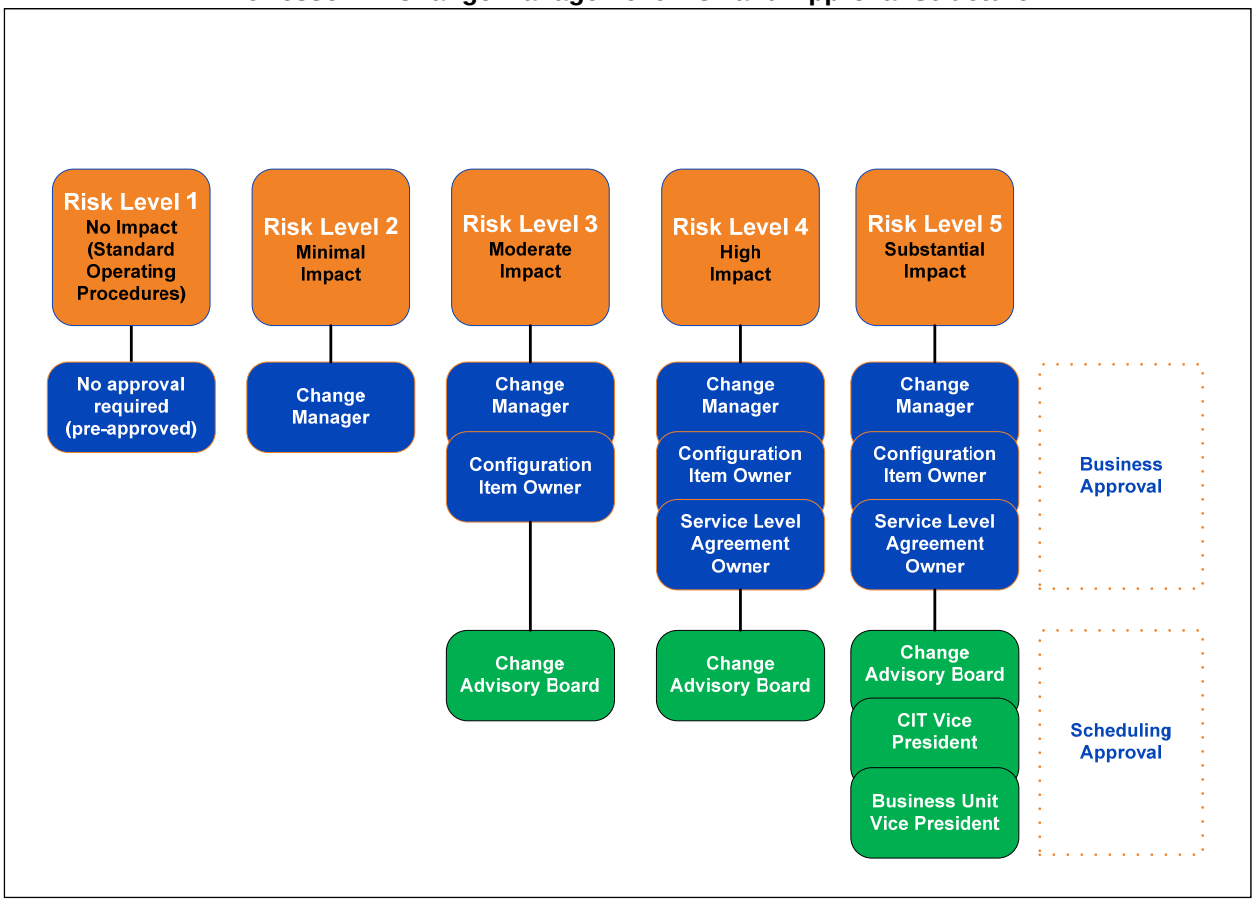
Control Objective: Controls provide reasonable assurance that new and modified network, system software, and database structures are tracked, authorized, tested and approved by management, and implemented in a complete, accurate, and timely manner.

McKesson IT has developed formal policies and procedures over the change management process, which requires system software, hardware, database, and network changes to be approved, tested, implemented, and documented.

Any representative of McKesson IT or a McKesson business unit can initiate a change request within the Remedy ticketing system. Once logged into the ticketing system, the requestor completes the relevant change information, assigns the ticket to the applicable technical group, and submits the change request. The ticketing system automatically assigns a unique tracking number to the ticket and systematically designates the

appropriate individual(s) to approve the change. Further, the ticketing system lists the approvers' e-mail addresses and sends a notification informing the approver of the change request. Once the ticket is routed to the change approver(s), a review is performed to evaluate and confirm the level of risk, impact, and priority associated with the change. Change approvers may be different depending on the technical group(s) that is impacted by the change. Additionally, multiple change approvers may be required based on the defined risk level associated with a change request, based on the risk and approval structure referenced below:

McKesson IT Change Management Risk and Approval Structure



Standard operating procedures (SOPs), such as a domain name system (DNS) change, are defined and formally documented as small routine changes that do not pose a financial or operational risk to the McKesson IT organization and its customers. Due to the low risk and impact associated with SOPs, a formal change approval is not required prior to production implementation. SOP changes are preapproved by applicable management personnel. Additionally, testing over SOPs have been benchmarked, and therefore, additional testing is not required for subsequent changes that occur. Changes are tested by individual(s) or group(s) depending on the type of change, and the results are captured within an e-mail or the ticket associated with the change, in accordance with change management policies and procedures. Changes categorized as Level 3 require testing. Issues identified during the testing are captured as needed in the ticket and resolved by the change owner prior to implementing the change.

Approvers have the authority to accept or reject a change. If rejected, the Remedy system automatically sends a notification to the requestor, who closes out the ticket and works with the change approver to determine the cause of the rejection. If approved, the change request is carried out and completed, and is tested by the IT, business, or quality assurance (QA) personnel to ensure that the change is operating as intended or specified by the requestor.

Since SOP-related changes do not require a real-time approval, the change facilitator (a designated technical team member) verifies that the change was preapproved prior to production implementation.

Development, test, and production environments are logically and/or physically separated, per established policies or customer specific SLAs. If the creation of a testing environment is not feasible (i.e., mainframe platforms), testing is performed in the development environment by restricting access to authorized testers only.

Management has established a change advisory board (CAB), which reviews and approves change requests with an associated risk level of 3, 4, or 5. If the risk level of the change is 1 or 2, the change does not require CAB approval. The CAB meets weekly to discuss, approve, and schedule the implementation date for proposed changes, and to review the status of past changes. Proposed changes are tested prior to being presented to the CAB for approval. The CAB approval is documented within the ticket. Changes with a risk level of 5 also require an approval from the McKesson IT vice president and vice president of the impacted business unit. Once the change has received required approvals, it is scheduled for implementation (i.e., "implementation in progress" status in Remedy) and a notice is automatically sent to the impacted or affected parties identified within the ticket.

A detailed implementation plan, including a back-out plan where applicable, is also documented within the ticket. The change is then implemented by an individual or group separate from the resource that performed or completed the change. Access to implement a change in production is restricted to the migration or operations team. Once the change has been successfully implemented, the ticket is closed by the requestor or a technical team member.

Emergency changes can result due to various reasons, such as system outages, software problems, or hardware failures. Emergency changes are implemented prior to a ticket being opened and completed. Due to the time sensitivity associated with emergency changes, approvals are provided verbally prior to the implementation; however, a Remedy ticket, including the documentation of approvals, testing, and other relevant information, is completed within 24 hours of the emergency change implementation.

System Patch Management

Notification of new vendor patches, service packs, bug fixes, or security alerts are received by the McKesson IT organization through various channels. McKesson IT technical teams subscribe to major vendors who regularly notify the applicable teams of new system updates or security-related information. Additionally, regular monitoring of vendor websites is performed by the McKesson IT technical team members to determine the availability of new system updates, threats, and/or vulnerabilities. The McKesson IT information security and risk management team also distributes periodic e-mails to the various technical teams of security-related threats and vulnerabilities that may potentially impact the McKesson IT infrastructure or environment.

If a system update is deemed necessary, the impacted team follows the general McKesson IT change management process, described above, which requires a documented approval and testing within the Remedy system.

Notifications of network-specific patches are received either through vendor alerts, software age and vulnerability reports, or through a request made within the central network SharePoint site. Once the patch notification or request has been received by McKesson IT, the Standards Committee assigns the subject matter expert (SME) to perform an initial review of the patch. The SME determines whether the patch is relevant and whether it will have an impact on the current infrastructure and environment. The analysis performed by the SME is subsequently sent to the standards committee, who reviews the conclusion of the analysis and determines whether to approve the patch. If rejected, the standards committee contacts the requestor and the applicable stakeholders. If approved, a "preliminary standard" (i.e., patching strategy) is published in the SharePoint site by the SME.

Once published, the requestor and applicable target groups (e.g., Microsoft Windows and Unix) and stakeholders review the preliminary standard and determine whether to approve it or not. If rejected, the SME responds to the feedback provided by the reviewers and reinitiates the process. If approved, the preliminary standard is relabeled as a "standard" and the patch is implemented. A notification is sent to the affected parties once the patching process has been completed.

Information and Communication Systems

Relevant Information

Information is necessary for McKesson to carry out internal control responsibilities to support the achievement of its objectives related to the McKesson system. Management obtains or generates and uses relevant and quality information from both internal and external sources to support the functioning of internal control.

The following provides a summary of internal and external sources of information used in the McKesson ETS:

- Real-time environment status and availability information
- Alerts received from enterprise monitoring applications
- Incident information received from customers
- Specific requests for changes from business units or other information received from business units that results in modifications to the production environment
- Information received from third parties, such as security and vulnerability alerts

Communication

Upper management is involved with day-to-day operations and is able to provide personnel with an understanding of their individual roles and responsibilities pertaining to internal controls. This includes the extent to which personnel understand how their activities relate to the work of others and the means of reporting exceptions to a higher level within the Company. McKesson's management believes that open communication channels helps make sure exceptions are reported and acted upon. For that reason, formal communication tools, such as organizational charts and employee handbooks, are in place.

Management's communication activities are made electronically, verbally, and through the actions of management.

Specific control activities that McKesson has implemented in this area include the following:

- The corporate communications department determines the forms of communication utilized for the type and timeliness of disseminating information throughout McKesson.
- Communications with regulators are managed by the executive vice president, the CFO, the controller, and general counsel. This senior team of executives reviews incoming communications and the Company's responses for appropriateness and accuracy before they are submitted to regulators.
- Communications to McKesson stockholders are handled by the investor relations department and the Corporate Secretary's office.

Monitoring

Monitoring Activities

Monitoring is a process that assesses the quality of internal control performance over time. It involves assessing the design and operation of controls and taking necessary corrective actions. This process is accomplished through ongoing activities, separate evaluation, or a combination of the two. Monitoring activities also include using information from communications from external parties such as user entity complaints and regulatory comments that may indicate problems or highlight areas in need of improvement. Management has implemented a self-assessment and compliance program to ensure the controls are consistently applied as designed.

Ongoing Monitoring

Specifically describe how monitoring procedures are built in to normal management and supervisory activities.

Describe how user entity complaints and/or regulator comments are utilized to identify problems and highlight areas in need of improvement.

Separate Evaluations

Management has implemented a self-assessment program to evaluate the performance of specific control activities and processes over time, and confirm that the in-scope controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority. As a result of management's risk analysis process, each control activity within scope has been assigned a risk level associated with the assessed level of risk it is intended to mitigate. Controls that serve to mitigate multiple risks are assigned the highest level of assessed risk among the pertinent risks.

Internal and External Auditing

McKesson supports many user entities in their efforts to meet the regulatory demands of their industry or governing agency. McKesson has assisted user entities in successfully meeting the requirements of many certifications and regulatory demands, including (remove or add to the listing):

- Sarbanes-Oxley (SOX)
- Internal audits
- Business unit reviews
- Payment Card Industry Data Security Standard (PCI DSS)
- ISO/IEC 27001

Reporting Deficiencies

The nature, timing and extent of the self-assessment tests and results are documented by the self-assessors, for management review. Deviations or deficiencies associated with controls are escalated to management for immediate correction action, when required.

COMPLEMENTARY CONTROLS AT USER ENTITIES

McKesson's ETS system is designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all of the control objectives related to McKesson's ETS system to be solely achieved by McKesson's control activities. Accordingly, user entities, in conjunction with the ETS system, should establish their own internal controls or procedures to complement those of McKesson.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the specified control objectives described within this report are met:

Physical Access and Environmental Safeguards

1. User entities are responsible for the physical security of all devices connected to the McKesson ETS environment that are not controlled by McKesson ETS and do not reside at McKesson ETS data center.

Backup and Recovery

2. User entities are responsible for determining that tape backup, retention, and rotation schedules are appropriate for their need.

3. User entities are responsible for the business recovery and backup over their non-McKesson ETS managed information systems that are networked to the customer's environment.

Computer Operations

4. User entities are responsible for manual checks of mainframe implementations prior to go-live.

Incident Management

5. User entities are responsible for reviewing service level and incident reports provided by McKesson IT and initiating any clarification or follow-up based on stipulated specifications in the customer SLA.

Logical Access

6. User entities are responsible for provisioning, modification, and removal of access to McKesson ETS systems.
7. User entities are responsible for reviewing user access privileges on a periodic basis.
8. User entities are responsible for notifying McKesson ETS of any unauthorized use of any password or account or any other known or suspected breach of security related to the McKesson ETS computing environment.

Network Security

9. User entities are responsible for network connections or for conditions or problems arising from or related to network connections, or caused by the Internet.
10. User entities are responsible for the results of any access to the McKesson IT environment by third parties for which they have provided such access (e.g., implementers, contractors, third party, end-users).

Change Management

11. User entities are responsible for ascertaining individuals creating and/or updating change tickets, or approving change requests, have the proper authorization.

SECTION 4

TESTING MATRICES

TESTS OF OPERATING EFFECTIVENESS AND RESULTS OF TESTS

Scope of Testing

This report on the controls relates to the McKesson ETS system provided by McKesson. The scope of the testing was restricted to the McKesson ETS System considered to be relevant to the internal control over financial reporting of respective user entities. Schellman & Company, LLC (Schellman) conducted the examination testing over the period October 1, 2015, through September 30, 2016.

Tests of Operating Effectiveness

The tests applied to test the operating effectiveness of controls are listed alongside each of the respective control activities within the Testing Matrices. Such tests were considered necessary to evaluate whether the controls were sufficient to provide reasonable, but not absolute, assurance that the specified control objectives were achieved during the review period. In selecting the tests of controls, Schellman considered various factors including, but not limited to, the following:

- The nature of the control and the frequency with which it operates;
- The control risk mitigated by the control;
- The effectiveness of entity-level controls, especially controls that monitor other controls;
- The degree to which the control relies on the effectiveness of other controls;
- Whether the control is manually performed or automated;

The types of tests performed with respect to the operational effectiveness of the control activities detailed in this section are briefly described below:

Test Approach	Description
Inquiry	Inquired of relevant personnel with the requisite knowledge and experience regarding the performance and application of the related control activity. This included in-person interviews, telephone calls, e-mails, web-based conferences, or a combination of the preceding.
Observation	Observed the relevant processes or procedures during fieldwork. This included, but was not limited to, witnessing the performance of controls or evidence of control performance with relevant personnel, systems, or locations relevant to the performance of control policies and procedures.
Inspection	Inspected the relevant audit records. This included, but was not limited to, documents, system configurations and settings, or the existence of sampling attributes, such as signatures, approvals, or logged events. In some cases, inspection testing involved tracing events forward to consequent system documentation or processes (e.g., resolution, detailed documentation, alarms, etc.) or vouching backwards for prerequisite events (e.g., approvals, authorizations, etc.).

Sampling

Consistent with American Institute of Certified Public Accountants (AICPA) authoritative literature, Schellman utilizes professional judgment to consider the tolerable deviation rate, the expected deviation rate, the audit risk, the characteristics of the population, and other factors, in order to determine the number of items to be selected in a sample for a particular test. Schellman, in accordance with AICPA authoritative literature, selected samples in such a way that the samples were expected to be representative of the population. This included judgmental selection methods, where applicable, to ensure representative samples were obtained.

System-generated population listings were obtained whenever possible to ensure completeness prior to selecting samples. In some instances, full populations were tested in cases including but not limited to, the uniqueness of the event or low overall population size.

Test Results

The results of each test applied are listed alongside each respective test applied within the Testing Matrices. Test results not deemed as control deviations are noted by the phrase "No exceptions noted." in the test result column of the Testing Matrices. Any phrase, other than the aforementioned, constitutes a test result that is the result of non-occurrence, a change in the application of the control activity, or a deficiency in the operating effectiveness of the control activity. Testing deviations identified within the Testing Matrices are not necessarily weaknesses in the total system of controls at user entities, as this determination can only be made after consideration of controls in place at user entities, and other factors. Control considerations that should be implemented by user entities in order to complement the control activities and achieve the stated control objective are presented in the "Complementary Controls at User Entities" within Section 3.

PHYSICAL ACCESS AND ENVIRONMENTAL SAFEGUARDS

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that information resources are protected against environmental hazards and related damage and physical access to information resources is appropriately restricted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.01	Physical security policies and procedures are in place to guide employees' activities for granting, controlling and revoking physical access to the data center.	Inspected the physical security policies and procedures to determine that physical security policies and procedures were documented to guide employee's activities for granting, controlling and revoking physical access to the data center.	No exceptions noted.
1.02	New access rights to the data center or the issuance of an electronic key card is approved by an authorized data center employee.	Inquired of the facility manager to determine that new access rights to the data center or the issuance of an electronic key card were approved by an authorized data center employee and to determine what employees were authorized to provision such access.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the access approval documentation for a sample of employees granted access to the data center or provisioned an electronic key card during the review period to determine that the new access rights were approved by an authorized data center employee prior to access being granted.	No exceptions noted.
1.03	On a daily basis, the Data Center Physical Security Personnel review unauthorized activity and failed access attempts logged by the access control system. Events are investigated as appropriate by the Data Center Security and Incident Management teams. The key card access logs are retained for a minimum of three months.	Inquired of the facility manager to determine that data center physical security personnel reviewed unauthorized activity and failed access attempts logged by the access control system on a daily basis and that events were investigated, as appropriate, by the data center security and incident management teams.	No exceptions noted.
		Inspected the review of unauthorized activity and failed access attempts for a sample of dates during the review period to determine that data center security personnel reviewed the logs for each date sampled.	No exceptions noted.
		Inspected the access management system log archives to determine that key card access logs were retained for at least three months.	No exceptions noted.
1.04	On a monthly basis, a review of individuals with access to the data center is performed by data center management. Access is removed if it is no longer required for job responsibilities.	Inspected the review of data center access for a sample of months during the review period to determine that a data center access review was performed for each in-scope data center for each month sampled and access was removed if no longer required.	No exceptions noted.
1.05	Entrance to the data center is only authorized by data center security after showing proof of identity (a photo ID issued by McKesson or a governmental entity).	Inquired of the facility manager regarding entrance to the data center to determine that entrance was only by authorized by security personnel after providing proof of identity (a photo ID issued by McKesson or a governmental entity).	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Observed the process for entering the data center to determine that entrance to the data center was only authorized by data center security after a valid McKesson ID or government issued ID was shown.	No exceptions noted.
1.06	Visitors are required to sign a visitor's log at the main reception desk upon entrance to the data center.	Observed the visitor access process to determine that visitors were required to sign a visitor's log at the reception desk upon entrance to the office facility.	No exceptions noted.
		Inspected the visitors log for a sample of months during the review period to determine that visitors signed a visitor's log for each month sampled.	No exceptions noted.
1.07	DVR IP cameras are located inside and outside the data center facilities and within the raised floor area. The cameras are monitored 24 hours a day, 7 days a week, by the Data Center Security team. Camera footage is recorded and retained for a minimum of 120 days based on the amount of activity.	Inquired of the facility manager and the chief engineer to determine that DVR IP cameras were located inside and outside the data center facilities and within the raised floor area, that camera surveillance was monitored 24 hours a day, seven days a week, and that camera footage was retained for at least 120 days.	No exceptions noted.
		Observed the camera locations with the assistance of the chief engineer and facility manager from the in-scope data centers that DVR IP cameras were located inside and outside of the data center facilities, including the raised floor area.	No exceptions noted.
		Inspected the historical camera footage from the in-scope data centers to determine that camera footage was retained for at least 120 days.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.08	The primary entrance to the data centers is through a manned reception area. Other doors or entry ways, such as fire doors exist within the data centers are controlled or secured through an access card reader, alarm system, or are made inaccessible from the outside.	Inquired of the facility manager regarding data center entrances to determine that the primary entrance to the data centers was through a manned reception area and that other doors or entry ways, such as fire doors were controlled or secured through an access card reader, alarm system, or made inaccessible from the outside.	No exceptions noted.
		Observed the primary and non-primary entrances to the data center during the review period to determine that the primary entrance was manned by security personnel and other entrances, including fire doors, were controlled or secured via an access card reader, alarm system, or otherwise inaccessible from the outside.	No exceptions noted.
1.09	Preventative maintenance procedures are performed for environmental equipment according to documented procedures and frequencies.	Inspected the maintenance documentation for a sample of devices located in the in-scope data centers to determine that preventative maintenance was performed for each device sampled according to the documented frequencies outlined in the maintenance schedules.	No exceptions noted.
1.10	Power supply and management systems are installed and operating to provide the data center with a continuous supply of conditioned power in the event of power loss or failure. These systems include UPS batteries and diesel generators.	Observed the UPS batteries and diesel generators at each of the in-scope data centers to determine that power supply and management systems were installed and operating to provide the data center with a continuous supply of conditioned power in the event of a power loss or failure.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.11	Ambient temperature sensors are located at each CRAC and within the server racks. CRAC units perform cooling of the raised floor area and maintain constant temperature and humidity conditions.	Inquired of the chief engineer and the facility manager regarding data center temperature management to determine that ambient temperature sensors were located at each CRAC and within the server racks and that CRAC units performed cooling of the raised floor area and maintained constant temperature and humidity conditions.	No exceptions noted.
		Observed ambient temperature sensors located at each CRAC and within the server rack to determine that CRAC units performed cooling of the raised floor area and maintained constant temperature and humidity conditions.	No exceptions noted.
1.12	Automatic fire detection and suppression equipment has been installed to prevent damage to computing hardware. The fire detection system utilizes smoke and/or heat detection sensors that are located in the data center ceiling plenum, main room, and below the raised floor as well as in data center support areas. These sensors monitor a pre-acting gaseous suppression system and will generate visible alarms in the raised floor and at the security console. Additionally, dry pipe fire sprinklers have been installed within the data centers and are configured to activate if the temperature exceeds a set heat limit.	Observed the fire detection system to determine that the fire detection system utilized smoke and/or heat detection sensors that were located in the data center ceiling plenum, main room, and below the raised floor as well as in data center support areas and that the sensors monitored a pre-acting gaseous suppression system and generated visible alarms in the raised floor and at the security console.	No exceptions noted.
		Observed dry pipe fire sprinklers to determine that dry pipe fire sprinklers were installed and configured to activate upon set heat limits being exceeded.	No exceptions noted.

BACKUP AND RECOVERY

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that programs, files, and datasets are routinely backed up and archived in a secure location and that measures have been taken to reduce the risk of a business interruption.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
2.01	McKesson IT has developed formal policies and procedures over the backup and recovery processes. The policy is updated on an as needed basis.	Inquired of the manager of IT compliance regarding backup and recovery policies and procedures to determine that formal policies and procedures over backup and recovery processes were documented and updated as needed.	No exceptions noted.
		Inspected the data backup and recovery policies and procedures to determine that formal policies and procedures over the backup and recovery processes were documented.	No exceptions noted.
2.02	McKesson ETS performs backups of databases and file systems according to the defined customer requirements.	Inspected the customer requirements and backup schedules for a sample of production servers and databases to determine that backups of databases and file systems were performed in accordance with defined customer requirements for each production server and database sampled.	No exceptions noted.
2.03	A ticket is systematically opened for each scheduled backup failure. Tickets that cannot be resolved automatically are assigned to the EDP group. EDP team members review and track assigned tickets through resolution in a timely manner.	Inquired of the storage operations director regarding tickets to determine tickets were systematically opened for scheduled backup failures and assigned to the EDP group when unable to be resolved automatically and that EDP team members reviewed and tracked through resolution.	No exceptions noted.
		Inspected the ticket detail for a sample of backup failures during the review period to determine that the tickets were opened, assigned and resolved for each backup failure sampled.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
2.04	McKesson computer operations personnel prepare backup tapes on a daily basis for transmittal to an off-site location via a third party.	Inquired of the director of data center operations regarding backups to determine that computer operations personnel prepared backup tapes on a daily basis for the transmittal to an off-site location via a third party.	No exceptions noted.
		Inspected the backup tape transmittal reports for a sample of dates during the review period to determine that McKesson computer operations prepared and transmitted backup tapes to an off-site location via a third party for each date sampled.	No exceptions noted.
2.05	McKesson EDP monitors data replication of data domain devices. Anomalies or failures resulting from the replication are tracked through tickets and resolved.	Inspected the data replication dashboard to determine that McKesson EDP monitored data replication of data domain devices.	No exceptions noted.
		Inspected the ticket detail for a sample of replication failures during the review period to determine that a ticket was created and that anomalies or failures were tracked and resolved for each replication failure sampled.	No exceptions noted.
2.06	Restorations (e.g., ad-hoc customer file system restores) of backups are performed upon request and recorded within the ticketing system.	Inspected the ticket detail for a sample of restoration requests during the review period to determine that restoration of backups were performed and recorded for each restoration request sampled.	No exceptions noted.

COMPUTER OPERATIONS

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that the implementation of new equipment and services (i.e., servers, storage, and network equipment) is tracked, reviewed, and authorized.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
3.01	McKesson IT has developed formal policies and procedures for confirming the production readiness of a server, database, or network service.	Inquired of the network operations manager regarding the development of policies and procedures to determine that formal policies and procedures were developed to confirm the production readiness of a server, database, or network service.	No exceptions noted.
		Inspected the implementation engineering product acceptance process policies and procedures to determine that McKesson IT developed formal policies and procedures confirming the production readiness of a Windows, Unix, or network service.	No exceptions noted.
3.02	Prior to deployment of a new service, steps (as defined in build team checklists) are performed to determine that the service meets engineering and security standards and operational requirements.	Inquired of the network operations manager regarding the steps performed prior to the deployment of a new service to determine that steps were performed to ensure the service met operational requirements, engineering and security standards.	No exceptions noted.
		Inspected the build team checklist for a sample of implementations during the review period to determine that build team checklists were completed for each implementation sampled.	No exceptions noted.
3.03	Upon successful completion of go-live, McKesson personnel responsible for implementation complete a PA checklist, signifying system acceptance.	Inquired of the network operations manager regarding implementations to determine that upon completion of go-live, McKesson personnel responsible for the implementation completed a PA checklist to signify system acceptance.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the PA checklist for a sample of change requests implemented during the review period to determine that McKesson personnel responsible for the implementation completed a PA checklist for each change request sampled.	The test of the control activity disclosed that PA checklists were not evidenced for one of 22 change requests sampled.
3.04	Prior to implementation of network services or equipment, a network team performs a peer review on changes with a risk level of two or higher to validate that the network configurations meet established design standards, and signoff of the peer review is documented in the Remedy ticket.	Inquired of the network operations manager regarding peer reviews to determine that a network team performed a peer review on changes with a risk level of two or higher to validate that network configurations met established design standards and that the signoff of the peer review was documented in the Remedy ticket.	No exceptions noted.
		Inspected the network change ticket detail for a sample of changes with a risk level of two or higher implemented during the review period to determine that signoff of peer review was documented in the Remedy ticket for each change sampled.	No exceptions noted.
3.05	Issues identified and unresolved prior to completion of the PA process are documented as an incident within the Remedy ticketing system and monitored to resolution by the appropriate team, in accordance with the production acceptance process.	Inquired of the network operations manager regarding the monitoring and resolution of unresolved issues prior to completion of the PA process to determine that unresolved issues prior to completion of the PA process were documented as an incident within the Remedy ticketing system and monitored to resolution.	No exceptions noted.
		Inspected the ticket detail for a sample of unresolved production acceptance issue tickets during the review period to determine that the issue was documented as an incident within the Remedy ticketing system and monitored to resolution by the appropriate team for each ticket sampled.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
3.06	Mainframe PA processes are executed by standard IVP jobs, and manual checks are performed by the mainframe team and customer prior to go-live.	Inquired of the TS/SYS - systems programmer regarding the mainframe PA process to determine that mainframe PA processes were executed by standard IVP jobs and that the mainframe team and customer performed manual checks prior to go-live.	No exceptions noted.
		No mainframe implementations occurred during the review period; therefore, no testing of operating effectiveness was performed.	

INCIDENT MANAGEMENT

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that processing incidents impacting infrastructure are identified, assigned, and resolved in a timely manner.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
4.01	A formal incident management and resolution process is in place to manage various types of incidents impacting normal operations processing and ability to provide services.	Inspected the incident management and resolution policies and procedures to determine that a formal incident management and resolution process was in place.	No exceptions noted.
4.02	Incidents reported to the McKesson IT Operations team are logged in the ticketing system, assigned a priority, and assigned to a support group for resolution.	Inquired of the systems manager regarding incidents logging to determine that incidents reported to the McKesson IT Operations team were logged in the ticketing system, assigned a priority, and assigned to a support group for resolution.	No exceptions noted.
		Inspected the incident ticket detail for a sample of incidents logged during the review period to determine that incidents reported to the McKesson IT Operations team were logged in the ticketing system, assigned a priority, and assigned to a support group for resolution for each incident sampled	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
4.03	Incidents assigned are resolved by the group responsible as per policy in accordance with their priority.	Inquired of the systems manager regarding incident resolution to determine that all incidents assigned were resolved by the group responsible, per policy, in accordance with priority.	No exceptions noted.
		Inspected the incident ticket detail for a sample of incidents logged during the review period to determine that incidents were resolved by the group responsible and in the time frames required by policy in accordance with their priority for each incident sampled	No exceptions noted.

Logical Access

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that logical security tools and techniques are configured, administered and monitored to restrict access to programs, data, and other information services.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
5.01	Formal policies and procedures are in place for the logical access and security processes, including password guidelines and standards.	Inspected the information security management policies and procedures to determine that formal policies and procedures were in place for logical access and security processes, including password guidelines and standards.	No exceptions noted.
5.02	User and privileged support accounts follow McKesson ETS security standards for password complexity, length, change frequency, and account lockout.	Inquired of the database administrator regarding privileged support accounts to determine that user and privileged support accounts followed McKesson ETS security standards for complexity, length, change frequency, and account lockout.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the password configurations for a sample of in-scope systems to determine that user and privileged support accounts followed McKesson ETS security standards for password complexity, length, change frequency, and account lockout for each in-scope system sampled.	No exceptions noted.
5.03	General and privileged access to servers or system resources and utilities are approved by the requesting user's manager prior to access being granted.	Inquired of the security operations manager regarding general and privileged access to servers or system resources to determine that approval for general and privileged access to servers or system resources and utilities was required by the requesting users' manager prior to access being granted.	No exceptions noted.
		Inspected the user account request and manager approval for a sample of user accounts granted access to in-scope system resources or utilities during the review period to determine that access was approved by the requesting users' managers prior to access being granted for each user account sampled.	No exceptions noted.
5.04	Administrative access privileges are restricted to user accounts accessible by authorized personnel for in-scope systems including: • Network domain • Production servers • Production databases	Inquired of the IT compliance manager regarding administrative access to determine that administrative access privileges were restricted to user accounts accessible by authorized personnel for the following in-scope systems: • Network domain • Production servers and mainframe • Databases	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the administrative access listings for a sample of in-scope systems with the assistance of the IT compliance manager to determine that administrative access privileges were restricted to user accounts accessible by authorized personnel for the following in-scope systems: • Network domain • Production servers and mainframe • Databases	No exceptions noted.
5.05	In accordance with frequency defined in established McKesson ETS policies and procedures, privileged access to critical systems and servers are reviewed by each technical team within the McKesson ETS organization and with certification from the privileged users' direct manager to confirm access is consistent with management's intentions.	Inquired of the IT compliance manager regarding the review of privileged access to critical systems and servers to determine that in accordance with frequency defined in established McKesson ETS policies and procedures, privileged access to critical systems and servers were reviewed by each technical team within the McKesson ETS organization and with certification from the privileged users' direct manager to confirm access was consistent with management's intentions.	No exceptions noted.
		Inspected the information security management policies and procedures to determine that policies and procedures were in place to define the frequency in which privileged access to critical systems and servers must be reviewed by each technical team.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected a sample of production system privileged user access reviews during the review period to determine that privileged access to critical systems and servers were reviewed by technical teams according to frequencies established by corporate policies and contained management certifications that access was appropriate for each production system sampled.	No exceptions noted.
5.06	An identity management solution is configured to automatically disable Active Directory user accounts assigned to terminated employees within 24 hours after employee termination in the HR system.	Inspected the identity management solution configurations to determine that the identity management solution is configured to automatically disable Active Directory user accounts assigned to terminated employees within 24 hours after employee termination in the HR system.	No exceptions noted.
		Inspected the Active Directory user listing for a sample of employees terminated during the review period to determine that the Active Directory accounts were disabled by the identity management solution for each terminated employee sampled.	No exceptions noted.
5.07	An automated audit job is configured to execute nightly to detect exceptions not captured by the identity management solution and automatically disable the associated accounts.	Inspected the automated audit job configuration and an example output to determine that an automated job was scheduled to run on a nightly basis to detect and disable terminated user accounts that were not detected by the identity management solution.	No exceptions noted.
		Inspected the Active Directory user listing for a sample of employees terminated during the review period to determine that the Active Directory accounts were disabled for each terminated employee sampled.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
5.08	A daily termination report is sent to the McKesson ETS security operations team and the various technical teams, who subsequently disable or remove the access privileges associated with the terminated employee.	Inquired of the IT compliance manager regarding daily termination reports to determine that a daily report of terminated employees was sent to the security operations team who subsequently disabled or removed access rights for each terminated employee.	No exceptions noted.
		Inspected the termination report e-mail messages for a sample of dates during the review period to determine that termination reports were e-mailed to security operations and technical teams for each date sampled.	No exceptions noted.
		Inspected the user access listings of a sample of in-scope systems for a sample of employees terminated during the review period to determine that access privileges for each terminated employee sampled were disabled or removed for each in-scope system sampled.	No exceptions noted.

NETWORK SECURITY

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that the network is secured, managed, and maintained.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
6.01	Formal procedures and checklists are in place for configuring and installing new routers and switches, as well as documented procedures to add a new server to the network.	Inspected the procedures and checklists to determine that procedures and checklists were in place for configuring and installing new routers and switches, as well as documented procedures to add a new server to the network.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
6.02	Firewall configurations are versioned using automated software which systematically captures prior configuration and new configuration changes.	Inquired of the director of network engineering regarding the capture of firewall configuration changes to determine that firewall configurations were versioned using automated software which systematically captured prior and new firewall configuration changes.	No exceptions noted.
		Inspected the automated software history detail to determine that firewall configurations were versioned using automated software which systematically captured prior and new firewall configuration changes.	No exceptions noted.
6.03	A network monitoring application is configured to generate alerts and create incident tickets upon reaching or exceeding configured thresholds. The network control center personnel track tickets from inception to resolution.	Inquired of the director of network engineering regarding network monitoring to determine that incident tickets were monitored from inception to resolution by network control center personnel.	No exceptions noted.
		Observed the network monitoring application alert and ticket generation configurations to determine that a network monitoring application was configured to generate alerts and create incident tickets upon reaching or exceeding configured thresholds.	No exceptions noted.
		Inspected the incident ticket detail for a sample of alerts generated by the network monitoring application during the review period to determine that incident tickets were tracked from inception to resolution for each alert sampled.	No exceptions noted.
6.04	Logical access to network devices is systematically restricted to authorized network engineers through TACACS.	Inquired of the director network engineering regarding logical access to network devices to determine that logical access to network devices was systematically restricted to authorized network engineers through TACACS.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the listing of users with access to network devices during the review period to determine that logical access to network devices was systematically restricted to authorized network engineers via TACACS.	No exceptions noted.

CHANGE MANAGEMENT

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that new and modified network, system software, and database structures are tracked, authorized, tested and approved by management, and implemented in a complete, accurate, and timely manner.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
7.01	Formal policies and procedures are in place for the change management process, which requires system software, hardware, database, and network changes to be tracked, authorized, tested and approved by management prior to implementation.	Inspected the change management policies and procedures to determine that formal policies and procedures were in place for the change management process and required system software, hardware, database, and network changes to be tracked, authorized, tested and approved by management prior to implementation.	No exceptions noted.
7.02	Changes, including system patches, are approved by an authorized approver(s) based on the risk level associated with the change, in accordance with change management policies and procedures.	Inquired of the business system analyst regarding the approval of changes, including system patches, to determine that changes, including system patches, were approved by authorized approver(s) based on the risk level associated with each change, in accordance with change management policies and procedures.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the change ticket detail for a sample of changes implemented during the review period to determine that changes were approved by authorized approver(s) based on the assigned risk level associated with the change in accordance with change management policies for each change sampled.	No exceptions noted.
7.03	Certain changes are tested by individual(s) or a group depending on the type of change, and the results are captured within an e-mail or the ticket associated with the change, in accordance with change management policies and procedures.	Inquired of the IT compliance manager regarding testing of changes to determine that certain changes were tested by individuals or a group depending on the type of change, and the results were captured within an e-mail or the ticket associated with the change, in accordance with change management policies and procedures.	No exceptions noted.
		Inspected the change ticket detail or e-mail documentation for a sample of changes implemented during the review period to determine that changes were tested and the results were captured within an e-mail or ticket for each of change sampled.	No exceptions noted.
7.04	Access to implement software, logical hardware, or maintenance changes to production environments is systematically restricted to the system administration group members representing their respective platform.	Inquired of the business systems analyst regarding the implementation of software, logical hardware, or maintenance changes to the production environment to determine that access to implement software, logical hardware, or maintenance changes was restricted to the system administration group members representing their respective platform.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the production access user listings for a sample of production systems with the assistance of business systems analyst to determine that access to implement changes was restricted to members of the system administration group representing their respective platform for each production system sampled.	No exceptions noted.
7.05	Latent (emergency) changes implemented to prevent or resolve a service outage must have a critical or high incident ticket assigned.	Inquired of the business systems analyst regarding latent (emergency) changes to determine that latent changes implemented to prevent or resolve a service outage and were required to have a critical or high incident ticket assigned.	No exceptions noted.
		Inspected the ticket detail for a sample of latent changes implemented during the review period to determine that latent changes implemented to prevent or resolve a service outage were documented in a critical or high priority incident ticket for each latent change sampled.	No exceptions noted.

SECTION 5

OTHER INFORMATION PROVIDED BY MANAGEMENT

MANAGEMENT'S RESPONSE TO TESTING EXCEPTIONS

Computer Operations

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
3.03	Upon successful completion of go-live, McKesson personnel responsible for implementation complete a PA checklist, signifying system acceptance.	Inspected the PA checklist for a sample of change requests implemented during the review period to determine that McKesson personnel responsible for the implementation completed a PA checklist for each change request sampled.	The test of the control activity disclosed that PA checklists were not evidenced for one of 22 change requests sampled.
Management's Response:	Several organizational changes occurred during the year requiring that McKesson ETS revisit this process and put a plan in place to ensure we meet the overall objective.		

IT Business Continuity and Disaster Recovery

The McKesson IT Service Continuity Office assists customers in developing and implementing an IT Service Continuity Management (SCM) System, which includes a series of IT business continuity and disaster recovery-related processes and solutions that are monitored, reviewed, and improved on a reoccurring basis. IT SCM includes 1) establishing IT business continuity and disaster recovery objectives; 2) defining customer requirements through a business impact analysis; 3) identifying and implementing the appropriate and relevant continuity and recovery strategies; and 4) performing program management activities, such as training, program maintenance, exercising/testing, etc. The IT SCM establishes and maintains processes and solutions designed to protect the customer's people, workplaces, and the continuity of critical business processes from natural disasters, operational incidents, accidents, and human-caused threats. Specific program objectives include:

- Contributing to the health and safety of McKesson's employees and customers
- Protecting key revenue streams
- Strengthening competitive positioning, market share, and organizational reputation
- Maintaining productivity
- Assuring legal and regulatory compliance
- Reducing continuity and availability risks and security threats to an appropriate level
- Enabling organizational certification goals and objectives

The categories and activities described above align to international practices and are consistent with the Plan-Do-Check-Act model found in other management systems (including ISO 27001).

Vulnerability Management

The threat and vulnerability management (TVM) team is responsible for network and web application based vulnerability scanning, and assessment of hosts within the McKesson enterprise. The purpose is to identify weaknesses and flaws within the infrastructure and provide the details of the findings to the appropriate parties for remediation. Additionally, the threat and vulnerability team is consulted when there are questions about the vulnerabilities and the associated remediation which need clarification, or prioritization outside of the individual business units. The TVM team is responsible for scanning in most situations, however, there are other business units which conduct scanning using the solution we have in place or an alternative solution.

Once a vulnerability is identified, it is evaluated and an action is taken. If it is determined the vulnerability is not really a security flaw in the environment, because of compensating reasons, then the risk can be accepted for a

period of time prior to review. In other instances, a risk may be accepted because an application will break with a new version of software and additional controls will need to be put into place to preserve the security posture of the host. In most cases, however, the results are handed off to groups who are able to remediate the findings and then tracked by the requestor which is usually a security oriented liaison between the individual business units and the functions within the Information Security Risk Management (ISRM) group.

Web application scanning is conducted monthly by an enterprise class scanning solution and is designed to identify the weaknesses residing at the web application layer such as PHP, ASP, C++, HTML, Java, and so on. The findings are then provided to the requestor and appropriate support personnel to review.

Network vulnerability scanning is conducted monthly using an enterprise class scanning solution and is performed against the internal and external networks operated by McKesson. The network scanning is used to identify the weaknesses in system and network layers of the environment such as Microsoft Windows, Linux, Unix, Cisco, Juniper, Java, Flash, default accounts, and other system level findings. The findings are then provided to the requestor and appropriate support personnel for review.

Audit Logging

Audit logging over specific activities is performed by the McKesson IT security operations team per established agreements or internal McKesson SLAs with internal technical teams and customers (i.e., business unit). If audit logging is required by a McKesson IT technical team or customer, the appropriate representative contacts and works with the security operations team to define the relevant audit criteria (e.g., log all sudo activity). Once defined, the criteria are configured as rules within the security information and event monitoring (SIEM) tool. Depending on the agreed-upon internal McKesson SLA, the SIEM tool produces reports and/or alerts using the generated audit logs. These reports or alerts are subsequently sent to the security operations center (SOC) as well as the applicable McKesson IT technical teams or customers for review, analysis, and action as warranted.

Security Incident Response

McKesson's information security incident management team has developed documented incident response procedures, tailored specifically for the unique environments and compliance requirements of each of the individual business units of the company. The procedures are validated and updated annually during mock incident table top exercises conducted with core incident response subject matter experts from each respective business unit. Every reported information security incident is reviewed, classified and escalated appropriately by a dedicated incident management expert, through closure, to long term corrective action documentation. All senior members of the incident management team maintain industry-certified digital forensic expertise which they leverage for real-time analysis of digital evidence through pre-deployed industry standard forensic toolkits. Resolved incident records and corrective actions are tracked in centralized risk management systems, where they can be correlated and analyzed to identify emerging risk trends and problem areas. Quarterly security incident metric reviews are conducted with each business unit, to review the findings.

Data Loss Prevention

The overarching data loss prevention program for McKesson locations is managed by the McKesson information security incident management team and centrally monitored 24/7 by dedicated SOC analysts. The system is comprised from a combination of industry-standard products providing end-point, server and network egress monitoring. All detected data exfiltration events are reported and correlated at the centralized risk management dashboard. In addition to traditional end-point monitoring, an enforced removable media encryption component is active on all McKesson managed systems, which effectively prevents unencrypted data from being copied to any portable storage media. Combined with mandatory full-disk encryption for all managed laptops and workstations, this has effectively eliminated all data loss events related to theft or loss of portable computing devices. As an additional control aimed at identification of inadvertent exposures of information shared with authorized partners, commercial cyber-crime intelligence monitoring services are being leveraged for proactive detection of fingerprinted McKesson-owned data being posted to public and "deep web" repositories.

MCKESSON

January 26, 2017

Dear McKesson Client,

McKesson Corporation – Enterprise Technology & Services completed a SOC2 Type 2 examination in the October-November 2016 timeframe. The reporting period reviewed for that examination was January 1, 2016 to September 30, 2016. The scope of the report included two data centers and related general computing controls. The Trusted Service Principles included in the examination were Security and Availability.

The objective of this letter is to provide our clients and our clients with an update regarding our services and the related controls included in the scope of the SOC 2 report for the period of time that has elapsed since the end of the review period.

In light of this, please be advised that the following statements are true to the best of our knowledge for the period of time between the conclusion of the review period and the date of this letter:

- ☐ There have been no events subsequent to the review period of the report that would have a significant effect on our assertion contained within the report.
- ☐ There have been no significant changes to our services or the underlying processes and/or systems since the conclusion of the review period.
- ☐ There have been no significant changes to our control objectives or the related control activities described in the SOC 2 report since the conclusion of the review period.
- ☐ Excluding the exceptions noted in the report, the control activities that govern our services have operated as described in the SOC 2 report since the conclusion of the review period.
- ☐ We are not aware of any significant operating or design deficiencies specific to the common criteria control activities described in the SOC 2 report that have occurred since the conclusion of the review period.
- ☐ We are making significant progress regarding the remediation of the exceptions defined in the report.

For additional questions, please contact your McKesson Customer Contact Representative.

Sincerely,

Kenneth Hogan
Manager ISRM Compliance – McKesson ETS

McKesson Corporation
One Post Street
San Francisco, CA 94104

www.mckesson.com

SOC 2 REPORT

FOR

MCKESSON ETS SYSTEM

A TYPE 2 INDEPENDENT SERVICE AUDITOR'S REPORT ON CONTROLS RELEVANT TO SECURITY AND AVAILABILITY

FOR THE PERIOD JANUARY 1, 2016, TO SEPTEMBER 30, 2016

Attestation and Compliance Services

Table of Contents

Section 1 Independent Service Auditor's Report 1

Section 2 Management's Assertion 4

Section 3 Description of the System 7

Section 4 Testing Matrices 26

Section 5 Other Information Provided by Management 58

SECTION I

INDEPENDENT SERVICE AUDITOR'S REPORT

schellman

INDEPENDENT SERVICE AUDITOR'S REPORT

To McKesson Corporation:

Scope

We have examined the attached description of McKesson Corporation's ("McKesson" or the "service organization") Enterprise Technology Services (ETS) system for the period January 1, 2016, to September 30, 2016, (the "description") performed at the San Francisco, California, Rancho Cordova, California, and Atlanta, Georgia, facilities, based on the criteria set forth in paragraph 1.26 of the AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®)* ("description criteria") and the suitability of the design and operating effectiveness of controls described therein to meet the criteria for the security and availability principles set forth in TSP section 100, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Principles and Criteria)* ("applicable trust services criteria"), throughout the period January 1, 2016, to September 30, 2016.

In Section 5, McKesson has provided additional information that is not a part of McKesson's description. Information about McKesson ETS management's responses to exceptions noted has not been subjected to the procedures applied in the examination of the description and the suitability of the design and operating effectiveness of controls to meet the applicable trust services criteria.

Service organization's responsibilities

McKesson has provided the attached assertion, in Section 2, about the fairness of the presentation of the description based on the description criteria and suitability of the design and operating effectiveness of the controls described therein to meet the applicable trust services criteria. McKesson is responsible for preparing the description of the service organization's system and the assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description of the service organization's system; selecting the trust services principle(s) addressed by the engagement and stating the applicable trust services criteria and related controls in the description of the service organization's system; identifying the risks that would prevent the applicable trust services criteria from being met; identifying any applicable trust services criteria related to the principle(s) being reported on that have been omitted from the description and explaining the reason for the omission; and designing, implementing, and documenting controls to meet the applicable trust services criteria.

Service auditor's responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description based on the description criteria and on the suitability of the design and operating effectiveness of the controls described therein to meet the applicable trust services criteria, based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included procedures that we considered necessary in the circumstances. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is fairly presented based on the description criteria, and the controls were suitably designed and operating effectively to meet the applicable trust services criteria throughout the period January 1, 2016, to September 30, 2016.

Our examination involved performing procedures to obtain evidence about the fairness of the presentation of the description based on the description criteria and that the controls were suitably designed and operating effectively to meet the applicable trust services criteria throughout the period January 1, 2016, to September 30, 2016. Our procedures included assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to meet the applicable trust services criteria. Our procedures also included testing the operating effectiveness of those controls to provide reasonable assurance that the applicable trust

services criteria were met. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Inherent limitations

Because of their nature and inherent limitations, controls at a service organization may not always operate effectively to meet the applicable trust services criteria. Also, the projection to the future of any evaluation of the fairness of the presentation of the description or conclusions about the suitability of the design or operating effectiveness of the controls to meet the applicable trust services criteria is subject to the risks that the system may change or that controls at a service organization may become inadequate or fail.

Opinion

In our opinion, in all material respects, based on the description criteria identified in McKesson's assertion and the applicable trust services criteria

a. the description fairly presents the system that was designed and implemented throughout the period January 1, 2016, to September 30, 2016;

b. the controls stated in the description were suitably designed to provide reasonable assurance that the applicable trust services criteria would be met if the controls operated effectively throughout the period January 1, 2016, to September 30, 2016; and

c. the controls that were tested, which were those necessary to provide reasonable assurance that the applicable trust services criteria were met, operated effectively throughout the period January 1, 2016, to September 30, 2016

Description of test of controls

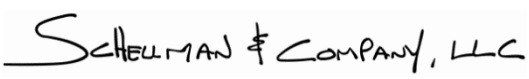
The specific controls we tested and the nature, timing, and results of our tests are presented in section 4 of our report titled "Testing Matrices."

Restricted use

This report, including the description of tests of controls and results thereof in section 4 are intended solely for the information and use of McKesson; user entities of McKesson's ETS system during some or all of the period January 1, 2016, to September 30, 2016; and prospective user entities, independent auditors and practitioners providing services to such user entities, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization;
- How the service organization's system interacts with user entities, subservice organizations, or other parties;
- Internal control and its limitations;
- The nature of user entity controls responsibilities and their role in the user entities internal control as it relates to, and how they interact with, related controls at the service organization;
- The applicable trust services criteria; and
- The risks that may threaten the achievement of the applicable trust services criteria and how controls address those risks.

This report is not intended to be and should not be used by anyone other than these specified parties.



Tampa, Florida
January 18, 2017

SECTION 2

MANAGEMENT'S ASSERTION

McKESSON

MANAGEMENT'S ASSERTION

We have prepared the attached description of McKesson's ETS system for the period January 1, 2016, to September 30, 2016, (the "description") based on the criteria in items (a)(i)–(ii) below, which are the criteria for a description of a service organization's system in paragraph 1.26 of the AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®)* (the "description criteria"). The description is intended to provide users with information about the ETS system, particularly system controls intended to meet the criteria for the security and availability principles set forth in TSP section 100, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Principles and Criteria)* ("applicable trust services criteria"). We confirm, to the best of our knowledge and belief, that

a. the description fairly presents the ETS system throughout the period January 1, 2016, to September 30, 2016, based on the following description criteria:

   i. The description contains the following information:

      1.) The types of services provided;

      2.) The components of the system used to provide the services, which are the following:

         a.) *Infrastructure*. The physical structures, IT, and other hardware (for example, facilities, computers, equipment, mobile devices, and telecommunications networks)

         b.) *Software*. The application programs and IT system software that supports application programs (operating systems, middleware, and utilities)

         c.) *People*. The personnel involved in the governance, operation and use of a system (developers, operators, entity users, vendor personnel, and managers)

         d.) *Procedures.* The automated and manual procedures;

         e.) *Data*. Transaction streams, files, databases, tables, and output used or processed by a system;

      3.) The boundaries or aspects of the system covered by the description;

      4.) For information provided to, or received from, subservice organizations and other parties;

         a.) How such information is provided or received and the role of the subservice organizations and other parties;

         b.) The procedures the service organization performs to determine that such information and its processing, maintenance, and storage are subject to appropriate controls;

      5.) The applicable trust services criteria and the related controls designed to meet those criteria, including, as applicable, the following:

         a.) Complementary user entity controls contemplated in the design of the service organization's system;

         b.) When the inclusive method is used to present a subservice organization, controls at the subservice organization;

      6.) If the service organization presents the subservice organization using the carve-out method;

         a.) The nature of the services provided by the subservice organization;

         b.) Each of the applicable trust services criteria that are intended to be met by controls at the subservice organization, alone or in combination with controls at the service organization, and the types of controls expected to be implemented at carved-out subservice organizations to meet those criteria;

      7.) Any applicable trust services criteria that are not addressed by a control and the reasons; and

8.) In the case of a type 2 report, relevant details of changes to the service organization's system during the period covered by the description.

ii. The description does not omit or distort information relevant to the service organization's system while acknowledging that the description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual report user may consider important to its own particular needs.

b. the controls stated in the description were suitably designed throughout the specified period to meet the applicable trust services criteria.

c. the controls stated in the description operated effectively throughout the specified period to meet the applicable trust services criteria.

SECTION 3

DESCRIPTION OF THE SYSTEM

OVERVIEW OF OPERATIONS

Company Background

McKesson Corporation ("McKesson"), delivers pharmaceuticals, medical supplies and healthcare information technology designed to make healthcare safer and reduce costs.

McKesson, founded in 1833 and headquartered in San Francisco, California, plays an integral role in healthcare and has a unique vision for its future. McKesson serves American hospitals, U.S. physicians and health plans, delivering medications used daily in North America.

Distribution Solutions

McKesson Distribution Solutions (MDS) delivers pharmaceutical and medical products and business services to retail pharmacies and institutional providers like hospitals and health systems throughout North America and internationally. MDS also provides specialty pharmaceutical solutions for biotech and pharmaceutical manufacturers, as well as practice management, technology, and clinical support to oncology and other specialty practices. Additionally, MDS delivers a suite of healthcare products, technology, equipment, and related services to the non-hospital market, including physician offices, surgery centers, long-term care facilities, and home healthcare businesses.

MDS consists of the US Pharmaceutical, McKesson Canada, McKesson Medical-Surgical, McKesson Specialty Health, McKesson Pharmacy Technology and Services, and Celesio business units.

Technology Solutions

McKesson Technology Solutions (MTS) provides software solutions, services and consulting to hospitals, physician offices, imaging centers, home health care agencies, and payers. MTS also provides connectivity services that streamline clinical, financial, and administrative communication between patients, providers, payers, pharmacies, and financial institutions. MTS solutions are designed to improve patient safety, reduce the cost and variability of care, improve health care efficiency, and better manage revenue streams and resources.

MTS consists of the McKesson Health Solutions, Imaging and Workflow Solutions, Connected Care and Analytics, Business Performance Solutions, and Enterprise Information Solutions business units.

[Intentionally Blank]

McKesson Enterprise Structure

Description of Services Provided

McKesson ETS system provides end-to-end information technology (IT) services and solutions to McKesson business units and employees, including support and infrastructure for technology solutions the business units deliver to McKesson customers.

For employees, McKesson ETS supports McKesson's IT and services, including the McKesson's technology infrastructure, IT support desk, Internet access, and e-mail, as well as business systems like SAP and human resource information system (HRIS).

McKesson ETS has demonstrated experience in developing, sustaining, and growing operational services for customers, and is driven by continuous operational improvement programs and initiatives. Furthermore, McKesson ETS has developed the infrastructure and required managed services to operate complex network and system environments in support of its internal and external customers.

McKesson ETS' portfolio is composed of a range of solutions, such as data center, network, security, server (operating system), and application (e.g., Web services) services. Customers can choose from a variety of solutions depending on their technical requirements (i.e., reliability, performance, security, and support) and the cost associated with the selected services. This approach allows customers to subscribe to solutions that reflect their business and technical requirements while providing the flexibility of managing risk against cost.

The services provided by McKesson ETS are supported by personnel located in various locations, including San Francisco, California (Corporate Headquarters); Rancho Cordova, California (Drohan Data Center (Drohan)); and Atlanta, Georgia (North Druid Hills 1 Data Center (NDH1)). Drohan and NDH1 are the primary McKesson ETS data centers that are managed and operated by McKesson ETS personnel. The aforementioned locations are in scope for the purposes of this report.

The following are the services and capabilities that are available and provided to customers by the McKesson ETS organization:

- **Colocation —** Facility services for systems installed within one of McKesson ETS's enterprise data centers. Services provided include space, power, cooling, physical security, fire suppression, outbound network firewalls, environmental controls, and facility plan operations.
- **Data Center —** Provides customers with server hosting and administration services. These services include maintaining the computing environment to be compliant with relevant security, compliance, and audit standards.
- **Hosting Services —** Provides server hosting to customers or access to hosted Application Service Provider applications. Services by the Hosting Services team include the ongoing engineering, administration, management, and certification of hardware infrastructure for applications and solutions.
- **IAAS —** Provides infrastructure as a service at a simple cost structure for managing customer applications and servers.
- **Network —** Provides network services (including local area network (LAN)/wide area network service offerings, corporate virtual private network (VPN), and Econolink) to McKesson customers

System Boundaries

As outlined in TSP section 100, *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy,* a system is designed, implemented, and operated to achieve specific business objectives (for example, delivery of services, production of goods) in accordance with management-specified requirements. The purpose of the system description is to delineate the boundaries of the system, which includes the services outlined above and the five components described below: infrastructure, software, people, procedures and data.

Infrastructure and Software

The production information systems are located the Drohan and NDH1 data centers used to by McKesson ETS to support McKesson business units. The ETS environment consists of various operating systems, including Microsoft Windows Server, CentOS Linux, and databases, including Oracle and Microsoft SQL. The environment is composed of virtual servers, with Citrix and VMWare hypervisors managing the virtualized environments. External connections to the environment are only permitted through the use of the McKesson access portal, which requires the use of a password and an RSA token that is installed on an individual's machine. IPSoft is used for enterprise monitoring and alerting.

The in-scope infrastructure consists of multiple applications, operating system platforms and databases, as shown in the table below:

Primary Infrastructure			
Production System	**Business Function Description**	**Operating System Platform**	**Physical Location**
Production information systems	Physical and virtual hosts that provide the infrastructure for ETS services	Microsoft Windows Server	Drohan Data Center
		CentOS Linux	NDH1 Data Center
		Mainframe	

Primary Infrastructure			
Production System	**Business Function Description**	**Operating System Platform**	**Physical Location**
Opsware	Configuration management tool utilized for	Windows	
McAfee Antivirus	Third-party antivirus tool utilized for scanning of network-attached Windows systems		
Remedy ticketing system	Automated ticketing system utilized for documentation and tracking of changes and data backups		
SupportNow ticketing system	Automated ticketing system utilized for reporting and documenting security incidents		
IPCenter	System performance and network monitoring tools utilized for detecting, recording, and reporting of events based on configured thresholds.		
Smarts			
Palo Alto Networks	Intrusion prevent system (IPS) for detection analysis and reporting of network events		

People

- Executive management – responsible for overseeing company-wide activities, establishing and accomplishing goals, and overseeing objectives.
- IT Department – manages, monitors and supports user entities' information and systems from unauthorized access and use while maintaining integrity and availability.

Procedures

Access Authentication and Authorization

Multiple layers of authentication are required to access customer systems within the McKesson ETS environment. The first level of authentication requires a user account and token password to access the McKesson VPN. The second level of access requires a user account and password to authenticate to the McKesson internal network. The third layer of access requires a user account and password to authenticate to a customer server.

Access and administration of logical security for systems under McKesson ETS administrative authority rely upon user IDs and passwords to authenticate users to systems and devices, as well as to authorize the level of access for the user. As this control is a primary component of the McKesson ETS security strategy, McKesson ETS has developed and implemented explicit password policies. Where possible, security controls built into system, such as specified characteristics and expiration, are used to enforce the password standards. In other cases, McKesson ETS employees are responsible for implementing the appropriate standards on passwords for which they have responsibility. For users with sensitive or privileged access, such as system or security administration functions, stronger password standards have been designed and implemented. Key standards within the McKesson ETS password policy are:

- Passwords must be a minimum of eight alpha-numeric characters using both upper and lowercase letters.
- Passwords must be changed every three months to a new and unique password.
- When possible, passwords should include numbers and/or symbols/special characters.
- Passwords must not be coded into login scripts, dial-in communications programs, browsers, or any executable program or file.

- When an account is created, it must be assigned a random and secure password that must be preset to expire upon login. The password can be generated by the system or by the creator of the account. The password assignments must be unique to each user, and the user must be forced to change the password upon login.
- After five consecutive incorrect password attempts are entered, the system will lock out the user's account.
- Users must not be able to construct passwords that are identical passwords they have previously employed in the last five times they have changed their password. User selections for new passwords must be checked against the history and rejected if there is a match.

Access Requests and Access Revocation

The granting or modification of system access privileges is requested through the shared service catalog application. If access is requested by the new or existing user's manager, the request is automatically approved through the McKesson ETS shared service catalog. The McKesson ETS security operations team manages the requests sent through the shared service catalog and provides general access for the various technical teams within the organization (e.g., Windows, Unix, ASP, Mainframe). Specific access to local servers or other system resources may be provisioned by the individual technical teams, but is performed on a limited basis and is accompanied by a ticket documenting the implementation. Once the request has been submitted, the McKesson ETS shared service catalog automatically notifies and sends the access request to the requestor's manager for review and approval. After management approval is obtained, the database administration (DBA) team creates a change ticket to implement access, and then subsequently provisions the specified access privileges. User IDs and one-time unique passwords are randomly generated and provided to the user via e-mail using workflow applications. First time passwords are generated leveraging known data elements from the user's profile so they are not transmitted in clear text (e.g., assignment of the first five numbers in a supplied password from a user's home zip code and the last four numbers from the user's Social Security Number (SSN)).If super user access to a specific platform (e.g., Unix "root" access) is required, the user's manager completes the "Super User — System Access Request" form in the service catalog and submits it to the Security Operations team. Once the form has been received with the manager's approval, the appropriate System Administrator creates a super user ID or "SID" for the user. Access to sensitive system utilities and resources are restricted to authorized individuals based on their job responsibilities.

Unix root access is provisioned by the Unix System Administration (USA) team, however most elevated privileges in UNIX leverage the sudo functionality and that access is also managed and provisioned by the USA team.

Unix root access is provisioned by the Unix system administration (USA) team. Elevated privileges in Unix leverage the sudo functionality. Sudoer access is managed and provisioned by the USA team. For users who require administrative (local or domain) access to a Windows production server, the user's manager completes the "Super User — System Access Request" form in the service catalog and submits it to the security operations team. Once the form has been received with the manager's approval, a system administrator creates a SID for the user. If a user requires temporary access to a production server, a change request is initiated through the ticketing system. The user or requestor is required to detail the reason for the access, the affected servers, and the timeline of the project that requires administrative capabilities. The approval process follows the standard McKesson ETS change management process. If a user requires permanent access, an incident ticket is created within the ticketing system and assigned to the Windows systems administration (WSA) group through the general McKesson ETS incident management process.

Periodic User Access Review

In accordance with frequency defined in established McKesson ETS policies and procedures, sensitive and privileged access privileges associated with system users are reviewed for appropriateness on a periodic basis for each technical area within the McKesson ETS organization. The user access review is performed separately by each technical team (usually management-level personnel). The review process for the McKesson ETS technical teams is described in detail below:

Windows

A review of privileged users is performed on a quarterly basis by the system manager and system administrator for Windows-based systems and servers. Privileged access is restricted to the appropriate individuals within the

windows implementation engineering, WSA, and storage administration (USS) teams. Once the user access review is completed, any required changes are formally documented and sent to the McKesson ETS system operations team for immediate disabling or removal of the requested access. A completion notification is subsequently sent to the reviewers once the access has been disabled or removed.

Unix/Linux

A review of privileged users is performed on a quarterly basis by the Unix manager and Unix technical lead for Unix-based systems and servers. Privileged access is restricted to appropriate individuals within the storage implementation engineering, Unix DBA, enterprise systems management, information security administration, middleware, OPS, USA, and USS teams. Once the user access review has been completed, any required changes are formally documented and sent to the McKesson ETS system operations team for immediate disabling or removal of the requested access. A completion notification is subsequently sent to the reviewers once the access has been disabled or removed.

Mainframe

A review of privileged users is performed on a monthly basis by the RACF group owners. Privileged access is restricted to appropriate individuals within the system administration, OPS, and information security teams. Once the user access review has been completed, any required changes are formally documented and sent to the McKesson ETS system operations team for immediate disabling or removal of the requested access. A completion notification is subsequently sent to the reviewers once the access has been disabled or removed. In addition to the aforementioned, manual monthly reports are generated for the security and operations users groups. Members of these groups must respond to e-mails providing notification of current status.

Network Security

A review of users with privileged access to network devices is performed on a biannual basis during SOX self-assessment process. Privileged access should be restricted to appropriate individuals within the network engineering team. Once the user access review has been completed, any required changes are formally documented and reflected within the Opsware configuration management application by the appropriate network administrator.

Antivirus

McKesson ETS has licensed and implemented a third party antivirus product to scan network-attached Windows systems. At a minimum, daily updates of antivirus signature files are pushed to the managed systems to ensure the maximum effectiveness of the antivirus software and solution.

When an employee is terminated from the company, HR or the terminated employee's manager enters the termination date within the HRMS system, which automatically disables the employee's domain or network account and remote access the evening of the entered date via an automated process. Access to single-sign-on enabled applications such as shared services catalog, Remedy ticketing system, PeopleSoft HRMS, and McKesson intranet (internal employee portal) is also disabled. A daily termination report is also sent by PeopleSoft to the McKesson ETS security operations team and the various technical teams. Furthermore, the terminated employee's manager is prompted to review a termination checklist to ensure that any physical or informational assets (e.g., PDA, CDs, and badges) are collected from the employee. Once the termination checklist has been completed, the terminated employee's manager returns it to the HR team for retention purposes.

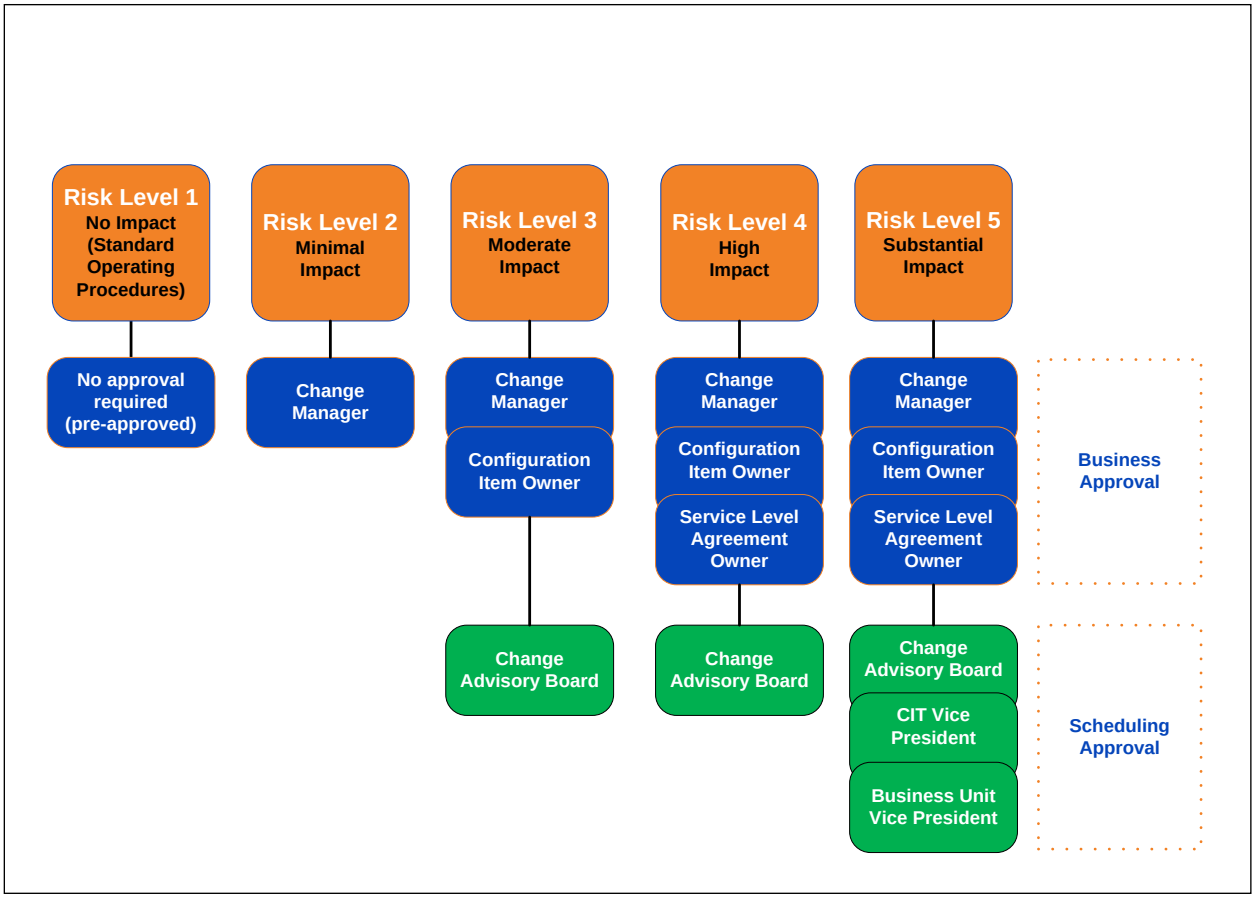
Change Management

McKesson IT has developed formal policies and procedures over the change management process, which requires system software, hardware, database, and network changes to be approved, tested, implemented, and documented.

Any representative of McKesson IT or a McKesson business unit can initiate a change request within the Remedy ticketing system. Once logged into the ticketing system, the requestor completes the relevant change information, assigns the ticket to the applicable technical group, and submits the change request. The ticketing system automatically assigns a unique tracking number to the ticket and systematically designates the appropriate individual(s) to approve the change. Further, the ticketing system lists the approvers' e-mail

addresses and sends a notification informing the approver of the change request. Once the ticket is routed to the change approver(s), a review is performed to evaluate and confirm the level of risk, impact, and priority associated with the change. Change approvers may be different depending on the technical group(s) that is impacted by the change. Additionally, multiple change approvers may be required based on the defined risk level associated with a change request, based on the risk and approval structure referenced below:

McKesson IT Change Management Risk and Approval Structure



Standard operating procedures (SOPs), such as a domain name system (DNS) change, are defined and formally documented as small routine changes that do not pose a financial or operational risk to the McKesson IT organization and its customers. Due to the low risk and impact associated with SOPs, a formal change approval is not required prior to production implementation. SOP changes are preapproved by applicable management personnel. Additionally, testing over SOPs have been benchmarked, and therefore, additional testing is not required for subsequent changes that occur. Changes are tested by individual(s) or group(s) depending on the type of change, and the results are captured within an e-mail or the ticket associated with the change, in accordance with change management policies and procedures. Changes categorized as Level 3 require testing. Issues identified during the testing are captured as needed in the ticket and resolved by the change owner prior to implementing the change.

Approvers have the authority to accept or reject a change. If rejected, the Remedy system automatically sends a notification to the requestor, who closes out the ticket and works with the change approver to determine the cause of the rejection. If approved, the change request is carried out and completed, and is tested by the IT, business, or quality assurance (QA) personnel to ensure that the change is operating as intended or specified by the requestor.

Since SOP-related changes do not require a real-time approval, the change facilitator (a designated technical team member) verifies that the change was preapproved prior to production implementation.

Development, test, and production environments are logically and/or physically separated, per established policies or customer specific SLAs. If the creation of a testing environment is not feasible (i.e., mainframe platforms), testing is performed in the development environment by restricting access to authorized testers only.

Management has established a change advisory board (CAB), which reviews and approves change requests with an associated risk level of 3, 4, or 5. If the risk level of the change is 1 or 2, the change does not require CAB approval. The CAB meets weekly to discuss, approve, and schedule the implementation date for proposed changes, and to review the status of past changes. Proposed changes are tested prior to being presented to the CAB for approval. The CAB approval is documented within the ticket. Changes with a risk level of 5 also require an approval from the McKesson IT vice president and vice president of the impacted business unit. Once the change has received required approvals, it is scheduled for implementation (i.e., "implementation in progress" status in Remedy) and a notice is automatically sent to the impacted or affected parties identified within the ticket.

A detailed implementation plan, including a back-out plan where applicable, is also documented within the ticket. The change is then implemented by an individual or group separate from the resource that performed or completed the change. Access to implement a change in production is restricted to the migration or operations team. Once the change has been successfully implemented, the ticket is closed by the requestor or a technical team member.

Emergency changes can result due to various reasons, such as system outages, software problems, or hardware failures. Emergency changes are implemented prior to a ticket being opened and completed. Due to the time sensitivity associated with emergency changes, approvals are provided verbally prior to the implementation; however, a Remedy ticket, including the documentation of approvals, testing, and other relevant information, is completed within 24 hours of the emergency change implementation.

System Patch Management

Notification of new vendor patches, service packs, bug fixes, or security alerts are received by the McKesson IT organization through various channels. McKesson IT technical teams subscribe to major vendors who regularly notify the applicable teams of new system updates or security-related information. Additionally, regular monitoring of vendor websites is performed by the McKesson IT technical team members to determine the availability of new system updates, threats, and/or vulnerabilities. The McKesson IT information security and risk management team also distributes periodic e-mails to the various technical teams of security-related threats and vulnerabilities that may potentially impact the McKesson IT infrastructure or environment.

If a system update is deemed necessary, the impacted team follows the general McKesson IT change management process, described above, which requires a documented approval and testing within the Remedy system.

Notifications of network-specific patches are received either through vendor alerts, software age and vulnerability reports, or through a request made within the central network SharePoint site. Once the patch notification or request has been received by McKesson IT, the Standards Committee assigns the subject matter expert (SME) to perform an initial review of the patch. The SME determines whether the patch is relevant and whether it will have an impact on the current infrastructure and environment. The analysis performed by the SME is subsequently sent to the standards committee, who reviews the conclusion of the analysis and determines whether to approve the patch. If rejected, the standards committee contacts the requestor and the applicable stakeholders. If approved, a "preliminary standard" (i.e., patching strategy) is published in the SharePoint site by the SME.

Once published, the requestor and applicable target groups (e.g., Microsoft Windows and Unix) and stakeholders review the preliminary standard and determine whether to approve it or not. If rejected, the SME responds to the feedback provided by the reviewers and reinitiates the process. If approved, the preliminary standard is relabeled as a "standard" and the patch is implemented. A notification is sent to the affected parties once the patching process has been completed.

Physical and Environmental Security

The McKesson ETS environment is housed in two primary data center facilities, which are geographically separated to protect against natural disasters.

The data centers are manned 24 hours a day, seven days a week, by the Data Center team, which includes dedicated security personnel. In addition, the data centers are located in unmarked buildings to protect their identity and reduce the risk of intentional attacks.

Formal access procedures exist for controlling physical access to the data centers. Entrants to the data center, whether McKesson ETS employees, visitors, or contractors, must identify themselves and show proof of identity. Proof of identity is a photo ID issued by McKesson or a governmental entity. Only escorted visitors, McKesson ETS employees, and authorized contractors are allowed admittance into the data centers. In addition to a valid proof of identify, visitors are required to provide a written record containing the date, time in, time out, and purpose of the visit. Visitors are also required to review the Data Center Access Policy prior to accessing the data center. Evidence of review is captured via a signature in the visitor's log. Once a visitor has signed in, the visitor is provided with a temporary badge and is escorted by a McKesson ETS employee throughout the duration of the visit.

Access to the data center, including restricted and secured areas (e.g., raised floor), requires approval from an authorized Data Center employee. Only McKesson ETS employees and authorized contractors who permanently work at the data center are granted access to the raised-floor area.

Data Backup & Disaster Recovery

McKesson ETS utilizes a combination of disk and tape backups to protect internal and customer data. Backups of customer data take place using dedicated backup servers and tape libraries. Backups of databases and file systems are performed according to formal procedures and/or the requirements and guidelines established within a customer's SLA. The standard backup schedule is daily for production servers. Any failures that occur during a database or file system backup are reviewed and resolved by the Operations team immediately or during the next business day. A Remedy ticket is opened for each backup failure to document and track the identified issues to resolution.

A contracted third party service provider performs secure transportation of the backups between the data center location and the tape storage location each day, in addition to providing off-site data storage services. Backup tapes transported by the third party, utilize dedicated transport containers and have scheduled times for pick-up and delivery.

Before tapes are picked up by the third party, operations personnel scan the bar code label of each tape to produce a shipping list that is sent to the third party electronically. A hard copy of the shipping list is also included in the shipment. When the third party receives the physical tape shipment, the tape bar code labels are scanned and compared to the shipping list that was sent electronically by the Drohan or NDH1 data centers. A notification is sent to operations personnel if any expected tapes were missing or if any unexpected tapes were included in the shipment.

Before tapes are shipped back to the data centers, the above process is repeated with the third party organization performing the preliminary scan of the tapes and providing the operations team with both electronic and hard-copy formats of the shipping list. Upon receipt at the data centers, the tape bar code labels are scanned and reconciled to the shipping list. If any expected tapes are missing or if any unexpected tapes are received, the third party is subsequently notified. The off-site rotation period is 14 days for daily backup tapes, three years for monthly backup tapes, and seven years for yearly backup tapes.

The McKesson IT Service Continuity Office assists customers in developing and implementing an IT Service Continuity Management (SCM) System, which includes a series of IT business continuity and disaster recovery-related processes and solutions that are monitored, reviewed, and improved on a reoccurring basis. IT SCM includes 1) establishing IT business continuity and disaster recovery objectives; 2) defining customer requirements through a business impact analysis; 3) identifying and implementing the appropriate and relevant continuity and recovery strategies; and 4) performing program management activities, such as training, program maintenance, exercising/testing, etc. The IT SCM establishes and maintains processes and solutions designed to protect the customer's people, workplaces, and the continuity of critical business processes from natural disasters, operational incidents, accidents, and human-caused threats. Specific program objectives include:

- Contributing to the health and safety of McKesson's employees and customers
- Protecting key revenue streams

- Strengthening competitive positioning, market share, and organizational reputation
- Maintaining productivity
- Assuring legal and regulatory compliance
- Reducing continuity and availability risks and security threats to an appropriate level
- Enabling organizational certification goals and objectives

The categories and activities described above align to international practices and are consistent with the Plan-Do-Check-Act model found in other management systems (including ISO 27001).

Incident Management

McKesson ETS has developed and implemented a formal incident management and resolution process, which is used to manage various types of incidents, such as connectivity problems, account lockouts, PC or laptop issues, and security events (e.g., intrusion and privilege abuse, malicious code, denial of service, unauthorized access, theft, or electronic information).

If an incident is identified, a ticket is automatically generated within the Remedy system or is manually opened by the McKesson SupportNow Help Desk ("Help Desk") or Operations personnel (system alerts). Once generated, the Help Desk reviews the ticket summary and determines the impact and priority level of the incident. Depending on the impact or severity rating of the incident associated with the ticket, the incident is internally resolved by the Help Desk or assigned to the designated technical or support group for resolution. Remedy is systematically configured to route an incident ticket to a designated group based on the type of incident reported. If the impact level of the incident is high or catastrophic, multiple departmental teams (e.g., Corporate Legal Team), as well as senior and executive-level personnel, are involved with the management, resolution, and communication of the incident.

Once the Remedy ticket has been assigned or routed to the designated group, an analysis or investigation is performed to determine the root cause of the incident. Based on the results of the analysis or investigation, the recovery or resolution plan is created and implemented to resolve the incident. The analysis and decisions, including the summary of the incident, actions taken by the incident responders, contact information of involved parties, and incident resolution date, are documented within or are attached to the Remedy ticket for reference purposes.

For non-security related incidents, a Daily Operations Meeting (DOM) is held with the Incident Management and Operations team to review and determine the risk and criticality associated with incident tickets with a high-impact level. As part of the meeting, the root cause and impact of each incident is discussed and the next steps are determined to resolve the incident. In addition to the DOM, the Security Incident Response Team generates monthly and quarterly reports that detail past and current security incidents. The reports are provided to the chief

information security officer, who determines whether any security related threats or trends exist within the Company's environment.

System Monitoring

Security monitoring applications and manual reviews are utilized to monitor and analyze the systems for noncompliance with security policies and possible or actual security breaches.

- Firewall: Firewalls are in place at various network entry points to monitor incoming and outgoing network traffic. The firewall filters and analyzes the data packets and determines whether traffic is allowed through or not, based on a predetermined rule sets.
- Network Monitoring: McKesson utilizes an IPS to analyze and report network events. Additionally, McKesson use various applications, such as IPCenter and Smarts, are installed and used to monitor the status and load of each managed network device and, where possible, the connection to the customer's network. The monitoring applications are configured to generate alerts when specified thresholds are reached or exceeded.
- Antivirus: McKesson utilizes McAfee antivirus products to protect Windows servers and Windows workstations. The antivirus software is configured to scan for updates to antivirus definitions and update registered clients on a daily basis. Scanning on the registered clients also occurs daily.

Data

The following table describes the data that is used to support the system and manage the servers and services for the ETS system.

Data Used and Supported by the System		
Data Description	**Data Reporting**	**Classification**
Customer requests	Information provided by customers for the provisioning and modification of services provided	Confidential
Enterprise monitoring system alerts	Information provided by real-time enterprise monitoring applications regarding current system status and health	Confidential
Backup and information security alerts	Automated alert notifications for processes related to data backup monitoring and information security monitoring	Confidential
Incident details	Automated ticketing systems for client reporting of service-related incidents or issues	Confidential
Security reports	Reports provided by third party specialists regarding the security of the system (e.g., vulnerability and penetration test results)	Confidential

Significant Changes During the Review Period

No relevant changes to the ETS system occurred during the review period.

Subservice Organizations

No subservice organizations were included in the scope of this assessment. Therefore, the description does not address the criteria in Section 2, items (a)(i)(4), (a)(i)(5)(b) and (a)(i)(6).

CONTROL ENVIRONMENT

The control environment at McKesson is the foundation for the other areas of internal control. It sets the tone of the organization and influences the control consciousness of its personnel. The components of the control environment factors include the integrity and ethical values, management's commitment to competence; its organizational structure; the assignment of authority and responsibility; and the oversight and direction provided by executive management and operations management.

Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of McKesson's control environment, affecting the design, administration, and monitoring of other components. McKesson management delivers consistent and periodic messages to its employees regarding the value of teamwork, collective versus individual success, the importance of client service versus self-service, and that success for the organization and the individual will not occur as the result of any unethical or deceptive behavior.
Specific control activities that McKesson has implemented in this area include the following:

- Management's commitment to integrity and ethical behavior is demonstrated through the application of the "integrity, customer first, accountability, respect, excellence" (ICARE) principles. ICARE training has been provided to employees and is included as part of new-hire orientation.
- Personnel who violate McKesson's *Code of Business Conduct and Ethics* (the "Code") are subject to disciplinary actions, up to and including immediate termination. The Code is located on the corporate intranet and McKesson's public website. Employees are required to acknowledge that they have read and understand The Code upon hire and annually thereafter.
- A third party service provider administers a company-wide telephone hotline service. The hotline called the McKesson Global Compliance and Ethics Line has a toll-free number in operation 24 hours day, seven days a week, through which employees and others who have suspicions of wrongdoing, illegal or unethical acts, breaches of Company policy, or any form of loss relating to the Company's operations, property, or employees, may file a report.
- Employees participate in ongoing training and certification regarding internal controls and processes.

McKesson business units have a Chief Compliance Officer who oversees the unit's compliance program and helps to ensure compliance with governing laws, contractual obligations, and company ethics.

Board of Directors and Audit Committee Oversight

McKesson control consciousness is influenced significantly by the Board of Directors and Audit Committee.

Specific control activities that McKesson has implemented in this area include the following:

- The board of directors makes an annual determination as to the independence of each of its members. Each year, members are asked by the corporate secretary's office to complete a questionnaire that explores respective histories, stock ownership, and relationships with McKesson. Answers to the questionnaires are reviewed by the corporate secretary's office and relationships or transactions are analyzed by McKesson's lawyers and disclosed, as required, to the board of directors, and to the Company's stockholders in the proxy statement.

- The board of directors has adopted a related-party transactions policy, which establishes standards and a process for evaluating transactions with entities in which directors have involvement.
- The audit committee has a written charter, which is posted on McKesson's website under "Corporate Governance".

Organizational Structure and Assignment of Authority and Responsibility

McKesson's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. McKesson's management believes that establishing a relevant organizational structure includes considering key areas of authority and responsibility and appropriate lines of reporting. McKesson has, therefore, developed an organizational structure that is suited to its needs and is based, in part, on its size and the nature of its activities.

McKesson's assignment of authority and responsibility activities includes factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It also includes policies relating to business practices, knowledge and experience of key personnel, and resources provided for carrying out duties.

In addition, it includes policies and communications directed at ensuring that personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and what they will be held accountable for. Organizational charts are in place to communicate key areas of authority, responsibility, and appropriate lines of reporting to personnel. These charts are communicated to employees and updated as needed.

Commitment to Competence

McKesson's management defines competence as the knowledge and skills necessary to accomplish tasks that define an employee's roles and responsibilities. Among McKesson's stated values are performance, excellence, and continuous improvement; thus, a fundamental aspect of performance measurement is the extent to which McKesson employees pursue and demonstrate a commitment to competence.

Specific control activities that McKesson has implemented in this area include the following:

- Hiring decisions are approved by the human resources department, and personnel are qualified through the hiring process for their assigned level or responsibility.
- Ongoing training is offered through courses in professional and technical development.
- A formal performance management process is in place that includes assessment of performance twice a year based on performance objectives and competencies defined at the beginning of each fiscal year.
- HR personnel perform criminal, credit, educational, and employment background checks on applications as a component of the hiring process.
- Drug testing is performed as a component of the hiring process.

Accountability

McKesson's management philosophy and operating style encompasses a broad range of characteristics. Such characteristics may include the following: management's approach to taking and monitoring business risks; management's attitudes and actions toward financial reporting (conservative or aggressive selection from available alternative accounting principles, and conscientiousness and conservatism with which accounting estimates are developed); and management's attitudes toward information processing, accounting functions, and personnel.

Additionally, McKesson's human resources policies and practices relate to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities.

Specific control activities that McKesson has implemented in these areas include the following:

- Management receives regulatory updates affecting services provided and industry correspondence on an ongoing basis. Management conducts periodic independent internal audits to ensure compliance to internal processes.
- Meetings are conducted on a regular basis to discuss operational issues related to McKesson services.
- A new hire checklist is completed for new employees.
- Termination checklists are completed as a component of the termination process.

RISK ASSESSMENT

Risk Identification

McKesson has placed into operation a risk-assessment process to identify and manage risks that could affect the organization's ability to provide reliable general IT control activities and infrastructure services for customers. This process requires management to identify significant risks in their areas of responsibility and to implement appropriate measures to address those risks. Key stakeholders, including service owners, ETS management, information security and risk management personnel, and executive management, meet on an annual basis to identify and review risks applicable to the services provided. These risks are documented in various means, including spreadsheets and the corporate GRC application.

The risk assessment process has three components: identifying risks; establishing a risk level by determining the likelihood of occurrence and impact; and finally, identifying controls and safeguards that reduce the impact of the risk to an acceptable level. To gather relevant information, the risk management team utilizes a number of techniques, including brainstorming, questionnaires, on-site interviews, and documentation reviews.

Risk Factors

Risks that are considered during management's risk assessment activities include consideration of the following events:

External Factors

- Technological developments
- Changing customer needs or expectations
- New legislation and regulation that could force changes in policies and strategies
- Natural catastrophes that could lead to changes in operations or information systems
- Economic changes that could have an impact on management decisions

Internal Factors

- Significant changes in policies, processes or personnel
- Types of fraud
- Fraud incentives and pressures for employees
- Fraud opportunities
- Employee attitudes and rationalizations for fraud
- A disruption in information systems processing
- The quality of personnel hired and methods of training utilized

- Changes in management responsibilities
- Expanded operations
- Corporate restructurings

Risk Analysis

Risk analysis is an essential process to McKesson ETS' success. It includes identification of key business processes where potential exposures of some consequence exist, as well as significant changes to those processes. Management has implemented a process whereby the likelihood and impact of identified risks are assessed. Once the likelihood and impact of each identified risk have been assessed, management determine a control rating for the risk, based on the type and level of controls and/or management activities that are currently in place to manage the risk. These factors are evaluated to determine the residual risk, which is the exposure to the business after consideration of management and control activities designed and implemented to specifically mitigate a risk. Management then considers how the residual risk should be managed using four risk mitigation strategies:

- Risk Acceptance: management accepts the potential risk and continues operating after performing due diligence of examining the risks and determining the risk level.
- Risk Mitigation: management approves the implementation of controls that lower the risk to an acceptable level. These control activities are documented in the Related Control Activities section below.
- Risk Avoidance: management avoids the risks by eliminating the function or process that could cause the risk.
- Risk Transference: management transfers the risk by using other options to compensate for a loss such as purchasing an insurance policy.

In addition to the above process, the McKesson Internal Audit department performs an annual risk assessment, which covers business units within the McKesson enterprise. Interviews are held with corporate and business unit leadership to identify and determine key objectives, initiatives, challenges, and risks that are being experienced at the business unit and/or enterprise-wide level. Once these interviews have been conducted, the Internal Audit management team compiles a register of the key risks identified (i.e., financial, operational, reputation, compliance, strategic, fraud) and assigns a risk score based on impact, likelihood, and management preparedness. The information compiled within the risk register is subsequently presented and confirmed with business unit leadership (business unit president/general manager and chief financial officer (CFO)/controller) and corporate executives. The Internal Audit management team develops its annual audit plan based on the highest risks identified during this process. The ranking of each risk is internally reevaluated and, if required, recalibrated on a quarterly basis. Additionally, the Vice President of internal audit presents the results of each audit during the quarterly audit committee meetings.

TRUST SERVICES CRITERIA AND RELATED CONTROL ACTIVITIES

Integration with Risk Assessment

Along with assessing risks, management has identified and put into effect actions needed to address those risks. In order to address risks, control activities have been placed into operation to help ensure that the actions are carried out properly and efficiently. Control activities serve as mechanisms for managing the achievement of the security and availability principles.

Selection and Development of Control Activities

The applicable trust criteria and related control activities are included in Section 4 of this report to eliminate the redundancy that would result from listing the items in this section and repeating them in Section 4. Although the applicable trust criteria and related control activities are included in Section 4, they are, nevertheless, an integral part of McKesson's description of the system.

The description of the service auditor's tests of operating effectiveness and the results of those tests are also presented in Section 4, the Testing Matrices, adjacent to the service organization's description of controls. The description of the tests of operating effectiveness and the results of those tests are the responsibility of the service auditor and should be considered information provided by the service auditor.

Trust Services Criteria Not Applicable to the In-Scope System

The Trust Services criteria presented below, are not applicable to the ETS system within the scope of this examination. As a result, an associated control is not required to be in place at the service organization for the omitted applicable trust services criterion. The following table presents the trust services criterion that are not applicable for the ETS system at McKesson. The not applicable trust services criteria are also described within Section 4.

Criteria #	Reason for Omitted Criteria
CC7.1	McKesson ETS does not develop software as a component of its services.

Information and Communication Systems

Relevant Information

Information is necessary for McKesson to carry out internal control responsibilities to support the achievement of its criteria related to the McKesson system. Management obtains or generates and uses relevant and quality information from both internal and external sources to support the functioning of internal control.

The following provides a summary of internal and external sources of information used in the McKesson ETS:

- Real-time environment status and availability information
- Alerts received from enterprise monitoring applications
- Incident information received from customers
- Specific requests for changes from business units or other information received from business units that results in modifications to the production environment
- Information received from third parties, such as security and vulnerability alerts

Communication

Upper management is involved with day-to-day operations and is able to provide personnel with an understanding of their individual roles and responsibilities pertaining to internal controls. This includes the extent to which personnel understand how their activities relate to the work of others and the means of reporting exceptions to a higher level within the Company. McKesson's management believes that open communication channels helps make sure exceptions are reported and acted upon. For that reason, formal communication applications, such as organizational charts and employee handbooks, are in place.

Management's communication activities are made electronically, verbally, and through the actions of management.

Specific control activities that McKesson has implemented in this area include the following:

- The corporate communications department determines the forms of communication utilized for the type and timeliness of disseminating information throughout McKesson.
- Communications with regulators are managed by the executive vice president, the CFO, the controller, and general counsel. This senior team of executives reviews incoming communications and the Company's responses for appropriateness and accuracy before they are submitted to regulators.
- Communications to McKesson stockholders are handled by the investor relations department and the Corporate Secretary's office.

MONITORING

Monitoring is a process that assesses the quality of internal control performance over time. It involves assessing the design and operation of controls and taking necessary corrective actions. This process is accomplished through ongoing activities, separate evaluation, or a combination of the two. Monitoring activities also include using information from communications from external parties such as user entity complaints and regulatory comments that may indicate problems or highlight areas in need of improvement. Management has implemented a self-assessment and compliance program to ensure the controls are consistently applied as designed.

Separate Evaluations

Management has implemented a self-assessment program to evaluate the performance of specific control activities and processes over time, and confirm that the in-scope controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority. As a result of management's risk analysis process, each control activity within scope has been assigned a risk level associated with the assessed level of risk it is intended to mitigate. Controls that serve to mitigate multiple risks are assigned the highest level of assessed risk among the pertinent risks.

Internal and External Auditing

McKesson supports many user entities in their efforts to meet the regulatory demands of their industry or governing agency. McKesson has assisted user entities in successfully meeting the requirements of many certifications and regulatory demands, including (remove or add to the listing):

- Sarbanes-Oxley (SOX)
- Internal audits
- Business unit reviews
- Payment Card Industry Data Security Standard (PCI DSS)
- ISO/IEC 27001

Reporting Deficiencies

The nature, timing and extent of the self-assessment tests and results are documented by the self-assessors, for management review. Deviations or deficiencies associated with controls are escalated to management for immediate correction action, when required.

COMPLEMENTARY CONTROLS AT USER ENTITIES

Complementary user entity controls are not required, or significant, to achieve the applicable trust services criteria. Therefore, the description does not address the (a)(i)(5)(a) criteria in Section 2.

SECTION 4

TESTING MATRICES

TESTS OF OPERATING EFFECTIVENESS AND RESULTS OF TESTS

Scope of Testing

This report on the controls relates to the ETS system provided by McKesson. The scope of the testing was restricted to the ETS system and its boundaries as defined in Section 3. Schellman conducted the examination testing over the period of January 1, 2016, to September 30, 2016.

Tests of Operating Effectiveness

The tests applied to test the operating effectiveness of controls are listed alongside each of the respective control activities within the Testing Matrices. Such tests were considered necessary to evaluate whether the controls were sufficient to provide reasonable, but not absolute, assurance that the applicable trust services criteria were achieved during the review period. In selecting the tests of controls, Schellman considered various factors including, but not limited to, the following:

- The nature of the control and the frequency with which it operates;
- The control risk mitigated by the control;
- The effectiveness of entity-level controls, especially controls that monitor other controls;
- The degree to which the control relies on the effectiveness of other controls;
- Whether the control is manually performed or automated;

The types of tests performed with respect to the operational effectiveness of the control activities detailed in this section are briefly described below:

Test Approach	Description
Inquiry	Inquired of relevant personnel with the requisite knowledge and experience regarding the performance and application of the related control activity. This included in-person interviews, telephone calls, e-mails, web-based conferences, or a combination of the preceding.
Observation	Observed the relevant processes or procedures during fieldwork. This included, but was not limited to, witnessing the performance of controls or evidence of control performance with relevant personnel, systems, or locations relevant to the performance of control policies and procedures.
Inspection	Inspected the relevant audit records. This included, but was not limited to, documents, system configurations and settings, or the existence of sampling attributes, such as signatures, approvals, or logged events. In some cases, inspection testing involved tracing events forward to consequent system documentation or processes (e.g. resolution, detailed documentation, alarms, etc.) or vouching backwards for prerequisite events (e.g. approvals, authorizations, etc.).

Sampling

Consistent with American Institute of Certified Public Accountants (AICPA) authoritative literature, Schellman utilizes professional judgment to consider the tolerable deviation rate, the expected deviation rate, the audit risk, the characteristics of the population, and other factors, in order to determine the number of items to be selected in a sample for a particular test. Schellman, in accordance with AICPA authoritative literature, selected samples in such a way that the samples were expected to be representative of the population. This included judgmental selection methods, where applicable, to ensure representative samples were obtained.

System-generated population listings were obtained whenever possible to ensure completeness prior to selecting samples. In some instances, full populations were tested in cases including but not limited to, the uniqueness of the event or low overall population size.

Test Results

The results of each test applied are listed alongside each respective test applied within the Testing Matrices. Test results not deemed as control deviations are noted by the phrase "No exceptions noted." in the test result column of the Testing Matrices. Any phrase other than the aforementioned, constitutes either a test result that is the result of non-occurrence, a change in the application of the control activity, or a deficiency in the operating effectiveness of the control activity. Testing deviations identified within the Testing Matrices are not necessarily weaknesses in the total system of controls, as this determination can only be made after consideration of controls in place at user entities and subservice organizations, if applicable, and other factors.

SECURITY PRINCIPLE AND CRITERIA TABLE

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.0: Common Criteria Related to Organization and Management			
CC1.1: The entity has defined organizational structures, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system enabling it to meet its commitments and requirements as they relate to security and availability.			
CC1.1.1	Roles and responsibilities are defined in written job descriptions by management.	Inspected the documented position description detail for a sample of employment positions to determine that roles and responsibilities were defined in written job descriptions for each employment position sampled.	No exceptions noted.
CC1.1.2	Reporting relationships and organizational structures are documented in organizational charts that are communicated to personnel and reviewed periodically by senior management as part of organizational planning and adjusted as needed based on changing entity commitments and requirements.	Inquired of the manager of IT compliance regarding organizational management to determine that organizational charts were in place and communicated to employees and updated as needed.	No exceptions noted.
		Observed the organizational charts on the company Intranet to determine that organizational charts were communicated to employees via the company Intranet.	No exceptions noted.
		Inspected the company organizational charts to determine that organizational charts were in place to communicate the defined key areas of authority, responsibility and lines of reporting to personnel related to the design, development, implementation, operation, maintenance, and monitoring of the system.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.2: Responsibility and accountability for designing, developing, implementing, operating, maintaining, monitoring, and approving the entity's system controls are assigned to individuals within the entity with authority to ensure policies, and other system requirements are effectively promulgated and placed in operations.			
CC1.2.1	Roles and responsibilities are defined in written job descriptions by management.	Inspected the documented position description detail for a sample of employment positions to determine that roles and responsibilities were defined in written job descriptions for each employment position sampled.	No exceptions noted.
CC1.2.2	Documented information security policies and procedures are in place that outline requirements and expectations related to safeguarding data and information assets.	Inspected the information security management policies and procedures to determine that formal policies and procedures define the requirements and expectations related to safeguarding data and information assets.	No exceptions noted.
CC1.2.3	Responsibility for the content of the entity security policies and procedures has been assigned to ISRM.	Inspected the information security management policies and procedures to determine that the responsibility for the information security management policies was assigned to ISRM.	No exceptions noted.
CC1.3: Personnel responsible for designing, developing, implementing, operating, maintaining, and monitoring of the system affecting security and availability have the qualifications and resources to fulfill their responsibilities.			
CC1.3.1	Roles and responsibilities are defined in written job descriptions by management.	Inspected the documented position description detail for a sample of employment positions to determine that roles and responsibilities were defined in written job descriptions for each employment position sampled.	No exceptions noted.
CC1.3.2	New employee hiring procedures are in place to guide the hiring process and include verification that candidates possess the required qualifications to perform the job duties and that a new hire checklist is completed.	Inspected the new employee hiring policies and procedures to determine that new employee hiring procedures were in place to guide the hiring process and included verification that candidates possessed the required qualifications to perform the job duties.	No exceptions noted.
CC1.3.3	Training courses and material are available to employees to maintain and advance the skill level of personnel.	Inspected training policy documentation to determine that training opportunities were available to employees to maintain and advance the skill level of personnel.	No exceptions noted.
		Inspected example training documentation to determine that training courses and material were available to employees to maintain and advance the skill level of personnel.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.3.4	Personnel competence to fulfill their responsibilities is evaluated through the annual performance evaluation process.	Inspected the annual performance evaluations for a sample of active employees to determine that each employee sampled was evaluated on their competence to fulfill their responsibilities.	No exceptions noted.
CC1.3.5	On an annual basis, personnel are required to complete compliance training to reaffirm understanding of confidentiality and privacy practices.	Inspected the compliance training detail for a sample of employees to determine that compliance training was completed during the review period for each employee sampled.	The test of control activity disclosed that compliance training was not evidenced during the review period for four of the 25 employees sampled.
CC1.4: The entity has established workplace conduct standards, implemented workplace candidate background screening procedures, and conducts enforcement procedures to enable it to meet its commitments and requirements as they relate to security and availability.			
CC1.4.1	Workplace conduct standards are documented in a formal code of conduct document.	Inspected the code of conduct standards to determine that the workplace conduct standards were documented in a formal code of conduct document.	No exceptions noted.
CC1.4.2	Personnel sign the code of conduct and the statement of confidentiality and privacy practices upon their hire.	Inspected the code of conduct and the statement of confidentiality and privacy for a sample of employees hired during the review period to determine that each employee sampled signed the code of conduct and the statement of confidentiality and privacy practices.	No exceptions noted.
CC1.4.3	An anonymous third party administered ethics hotline is in place to monitor employees' compliance with the code of conduct.	Inspected the landing page detail of the anonymous third party administered ethics hotline website to determine that an anonymous third party administered ethics hotline was in place to monitor employees' compliance with the code of conduct.	No exceptions noted.
CC1.4.4	Criminal background check are completed for employees as a component of the hiring process.	Inspected criminal background check documentation for a sample of employees hired during the review period to determine that criminal background check was completed for each employee sampled.	No exceptions noted.
CC2.0: Common Criteria Related to Communications			
CC2.1: Information regarding the design and operation of the system and its boundaries has been prepared and communicated to authorized internal and external system users to permit users to understand their role in the system and the results of system operation.			
CC2.1.1	A description of the system is posted on the corporate intranet site available to all internal and external users of the system.	Inspected the corporate intranet site to determine that a description of the system was posted on the corporate intranet site and was available to all internal and external users of the system.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.2: The entity's security and availability commitments are communicated to external users, as appropriate, and those commitments and the associated system requirements are communicated to internal system users to enable them to carry out their responsibilities.			
CC2.2.1	The entity's security and availability commitments regarding the system are included in the master services agreement.	Inspected the master service agreements for a sample of vendors to determine that the entity's security and availability commitments regarding the system were included in the master services agreement for each vendor sampled.	No exceptions noted.
CC2.2.2	Personnel are required to sign the code of conduct and the statement of confidentiality and privacy practices upon their hire.	Inspected the code of conduct and the statement of confidentiality and privacy for a sample of employees hired during the review period to determine that each employee sampled signed the code of conduct and the statement of confidentiality and privacy practices.	No exceptions noted.
CC2.2.3	On an annual basis, personnel are required to complete compliance training to reaffirm understanding of confidentiality and privacy practices.	Inspected the compliance training detail for a sample of employees to determine that compliance training was completed during the review period for each employee sampled.	Refer to the test results for control activity CC1.3.5.
CC2.2.4	An anonymous third party administered ethics hotline is in place to monitor employees' compliance with the code of conduct.	Inspected the landing page detail of the anonymous third party administered ethics hotline website to determine that an anonymous third party administered ethics hotline was in place to monitor employees' compliance with the code of conduct.	No exceptions noted.
CC2.3: The entity communicates the responsibilities of internal and external users and others whose roles affect system operation.			
CC2.3.1	Personnel are required to sign the code of conduct and the statement of confidentiality and privacy practices upon their hire.	Inspected the code of conduct and the statement of confidentiality and privacy for a sample of employees hired during the review period to determine that each employee sampled signed the code of conduct and the statement of confidentiality and privacy practices.	No exceptions noted.
CC2.3.2	An anonymous third party administered ethics hotline is in place to monitor employees' compliance with the code of conduct.	Inspected the landing page detail of the anonymous third party administered ethics hotline website to determine that an anonymous third party administered ethics hotline was in place to monitor employees' compliance with the code of conduct.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.4: Internal and external personnel with responsibility for designing, developing, implementing, operating, maintaining, and monitoring controls, relevant to the security and availability of the system, have the information necessary to carry out those responsibilities.			
CC2.4.1	Policy and procedures documents for processes, which include responsibility for reporting operational failures, incidents, system problems, concerns, and user complaints (and the process for doing so) are published and available on the intranet.	Inspected the intranet site to determine that policy and procedure documents for processes were published on the intranet site.	No exceptions noted.
CC2.5: Internal and external system users have been provided with information on how to report security and availability failures, incidents, concerns, and other complaints to appropriate personnel.			
CC2.5.1	Policy and procedures documents for processes, which include responsibility for reporting operational failures, incidents, system problems, concerns, and user complaints (and the process for doing so) are published and available on the intranet.	Inspected the intranet site to determine that policy and procedure documents for processes were published on the intranet site.	No exceptions noted.
CC2.5.2	An anonymous third party administered ethics hotline is in place to monitor employees' compliance with the code of conduct.	Inspected the landing page detail of the anonymous third party administered ethics hotline website to determine that an anonymous third party administered ethics hotline was in place to monitor employees' compliance with the code of conduct.	No exceptions noted.
CC2.6: System changes that affect internal and external system user responsibilities or the entity's commitments and requirements relevant to security and availability are communicated to those users in a timely manner.			
CC2.6.1	The system change calendar that describes changes to be implemented is posted on the corporate intranet site.	Inspected the corporate intranet site to determine that the system change calendar that described changes to be implemented was posted on the corporate intranet site.	No exceptions noted.
CC2.6.2	System changes affecting availability and security that affect the entire organization are communicated to internal users through e-mail as part of the implementation process.	Inspected an example system change e-mail to determine that system changes that related to availability and security were communicated to internal users through e-mail as part of the implementation process.	No exceptions noted.
CC3.0: Common Criteria Related to Risk Management and Design and Implementation of Controls			
CC3.1: The entity (1) identifies potential threats that would impair system security and availability commitments and requirements, (2) analyzes the significance of risks associated with the identified threats, and (3) determines mitigation strategies for those risks (including controls and other mitigation strategies).			
CC3.1.1	Documented policies and procedures are in place to guide personnel when performing the risk assessment process.	Inspected the risk assessment policies and procedures to determine that documented policies and procedures were in place to guide personnel when performing the risk assessment process.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC3.1.2	A formal risk assessment is performed on an annual basis. Risks that are identified are rated using a risk evaluation process and are formally documented.	Inspected the most recent risk assessment to determine that a formal risk assessment was performed during the review period and identified risks were rated using a risk evaluation process and were formally documented.	No exception noted.
CC3.1.3	Infrastructure vulnerability scans are performed on a monthly basis against defined in-scope assets internally and externally.	Inspected the infrastructure vulnerability scan schedules for a sample of months during the review period to determine that scans were performed against defined in scope assets internally and externally for each month sampled.	No exceptions noted.
CC3.1.4	Results from monthly vulnerability scans are reviewed during monthly management meetings and incorporated as necessary into the ongoing risk management process.	Inquired of the IT compliance manager regarding the review of monthly vulnerability scans to determine that scans were reviewed during monthly management meetings and incorporated as necessary into the ongoing risk management process.	No exceptions noted.
		Inspected the management meeting minutes for a sample of months during the review period to determine that meetings were held and monthly vulnerability scans were reviewed during management meetings and incorporated as necessary into the ongoing risk management process for each month sampled.	No exceptions noted.
CC3.2: The entity designs, develops, and implements controls, including policies and procedures, to implement its risk mitigation strategy.			
CC3.2.1	Results from monthly vulnerability scans are reviewed during monthly management meetings and incorporated as necessary into the ongoing risk management process.	Inquired of the IT compliance manager regarding the review of monthly vulnerability scans to determine that scans were reviewed during monthly management meetings and incorporated as necessary into the ongoing risk management process.	No exceptions noted.
		Inspected the management meeting minutes for a sample of months during the review period to determine that meetings were held and monthly vulnerability scans were reviewed during management meetings and incorporated as necessary into the ongoing risk management process for each month sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC3.2.2	Policy and procedures documents for processes, which include responsibility for reporting operational failures, incidents, system problems, concerns, and user complaints (and the process for doing so) are published and available on the intranet.	Inspected the intranet site to determine that policy and procedure documents for processes were published on the intranet site.	No exceptions noted.
CC3.2.3	An ERC ETS integrated findings report is e-mailed to senior executives providing a status of risk assessment findings to date, as well as the associated remediation plans and dates.	Inspected an example ERC ETS integrated findings report to determine that the report was e-mailed to senior executives and tracked findings to date in addition to remediation plans and dates.	No exceptions noted.
CC3.2.4	A formal risk assessment is performed on an annual basis. Risks that are identified are rated using a risk evaluation process and are formally documented.	Inspected the most recent risk assessment to determine that a formal risk assessment was performed during the review period and identified risks were rated using a risk evaluation process and were formally documented.	No exception noted.
CC3.3: The entity (1) identifies and assesses changes (for example, environmental, regulatory, and technological) that could significantly affect the system of internal control for security and availability and reassess risks and mitigation strategies based on the changes and (2) reassesses the suitability of the design and deployment of control activities based on the operation and monitoring of those activities, and updates them as necessary.			
CC3.3.1	Developments in technology and the impact of applicable laws or regulations are considered by senior management as part of the annual risk assessment and IT security planning process.	Inspected the most recent risk assessment to determine that developments in technology and the impact of applicable laws or regulations were considered by senior management as part of the annual risk assessment and IT security planning process.	No exceptions noted.
CC3.3.2	The IT security group receives periodic security notifications and bulletins to monitor the security impact of emerging technologies and the impact of applicable laws or regulations.	Inspected an example security notification and subscription during the review period to determine that the IT security group receives periodic security notifications and bulletins during the review period regarding the security impact of emerging technologies and the impact of applicable laws or regulations.	No exceptions noted.
CC4.0: Common Criteria Related to Monitoring Controls			
CC4.1: The design and operating effectiveness of controls are periodically evaluated against security and availability commitments and requirements. Corrections and other necessary actions relating to identified deficiencies are taken in a timely manner.			
CC4.1.1	A network monitoring application is configured to generate alerts and create incident tickets upon reaching or exceeding configured thresholds. The network control center personnel track tickets from inception to resolution.	Inquired of the director of network engineering regarding network monitoring to determine that incident tickets were monitored from inception to resolution by network control center personnel.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Observed the network monitoring application alert and ticket generation configurations to determine that a network monitoring application was configured to generate alerts and create incident tickets upon reaching or exceeding configured thresholds.	No exceptions noted.
		Inspected the incident ticket detail for a sample of alerts generated by the network monitoring application during the review period to determine that incident tickets were tracked from inception to resolution for each alert sampled.	No exceptions noted.
CC4.1.2	A formal risk assessment is performed on an annual basis. Risks that are identified are rated using a risk evaluation process and are formally documented.	Inspected the most recent risk assessment to determine that a formal risk assessment was performed during the review period and identified risks were rated using a risk evaluation process and were formally documented.	No exception noted.
CC4.1.3	Infrastructure vulnerability scans are performed on a monthly basis against defined in-scope assets internally and externally.	Inspected the infrastructure vulnerability scan schedules for a sample of months during the review period to determine that scans were performed against defined in scope assets internally and externally for each month sampled.	No exceptions noted.
CC4.1.4	Results from monthly vulnerability scans are reviewed during monthly management meetings and incorporated as necessary into the ongoing risk management process.	Inquired of the IT compliance manager regarding the review of monthly vulnerability scans to determine that scans were reviewed during monthly management meetings and incorporated as necessary into the ongoing risk management process.	No exceptions noted.
		Inspected the management meeting minutes for a sample of months during the review period to determine that meetings were held and monthly vulnerability scans were reviewed during management meetings and incorporated as necessary into the ongoing risk management process for each month sampled.	No exceptions noted.
CC4.1.5	An IPS is in place to monitor system traffic for predefined events and changes.	Inspected IPS security profile group configurations to determine that an IPS was in place to monitor system traffic for predefined events and changes.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC4.1.6	The IPS system generates a daily threat report that is reviewed by security personnel.	Inquired of the security operations lead regarding reviews of IPS reports to determine that the IPS system generated a daily threat report that was reviewed by security personnel.	No exceptions noted.
		Inspected an example IPS report to determine that a report containing threats was generated during the review period.	No exceptions noted.
CC5.0: Common Criteria Related to Logical and Physical Access Controls			
CC5.1: Logical access to security software, infrastructure, and architectures have been implemented to support (1) identification and authentication of authorized users; (2) restriction of authorized users access to system components, or portions thereof, authorized by management including hardware, data, software, mobile devices, output, and offline elements; and (3) prevention and detection of unauthorized access.			
CC5.1.1	Formal policies and procedures are in place for the logical access and security processes, including password guidelines and standards.	Inspected the information security management policies and procedures to determine that formal policies and procedures were in place for logical access and security processes, including password guidelines and standards.	No exceptions noted.
CC5.1.2	User and privileged support accounts follow McKesson ETS security standards for password complexity, length, change frequency, and account lockout.	Inquired of the database administrator regarding privileged support accounts to determine that user and privileged support accounts followed McKesson ETS security standards for complexity, length, change frequency, and account lockout.	No exceptions noted.
		Inspected the security and logical access policies and password configurations for a sample of in-scope systems to determine that user and privileged support accounts followed McKesson ETS security standards for password complexity, length, change frequency, and account lockout for each in-scope system sampled.	No exceptions noted.
CC5.1.3	General and privileged access to servers or system resources and utilities are approved by the requesting user's manager prior to access being granted.	Inquired of the security operations manager regarding general and privileged access to servers or system resources to determine that general and privileged access to servers or system resources and utilities were approved by the requesting user's manager prior to access being granted.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the user account request and manager approval for a sample of user accounts granted access to in-scope system resources or utilities during the review period to determine that general and privileged access to servers or system resources was approved by the requesting users' managers prior to access being granted for each user account request sampled.	No exceptions noted.
CC5.1.4	Administrative access privileges are restricted to user accounts accessible by authorized personnel for in-scope systems including: • Network domain • Production servers • Production databases	Inquired of the IT compliance manager regarding administrative access to determine that administrative access privileges were restricted to user accounts accessible by authorized personnel for the following in-scope systems: • Network domain • Production servers and mainframe • Production databases	No exceptions noted.
		Inspected the administrative access listings for a sample of in-scope systems with the assistance of the IT compliance manager to determine that administrative access privileges were restricted to user accounts accessible by authorized personnel for the following in-scope systems: • Network domain • Production servers and mainframe • Production databases	No exceptions noted.
CC5.1.5	In accordance with frequency defined in established McKesson ETS policies and procedures, privileged access to critical systems and servers is reviewed by each technical team within the McKesson ETS organization and with certification from the privileged users' direct manager to confirm access is consistent with management's intentions.	Inquired of the IT compliance manager regarding the review of privileged access to critical systems and servers to determine that privileged access to critical systems and servers was reviewed by each technical team within the McKesson ETS organization with certification from the privileged users' direct manager to confirm access was consistent with management's intentions in accordance with frequency defined in established McKesson ETS policies and procedures.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the information security management policies and procedures to determine that policies and procedures were in place to define the frequency in which privileged access to critical systems and servers was reviewed by each technical team within the McKesson ETS organization.	No exceptions noted.
		Inspected privileged user access reviews during the review period for a sample of in-scope production system to determine that privileged access to critical systems and servers was reviewed by each technical team within the McKesson ETS organization with certification from the privileged users' direct manager to confirm access was consistent with management's intentions in accordance with frequency defined in established McKesson ETS policies and procedures.	No exceptions noted.
CC5.1.6	External access by employees is configured to require multi-factor authentication and an encrypted VPN connection.	Inquired of the IT compliance manager regarding external access to determine that external access was configured to require multi-factor authentication and an encrypted VPN connection.	No exceptions noted.
		Inspected the RSA configuration and the McKesson access portal login page to determine that external access to employees was configured to require multi-factor authentication and an encrypted VPN connection.	No exceptions noted.
CC5.1.7	Logical access to network devices is systematically restricted to authorized network engineers through TACACS.	Inquired of the director of network engineering regarding logical access to network devices to determine that logical access to network devices was systematically restricted to authorized network engineers through TACACS.	No exceptions noted.
		Inspected the listing of users with access to network devices during the review period to determine that logical access to network devices was systematically restricted to authorized network engineers via TACACS.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC5.2: New internal and external system users are registered and authorized prior to being issued system credentials and granted the ability to access the system. User system credentials are removed when user access is no longer authorized.			
CC5.2.1	General and privileged access to servers or system resources and utilities are approved by the requesting user's manager prior to access being granted.	Inquired of the security operations manager regarding general and privileged access to servers or system resources to determine that general and privileged access to servers or system resources and utilities were approved by the requesting user's manager prior to access being granted.	No exceptions noted.
		Inspected the user account request and manager approval for a sample of user accounts granted access to in-scope system resources or utilities during the review period to determine that general and privileged access to servers or system resources was approved by the requesting users' managers prior to access being granted for each user account request sampled.	No exceptions noted.
CC5.2.2	User and privileged support accounts follow McKesson ETS security standards for password complexity, length, change frequency, and account lockout.	Inquired of the database administrator regarding privileged support accounts to determine that user and privileged support accounts followed McKesson ETS security standards for complexity, length, change frequency, and account lockout.	No exceptions noted.
		Inspected the security and logical access policies and password configurations for a sample of in-scope systems to determine that user and privileged support accounts followed McKesson ETS security standards for password complexity, length, change frequency, and account lockout for each in-scope system sampled.	No exceptions noted.
CC5.2.3	An identity management solution is configured to automatically disable Active Directory user accounts assigned to terminated employees within 24 hours after employee termination in the HR system.	Inspected the identity management solution configurations to determine that an identity management solution was configured to automatically disable Active Directory user accounts assigned to terminated employees within 24 hours after employee termination in the HR system.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the Active Directory user listing for a sample of employees terminated during the review period to determine that the Active Directory accounts were disabled by the identity management solution for each terminated employee sampled.	No exceptions noted.
CC5.2.4	An automated audit job is configured to execute nightly to detect exceptions not captured by the identity management solution and automatically disable the associated accounts.	Inspected the automated audit job configuration and an example output to determine that an automated job was configured to execute nightly to detect and disable terminated user accounts that were not detected by the identity management solution.	No exceptions noted.
		Inspected the Active Directory user listing for a sample of employees terminated during the review period to determine that the Active Directory accounts were disabled for each terminated employee sampled.	No exceptions noted.
CC5.2.5	In accordance with frequency defined in established McKesson ETS policies and procedures, privileged access to critical systems and servers is reviewed by each technical team within the McKesson ETS organization and with certification from the privileged users' direct manager to confirm access is consistent with management's intentions.	Inquired of the IT compliance manager regarding the review of privileged access to critical systems and servers to determine that in accordance with frequency defined in established McKesson ETS policies and procedures, privileged access to critical systems and servers was reviewed by each technical team within the McKesson ETS organization and with certification from the privileged users' direct manager to confirm access was consistent with management's intentions.	No exceptions noted.
		Inspected the information security management policies and procedures to determine that policies and procedures were in place to define the frequency in which privileged access to critical systems and servers was reviewed by each technical team.	No exceptions noted.
		Inspected privileged user access reviews during the review period for a sample of in-scope production system to determine that privileged access to each system sampled was reviewed by technical teams according to frequencies established by corporate policies and contained management certifications that access was appropriate.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC5.2.6	A daily termination report is e-mailed to the McKesson ETS security operations team and the various technical teams who subsequently disable or remove the access privileges associated with the terminated employee.	Inquired of the IT compliance manager regarding review of daily termination reports to determine that a daily report of terminated employees was e-mailed to the security operations team who subsequently disabled or removed access privileges for each terminated employee.	No exceptions noted.
		Inspected the termination report e-mail messages for a sample of dates during the review period to determine that daily termination reports were e-mailed to the McKesson ETS security operations and various technical teams for each date sampled.	No exceptions noted.
		Inspected the in-scope system user access listings for a sample of employees terminated during the review period to determine that access privileges were disabled or removed for each employee sampled.	No exceptions noted.
CC5.3: Internal and external system users are identified and authenticated when accessing the system components (for example, infrastructure, software and data).			
CC5.3.1	User and privileged support accounts follow McKesson ETS security standards for password complexity, length, change frequency, and account lockout.	Inquired of the database administrator regarding privileged support accounts to determine that user and privileged support accounts followed McKesson ETS security standards for complexity, length, change frequency, and account lockout.	No exceptions noted.
		Inspected the security and logical access policies and password configurations for a sample of in-scope systems to determine that user and privileged support accounts followed McKesson ETS security standards for password complexity, length, change frequency, and account lockout for each in-scope system sampled.	No exceptions noted.
CC5.3.2	External access by employees is configured to require multi-factor authentication and an encrypted VPN connection.	Inquired of the IT compliance manager regarding external access to determine that external access was configured to require multi-factor authentication and an encrypted VPN connection.	No exceptions noted.
		Inspected the RSA configuration and the McKesson access portal login page to determine that external access to employees was configured to require multi-factor authentication and an encrypted VPN connection.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC5.4: Access to data, software, functions, and other IT resources is authorized and is modified or removed based on roles, responsibilities, or the system design and changes to them.			
CC5.4.1	Administrative access privileges are restricted to user accounts accessible by authorized personnel for in-scope systems including: • Network domain • Production servers • Production databases	Inquired of the IT compliance manager regarding administrative access to determine that administrative access privileges were restricted to user accounts accessible by authorized personnel for the following in-scope systems: • Network domain • Production servers and mainframe • Production databases	No exceptions noted.
		Inspected the administrative access listings for a sample of in-scope systems with the assistance of the IT compliance manager to determine that administrative access privileges were restricted to user accounts accessible by authorized personnel for the following in-scope systems: • Network domain • Production servers and mainframe • Production databases	No exceptions noted.
CC5.4.2	Logical access to network devices is systematically restricted to authorized network engineers through TACACS.	Inquired of the director of network engineering regarding logical access to network devices to determine that logical access to network devices was systematically restricted to authorized network engineers through TACACS.	No exceptions noted.
		Inspected the listing of users with access to network devices during the review period to determine that logical access to network devices was systematically restricted to authorized network engineers via TACACS.	No exceptions noted.
CC5.4.3	General and privileged access to servers or system resources and utilities are approved by the requesting user's manager prior to access being granted.	Inquired of the security operations manager regarding general and privileged access to servers or system resources to determine that general and privileged access to servers or system resources and utilities were approved by the requesting user's manager prior to access being granted.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the user account request and manager approval for a sample of user accounts granted access to in-scope system resources or utilities during the review period to determine that general and privileged access to servers or system resources was approved by the requesting users' managers prior to access being granted for each user account request sampled.	No exceptions noted.
CC5.4.4	In accordance with frequency defined in established McKesson ETS policies and procedures, privileged access to critical systems and servers are reviewed by each technical team within the McKesson ETS organization and with certification from the privileged users' direct manager to confirm access is consistent with management's intentions.	Inquired of the IT compliance manager regarding the review of privileged access to critical systems and servers to determine that privileged access to critical systems and servers was reviewed by each technical team within the McKesson ETS organization with certification from the privileged users' direct manager to confirm access was consistent with management's intentions in accordance with frequency defined in established McKesson ETS policies and procedures.	No exceptions noted.
		Inspected the information security management policies and procedures to determine that policies and procedures were in place to define the frequency in which privileged access to critical systems and servers was reviewed by each technical team within the McKesson ETS organization.	No exceptions noted.
		Inspected privileged user access reviews during the review period for a sample of in-scope production system to determine that privileged access to critical systems and servers was reviewed by each technical team within the McKesson ETS organization with certification from the privileged users' direct manager to confirm access was consistent with management's intentions in accordance with frequency defined in established McKesson ETS policies and procedures.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC5.4.5	A daily termination report is e-mailed to the McKesson ETS security operations team and the various technical teams who subsequently disable or remove the access privileges associated with the terminated employee.	Inquired of the IT compliance manager regarding review of daily termination reports to determine that a daily report of terminated employees was e-mailed to the security operations team who subsequently disabled or removed access privileges for each terminated employee.	No exceptions noted.
		Inspected the termination report e-mail messages for a sample of dates during the review period to determine that daily termination reports were e-mailed to the McKesson ETS security operations and various technical teams for each date sampled.	No exceptions noted.
		Inspected the in-scope system user access listings for a sample of employees terminated during the review period to determine that access privileges were disabled or removed for each employee sampled.	No exceptions noted.
CC5.5: Physical access to facilities housing the system (for example, data centers, backup media storage, and other sensitive locations as well as sensitive system components within these locations) is restricted to authorized personnel.			
CC5.5.1	New access privileges to the data center or the issuance of an electronic key card are approved by an authorized data center employee.	Inquired of the facility manager to determine that new access privileges to the data center or the issuance of an electronic key card were approved by an authorized data center employee and to determine what employees were authorized to provision such access.	No exceptions noted.
		Inspected the access approval documentation for a sample of employees granted access to the data center or provisioned an electronic key card during the review period to determine that the new access privileges to the data center or the issuance of an electronic key card were approved by an authorized data center employee prior to access being granted.	No exceptions noted.
CC5.5.2	Entrance to the data center is only authorized by data center security personnel after providing proof of identity (a photo ID issued by McKesson or a governmental entity).	Inquired of the facility manager regarding entrance to the data center to determine that entrance to the data center was only by authorized by data center security personnel after providing proof of identity (a photo ID issued by McKesson or a governmental entity).	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Observed the process for entering the data center to determine that entrance to the data center was only authorized by data center security personnel after a valid McKesson ID or government issued ID was provided.	No exceptions noted.
CC5.5.3	On a monthly basis, a review of individuals with access to the data center is performed by data center management.	Inspected the review of data center access for a sample of months during the review period to determine that a data center access review was performed for each in-scope data center for each month sampled.	No exceptions noted.
CC5.5.4	The human resources system sends the physical security team a weekly report of terminated employees for removal of physical access.	Inspected the report of terminated employees e-mail for a sample of weeks during the review period to determine that the human resources system sent a list of terminated employees to the physical security team for removal of physical access for each week sampled.	No exceptions noted.
CC5.5.5	On a daily basis the data center physical security personnel review unauthorized activity and failed access attempts logged by the access control system. Events are investigated as appropriate by the data center security and incident management teams. The key card access logs are retained for a minimum of three months.	Inquired of the facility manager to determine that data center physical security personnel reviewed unauthorized activity and failed access attempts logged by the access control system on a daily basis and that events were investigated, as appropriate, by the data center security and incident management teams.	No exceptions noted.
		Inspected the review of unauthorized activity and failed access attempts for a sample of dates during the review period to determine that data center security personnel reviewed the unauthorized activity and failed access attempts logs for each date sampled.	No exceptions noted.
		Inspected the access management system log archives to determine that key card access logs were retained for at least three months.	No exceptions noted.
CC5.5.6	The primary entrance to the data centers is through a manned reception area. Other doors or entry ways, such as fire doors within the data centers are controlled or secured through an access card reader, alarm system, or are made inaccessible from the outside.	Inquired of the facility manager regarding data center entrances to determine that the primary entrance to the data centers was through a manned reception area and that other doors or entry ways, such as fire doors were controlled or secured through an access card reader, alarm system, or made inaccessible from the outside.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Observed the primary and non-primary entrances to the data center during the review period to determine that the primary entrance was manned by security personnel and other entrances, including fire doors, were controlled or secured via an access card reader, alarm system, or otherwise inaccessible from the outside.	No exceptions noted.
CC5.5.7	DVR IP cameras are located inside and outside the data center facilities and within the raised floor area. The cameras are monitored 24 hours a day, 7 days a week, by the data center security team. Camera footage is recorded and retained for a minimum of 120 days based on the amount of activity.	Inquired of the facility manager and the chief engineer to determine that DVR IP cameras were located inside and outside the data center facilities and within the raised floor area, camera surveillance was monitored 24 hours a day, seven days a week, and camera footage was retained for at least 120 days.	No exceptions noted.
		Observed the camera locations with the assistance of the chief engineer and facility manager from the in-scope data centers that DVR IP cameras were located inside and outside of the data center facilities, including the raised floor area.	No exceptions noted.
		Inspected the historical camera footage archives from the in-scope data centers to determine that camera footage was retained for at least 120 days.	No exceptions noted.
CC5.6: Logical access security measures have been implemented to protect against to security and availability threats from sources outside the boundaries of the system.			
CC5.6.1	Formal procedures and checklists are in place for configuring and installing new routers and switches, as well as documented procedures to add a new server to the network.	Inspected the procedures and checklists to determine that procedures and checklists were in place for configuring and installing new routers and switches, as well as documented procedures to add a new server to the network.	No exceptions noted.
CC5.6.2	Firewall configurations are versioned using automated software which systematically captures prior configuration and new configuration changes.	Inquired of the director of network engineering regarding the capture of firewall configuration changes to determine that firewall configurations were versioned using automated software which systematically captured prior and new firewall configuration changes.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the automated software history detail to determine that firewall configurations were versioned using automated software which systematically captured prior and new firewall configuration changes.	No exceptions noted.
CC5.6.3	An IPS is in place to monitor system traffic for predefined events and changes.	Inspected IPS security profile group configurations to determine that an IPS was in place to monitor system traffic for predefined events and changes.	No exceptions noted.
CC5.6.4	The IPS system generates a daily threat report that is reviewed by security personnel.	Inquired of the security operations lead regarding reviews of IPS reports to determine that IPS reports were reviewed on a daily basis by security personnel.	No exceptions noted.
		Inspected an example IPS report to determine that a report containing threats was generated on daily basis.	No exceptions noted.
CC5.6.5	A network monitoring application is configured to identify abnormal patterns and anomalies in network traffic and submit identified action items to the SIEM. If an investigation is required, an incident ticket is opened and tracked to resolution.	Inquired of the manager of IT compliance regarding tracking of incidents identified by the network monitoring application to determine that incident tickets were opened and tracked to resolution.	No exception noted.
		Inspected the network monitoring application configurations to determine that the network monitoring application was configured to identify abnormal patterns and anomalies in network traffic and submit identified action items to the SIEM.	No exceptions noted.
CC5.6.6	External access by employees is configured to require multi-factor authentication and an encrypted VPN connection.	Inquired of the IT compliance manager regarding external access to determine that external access was configured to require multi-factor authentication and an encrypted VPN connection.	No exceptions noted.
		Inspected the RSA configuration and the McKesson access portal login page to determine that external access to employees was configured to require multi-factor authentication and an encrypted VPN connection.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC5.7: The transmission, movement, and removal of information is restricted to authorized users and processes, and is protected during transmission, movement, or removal enabling the entity to meet its commitments and requirements as they related to security and availability.			
CC5.7.1	Data loss prevention software is configured to scan for sensitive information in outgoing transmissions over public communication paths.	Inspected the data loss prevention software configurations to determine that data loss prevention software was configured to scan for sensitive information in outgoing transmissions over public communication paths.	No exceptions noted.
CC5.7.2	Access to backup systems is restricted to user accounts accessible by authorized personnel.	Inquired of the director of storage operations regarding access to the backup system to determine that access to backup systems was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
		Inspected the backup system access listing with the assistance of the director of storage operations to determine that access to backup systems was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
CC5.7.3	The ability to recall backup media from the off-site vendor is restricted to user accounts accessible by authorized personnel.	Inquired of the director of data center operations regarding access to recall backup media from the off-site vendor to determine that the ability to recall backup media from the off-site vendor was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
		Inspected the backup media recall listing with the assistance of the director of data center operations to determine that the ability to recall backup media from the off-site vendor was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
CC5.7.4	Access to modify the job schedule application is restricted to user accounts accessible by authorized personnel.	Inquired of the director of data center operations regarding access to modify the job scheduling application to determine that access to modify the job scheduling application was restricted to user accounts accessible by authorized personnel.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the job schedule application access listing with the assistance of the director of data center operations to determine that access to modify the job schedule application was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
CC5.8: Controls have been implemented to prevent or detect and act upon the introduction of unauthorized or malicious software.			
CC5.8.1	A central antivirus server is configured with antivirus software to protect registered production Windows servers and workstations with the following configurations: • Scan for updates to antivirus definitions and update registered servers and workstations daily • Scan registered servers and workstations on a daily basis	Inspected the enterprise antivirus software configurations and registered client list to determine that a central antivirus server was configured with antivirus software to protect registered production Windows servers and workstations with the following configurations: • Scan for updates to antivirus definitions and update registered servers and workstations daily • Scan registered servers and workstations on a daily basis	No exceptions noted.
CC5.8.2	Access to implement software, logical hardware, or maintenance changes to production environments is systematically restricted to the system administration group members representing their respective platform.	Inquired of the business systems analyst regarding the implementation of software, logical hardware, or maintenance changes to the production environment to determine that access to implement software, logical hardware, or maintenance changes was systematically restricted to the system administration group members representing their respective platform.	No exceptions noted.
		Inspected the production access user listings for a sample of production systems with the assistance of business systems analyst to determine that access to implement changes was systematically restricted to members of the system administration group representing their respective platform for each production system sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.0: Common Criteria Related to System Operations			
CC6.1: Vulnerabilities of system components to security and availability breaches and incidents due to malicious acts, natural disasters, or errors are monitored and evaluated and countermeasures are implemented to compensate for known and new vulnerabilities.			
CC6.1.1	Upon reaching or exceeding configured thresholds, network monitoring applications generate alerts, which systematically create incident tickets. The network control center tracks tickets from inception to resolution.	Inquired of the director of network engineering regarding network monitoring to determine that incident tickets were monitored from inception to resolution by network control center personnel.	No exceptions noted.
		Observed the network monitoring application alert and ticket generation configurations to determine that a network monitoring application was configured to generate alerts and create incident tickets upon reaching or exceeding configured thresholds.	No exceptions noted.
		Inspected the incident ticket detail for a sample of alerts generated by the network monitoring application during the review period to determine that incident tickets were tracked from inception to resolution for each alert sampled.	No exceptions noted.
CC6.1.2	Documented procedures are in place to guide call center personnel in the escalation and resolution of support requests including, but not limited to the following • Telephone and e-mail requests for support • User password reset • Incident and potential breach notification	Inspected the call center procedures to determine that documented procedures were in place to guide call center personnel in the escalation and resolution of support requests including, but not limited to the following • Telephone and e-mail requests for support • User password reset • Incident and potential breach notification	No exceptions noted.
CC6.1.3	Results from monthly vulnerability scans are reviewed during monthly management meetings and incorporated as necessary into the ongoing risk management process.	Inquired of the IT compliance manager regarding the review of monthly vulnerability scans to determine that scans were reviewed during monthly management meetings and incorporated as necessary into the ongoing risk management process.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the management meeting minutes for a sample of months during the review period to determine that meetings were held and monthly vulnerability scans were reviewed during management meetings and incorporated as necessary into the ongoing risk management process for each month sampled.	No exceptions noted.
CC6.2: Security and availability incidents, including logical and physical security breaches, failures, concerns, and other complaints are identified, reported to appropriate personnel, and acted on in accordance with established incident response procedures.			
CC6.2.1	A formal incident management and resolution process is in place to manage various types of incidents impacting normal operations processing and ability to provide services.	Inspected the incident management and resolution policies and procedures to determine that a formal incident management and resolution process was in place.	No exceptions noted.
CC6.2.2	Incidents reported to the McKesson IT Operations team are logged in the ticketing system, assigned a priority, and assigned to a support group for resolution.	Inquired of the systems manager regarding incidents logging to determine that incidents reported to the McKesson IT Operations team were logged in the ticketing system, assigned a priority, and assigned to a support group for resolution.	No exceptions noted.
		Inspected the incident ticket detail for a sample of incidents logged during the review period to determine that incidents reported to the McKesson IT Operations team were logged in the ticketing system, assigned a priority, and assigned to a support group for resolution for each incident sampled.	No exceptions noted.
CC6.2.3	Incidents assigned are resolved by the group responsible as per policy in accordance with their priority.	Inquired of the systems manager regarding incident resolution to determine that all incidents assigned were resolved by the group responsible, per policy, in accordance with priority.	No exceptions noted.
		Inspected the incident ticket detail for a sample of incidents logged during the review period to determine that incidents were resolved by the group responsible and in the time frames required by policy in accordance with their priority for each incident sampled.	No exceptions noted.
CC7.0: Common Criteria Related to Change Management			
CC7.1: Security and availability commitments and requirements are addressed during the system development lifecycle including design, acquisition, implementation, configuration, testing, modification, and maintenance of system components.			
Not Applicable – McKesson ETS does not develop software as a component of its services.			

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.2: Infrastructure, data, software, and procedures are updated as necessary to remain consistent with the system commitments and requirements as they relate to security and availability.			
CC7.2.1	A formal risk assessment is performed on an annual basis. Risks that are identified are rated using a risk evaluation process and are formally documented.	Inspected the most recent risk assessment to determine that a formal risk assessment was performed during the review period and identified risks were rated using a risk evaluation process and were formally documented.	No exceptions noted.
CC7.2.2	Monthly security meetings are held to discuss security threats and output from vulnerability scans.	Inspected the security meeting agenda for a sample of months during the review period to determine that monthly security meetings were held to discuss security threats and output from vulnerability scans for each month sampled.	No exceptions noted.
CC7.3: Change management processes are initiated when deficiencies in the design or operating effectiveness of controls are identified during system operation and monitoring.			
CC7.3.1	System deficiencies identified during internal audits or vulnerability assessments that require a change to be made including latent (emergency) changes go through standard change management procedures.	Inspected the ticket details for a sample of deficiencies identified during internal audits and vulnerability assessments that required changes to be made to determine that changes went through the standard change management procedures for each deficiency sampled.	The test of control activity disclosed that a population of deficiencies identified during internal audits and vulnerability assessments that required changes to be made during the review period was not evidenced.
CC7.3.2	Upon reaching or exceeding configured thresholds, network monitoring applications generate alerts, which systematically create incident tickets. The network control center tracks tickets from inception to resolution.	Inquired of the director of network engineering regarding network monitoring to determine that incident tickets were monitored from inception to resolution by network control center personnel.	No exceptions noted.
		Observed the network monitoring application alert and ticket generation configurations to determine that a network monitoring application was configured to generate alerts and create incident tickets upon reaching or exceeding configured thresholds.	No exceptions noted.
		Inspected the incident ticket detail for a sample of alerts generated by the network monitoring application during the review period to determine that incident tickets were tracked from inception to resolution for each alert sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.4: Changes to system components are authorized, designed, developed, configured, documented, tested, approved, and implemented in accordance with security and availability commitments and requirements.			
CC7.4.1	Changes, including system patches, are approved by an authorized approver(s) based on the risk level associated with the change in accordance with change management policies and procedures.	Inquired of the business system analyst regarding the approval of changes, including system patches, to determine that changes, including system patches, were approved by an authorized approver(s) based on the risk level associated with each change, in accordance with change management policies and procedures.	No exceptions noted.
		Inspected the change ticket detail for a sample of changes implemented during the review period to determine that changes were approved by an authorized approver(s) based on the assigned risk level associated with the change in accordance with change management policies for each change sampled.	No exceptions noted.
CC7.4.2	Certain changes are tested by individual(s) or group, depending on the type of change, and the results are captured within an e-mail or the Remedy ticket associated with the change, in accordance with change management policies and procedures.	Inquired of the IT compliance manager regarding testing of changes to determine that certain changes were tested by individuals or a group depending on the type of change, and the results were captured within an e-mail or the ticket associated with the change, in accordance with change management policies and procedures.	No exceptions noted.
		Inspected the change ticket detail or e-mail documentation for a sample of changes implemented during the review period to determine that changes were tested and the results were captured within an e-mail or ticket for each of change sampled.	No exceptions noted.
CC7.4.3	Access to implement software, logical hardware, or maintenance changes to production environments is systematically restricted to the system administration group members representing their respective platform.	Inquired of the business systems analyst regarding the implementation of software, logical hardware, or maintenance changes to the production environment to determine that access to implement software, logical hardware, or maintenance changes was systematically restricted to the system administration group members representing their respective platform.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the production access user listings for a sample of production systems with the assistance of business systems analyst to determine that access to implement changes was systematically restricted to members of the system administration group representing their respective platform for each production system sampled.	No exceptions noted.

AVAILABILITY PRINCIPLE AND CRITERIA TABLE

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
A1.1: Current processing capacity and usage are maintained, monitored and evaluated to manage capacity demand and to enable the implementation of additional capacity to help meet availability commitments and requirements.			
A1.1.1	An enterprise monitoring application is configured to monitor system capacity and generate automated alert notifications to notify operations personnel when predefined thresholds are exceeded on monitored devices.	Inquired of the manager of IT compliance regarding process monitoring to determine that an enterprise monitoring application was configured to monitor system capacity and generate alert notifications to notify operations personnel when predefined thresholds were exceeded on monitored devices.	No exceptions noted.
		Inspected the enterprise monitoring application configurations and notification configurations to determine that the enterprise monitoring application was configured to monitor system capacity and generate alert notifications.	No exceptions noted
A1.2: Environmental protections, software, data backup processes, and recovery infrastructure are designed, developed, implemented, operated, maintained and monitored to meet availability commitments and requirements.			
A1.2.1	Preventative maintenance procedures are performed for environmental equipment according to documented procedures and frequencies.	Inspected the maintenance documentation for a sample of environmental equipment items located in the in-scope data centers to determine that preventative maintenance was performed for each environmental equipment item sampled according to the documented frequencies outlined in the maintenance schedules.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
A1.2.2	UPS batteries and diesel generators are installed and operating to provide the data center with a continuous supply of conditioned power in the event of power loss or failure. .	Observed the UPS batteries and diesel generators at each of the in-scope data centers to determine that UPS batteries and diesel generators were installed and operating to provide the data center with a continuous supply of conditioned power in the event of a power loss or failure.	No exceptions noted.
A1.2.3	Ambient temperature sensors are located at each CRAC and within the server racks. CRAC units perform cooling of the raised floor area and maintain constant temperature and humidity conditions.	Inquired of the chief engineer and the facility manager to determine that ambient temperature sensors were located at each CRAC and within the server racks and that CRAC units performed cooling of the raised floor area and maintained constant temperature and humidity conditions.	No exceptions noted.
		Observed ambient temperature sensors located at each CRAC and within the server rack to determine that CRAC units performed cooling of the raised floor area and maintained constant temperature and humidity conditions.	No exceptions noted.
A1.2.4	Automatic fire detection and suppression equipment has been installed to prevent damage to computing hardware. The fire detection system utilizes smoke and/or heat detection sensors that are located in the data center ceiling plenum, main room, and below the raised floor as well as in data center support areas. These sensors monitor a pre-acting gaseous suppression system and will generate visible alarms in the raised floor and at the security console. Additionally, dry pipe fire sprinklers have been installed within the data centers and are configured to activate if the temperature exceeds a set heat limit.	Observed the fire detection system to determine that the fire detection system utilized smoke and/or heat detection sensors that were located in the data center ceiling plenum, main room, and below the raised floor as well as in data center support areas and that the sensors monitored a pre-acting gaseous suppression system and generated visible alarms in the raised floor and at the security console	No exceptions noted.
		Observed dry pipe fire sprinklers to determine that dry pipe fire sprinklers were installed and configured to activate upon set heat limits being exceeded.	No exceptions noted.
A1.2.5	McKesson ETS performs backups of databases and file systems according to the defined customer requirements.	Inspected the customer requirements and backup schedules for a sample of production servers and databases to determine that backups of databases and file systems were performed in accordance with defined customer requirements for each production server and database sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
A1.2.6	A ticket is systematically opened for each scheduled backup failure. Tickets that cannot be resolved automatically are assigned to the EDP group. EDP team members review and track assigned tickets through resolution in a timely manner.	Inquired of the storage operations director regarding tickets to determine tickets were systematically opened for scheduled backup failures and assigned to the EDP group when unable to be resolved automatically and that EDP team members reviewed and tracked through resolution.	No exceptions noted.
		Inspected the ticket detail for a sample of backup failures during the review period to determine that the tickets were opened, assigned and resolved for each backup failure sampled.	No exceptions noted.
A1.2.7	McKesson computer operations personnel prepare backup tapes on a daily basis for transmittal to an off-site location via a third party.	Inquired of the director of data center operations regarding backups to determine that computer operations personnel prepared backup tapes on a daily basis for the transmittal to an off-site location via a third party.	No exceptions noted.
		Inspected the backup tape transmittal reports for a sample of dates during the review period to determine that McKesson computer operations prepared and transmitted backup tapes to an off-site location via a third party for each date sampled.	No exceptions noted.
A1.2.8	McKesson EDP monitors data replication of data domain devices. Anomalies or failures resulting from the replication are tracked through tickets and resolved.	Inspected the data replication dashboard to determine that McKesson EDP monitored data replication of data domain devices.	No exceptions noted.
		Inspected the ticket detail for a sample of replication failures during the review period to determine that a ticket was created and that anomalies or failures were tracked and resolved for each replication failure sampled.	No exceptions noted.
A1.3: Procedures supporting system recovery in accordance with recovery plans are periodically tested to help meet availability commitments and requirements.			
A1.3.1	Restorations (e.g., ad-hoc customer file system restores) of backups are performed upon request and recorded within the ticketing system.	Inspected the ticket detail for a sample of restoration requests during the review period to determine that restoration of backups were performed and recorded for each restoration request sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
	Business continuity and disaster recovery plans are in place to guide personnel in procedures to protect against disruptions caused by an unexpected event.	Inspected the business continuity and disaster recovery plans to determine that business continuity and disaster recovery plans were in place to guide personnel in procedures to protect against disruptions caused by an unexpected event.	No exceptions noted.
A1.3.2	McKesson ETS performs disaster recovery testing exercises according to the defined customer requirements.	Inspected the results of the most recent customer disaster recovery testing exercise to determine that disaster recovery testing exercises were performed during the review period according to defined customer requirements.	No exceptions noted.

SECTION 5

OTHER INFORMATION PROVIDED BY MANAGEMENT

MANAGEMENT'S RESPONSE TO TESTING EXCEPTIONS

Security Principle

#	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.3	Personnel responsible for designing, developing, implementing, operating, maintaining, and monitoring of the system affecting security and availability have the qualifications and resources to fulfill their responsibilities.	On an annual basis, personnel are required to complete compliance training to reaffirm understanding of confidentiality and privacy practices.	Inspected the compliance training detail for a sample of employees to determine that compliance training was completed during the review period for each employee sampled.	The test of control activity disclosed that compliance training was not evidenced during the review period for four of the 25 employees sampled.
CC2.2	The entity's security and availability commitments are communicated to external users, as appropriate, and those commitments and the associated system requirements are communicated to internal system users to enable them to carry out their responsibilities.			
Management's Response:	Throughout the year senior management have communicated to everyone the importance of training and the fact that it is expected for all to complete. Additional measures will be added around year end to inform individuals who haven't completed it yet that they must do so or could face possible sanctions.			

#	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.3	Change management processes are initiated when deficiencies in the design or operating effectiveness of controls are identified during system operation and monitoring.	System deficiencies identified during internal audits or vulnerability assessments that require a change to be made including latent (emergency) changes go through standard change management procedures.	Inspected the ticket details for a sample of deficiencies identified during internal audits and vulnerability assessments that required changes to be made to determine that changes went through the standard change management procedures for each deficiency sampled.	The test of control activity disclosed that a population of deficiencies identified during internal audits and vulnerability assessments that required changes to be made was not evidenced.
Management's Response:	Changes will be introduced into the process to help tie out changes that are being implemented as a component of remediation action plans that are associated with findings.			

LHCL CHECKLIST FY2017

OPERATIONAL QUESTIONS	
1	LHCL Name:
2	Job Title
3	Date:
4	Site Code:
5	What is your location's mailing address?
6	How many employees are located in your office?
7	City:
8	Specialty:
9	Site Manager:
10	Site Vice President:
11	Compliance Program Director (CPD):
12	Is the LHCL's location marked?
13	What is the name of the person who is the "back up" HIPAA contact for your office when you are not available?
14	What is her/his telephone number?
15	Are New Hires introduced to the LHCL as part of their orientation?
16	Who introduces new hires to the LHCL?
17	Does your site have a designated Site Security Officer?
18	Who is the Site Security Officer?
19	Does your site have a designated Records Information Management (RIM) Coordinator?
20	Who is the designated RIM Coordinator?
21	Are employees aware of the procedures that must be followed when sending PHI via email?
22	How are employees made aware of these procedures?
23	Does your site have a restricted access system operated by a badge, fob or key code?
24	If Yes, Type of access system:
25	Were visitors issued badges or fobs that allow them to access this system?
26	How are these badges managed?
27	If Key Code, Were visitors given the key code to access this system?
28	If Key Code, How often is the access code changed?
29	If other type of system, explain access system.
30	Where in the office are printed copies of the Billing Compliance Policies located?
31	Where in the office are printed copies of the Privacy and Security located? (HIPAA policy & procedures, PCI, etc.)
32	Where in the office are printed copies of any Local policies located?
33	What is the date of the printed policies in your office/building?
34	Have all employees with PCs been given instructions on how to access BPS Billing Compliance and Privacy and Security policies on the Intranet (McKNet)?
35	Have you and/or site management verified that the employees understand these instructions, have the correct links saved on their computers, and can access the policies on the SharePoint site?
36	If "No", why not?
37	Do you routinely receive and deposit checks and/or cash for any clients in your office?
38	How are checks/cash secured during the day?
39	Does the same person that initially receives the checks/cash also prepare the deposit slip and deposit the money?
40	Describe the controls and balances in place to ensure all checks/cash received are accounted for and deposited in the correct account.
41	Who verifies/balances the bank account(s)?
42	Does your office process credit card payments?

43	Who is the PCI Rep for your office?
44	Are there any clients whose credit card payments are processed using a tool other than the BPS Virtual Payment Portal, PerYourHealth or IVR?
45	List these clients:
46	Does the PCI Rep have appropriate documentation showing that these Alternative Processes have been approved by Compliance?
47	Are there any credit card processing machines still in your office?
48	If so how are the credit card crocessing machines locked in a separate room or area?
49	List the names and titles of employees who have access to the area/keys to where the machines are stored.
50	Do all credit card processing machines print only the last 4 numbers on the patient's receipt?
51	Do all credit card processing machines print only the last 4 numbers on reports?
52	Have all documents with full credit card numbers been removed from your office?
53	If "No", how and where is this information securely stored?
54	For what purpose is this information retained?
55	Is all onsite document storage in compliance with the BPS "Records Retention, Storage and Destruction Within BPS Offices" policy? (PHYSN-CMPL-102.5)
56	If "No", what is your office's plan to meet this policy requirement and the time frame for doing so?
57	Is PHI and/or Confidential information stored on CDs, DVDs, Thumb/Flash Drives or any other portable media/drive (excluding McKesson issued laptop computers) in your office?"
58	If "Yes", is the data encrypted?
59	Describe the type(s) of data and why is it stored?
60	Where are the CDs, flash drives, or other portable media stored, and how are they secured?
61	What is the name of off-site storage company?
62	Is a BAA in place for your off-site storage company?
63	What is location of the BAA for the off-site storage company?
64	What is the name of Shredding/Document Destruction company?
65	Is a BAA in place with your Shredding/Document Destruction company?
66	What is the location of BAA for the Shredding/Document Destruction company?
67	If your site has a separate mailroom - Is the mailroom locked/secure when it is not staffed?
68	If no, explain why mailroom is not secure when not staffed:
69	Do patients come to your office regularly to make payments?
70	What precautions are taken to keep patients away from the secure work area?
71	Are any non-BPS employees co-located in this office space?
72	List these individuals and their relationship to McKesson BPS:
73	Are all employees briefed on how to recognize a possible HIPAA incident?
74	Are all employees aware of the procedure for reporting an incident?
WALKTHROUGH QUESTIONS	
75	Were "PHI FAX Forms" at all fax machines?
76	Was a "PHI That Leaves The Building Log" in use?
77	What is/are the Location(s) of the Log(s)?
78	Do all batches of PHI that leave your office for any reason contain less than 500 patients? (This includes paper copies or unencrypted electronic information saved to any media. This does NOT include records being sent to off-storage via secure transport.)
79	If "No" explain:
80	During the walkthrough was all PHI / Confidential Information locked up at the end of the work day?
81	If not, what is the office plan for complying with this policy?

82	During your last after hours walk through were all drawers or cabinets containing PHI/Confidential information, or doors to PHI storage rooms properly locked?
83	If "no", list location(s) and employee(s) responsible.
84	Periodic checks of trash cans should be performed to ensure no PHI or Confidential Information is disposed of improperly. During your walkthrough were all trash cans clear of PHI/Confidential information?
85	If any Confidential Information/PHI was found disposed of improperly, list location(s) and employee(s) responsible.
86	During office walkthroughs were all work areas clear of passwords - none found taped to monitors, keyboards, cube walls, on sticky notes, easily located in unlocked drawers, etc.?
87	During the walkthrough were all employees locking their computers/workstations when they leave their work area?
88	Were there any recycle bins in your office for non-confidential materials? (Excluding can/bottle bins in a break area.)
89	Were the recycle only bins clearly marked to discourage disposal of PHI or other confidential materials?
90	Were all monitors protected from view through external windows or from public areas?
91	If "No", list location(s) and describe your office plan for securing these monitors.
92	Were all paper documents with PHI or Confidential Information protected from view through external windows or from public areas?
93	If "No", list location(s) and describe your office plan for securing these areas.
94	Were keys to employee desks, restricted areas, and shred bins kept secure?
95	Was all unused/retired computer equipment in a locked, secure area?
96	If no, what is your office plan for securing these items?
97	Were all doors to the work area(s) secured properly?
98	If no, list location(s) and issue.
99	Were there higher access restrictions in place for Network/Telephone/Computer rooms?
100	If No, What is your office plan for securing this area?
101	Was the Network/Telephone/Computer room(s) or area(s) free from any flammable materials (boxes, paper)?
102	If No, what is your office plan for correcting this?
103	Were all shred bins locked?
104	Were shred bins emptied frequently enough that none of the contents is accessible by unauthorized persons?
105	Were all employee personal shred bins emptied every night?
106	Were all FedEx slips pre-printed with McKesson account numbers in a secure/locked area? (Both unused and used slips)
107	If your office has a postage meter - Is the postage meter password protected?
108	If no, explain why Postage Meter is not password protected:
109	If your office has a separate computer specifically for FedEx and/or UPS - Is this computer password protected?
110	FedEx/UPS - If "No", Explain:
111	Were HIPAA Signs posted properly on all COPIERS?
112	Were HIPAA signs posted properly on all FAX MACHINES?
113	Were HIPAA signs posted properly on all SHRED BINS?
114	Were HIPAA signs posted properly on all EMPLOYEE PERSONAL SHRED BINS?
115	Is an Integrity Line poster on display in your office?
116	What is the location of the Integrity Line poster(s)?
117	Does your office have a Visitor Sign-In sheet as required by policy?
118	Were Non-Employee Confidentiality Agreement forms available and used in accordance with policy?
119	Have all visitors signed a Confidentiality Agreement where required?

120	Were visitors/vendors in restricted access areas monitored and escorted?
121	Was a current (signed within the last 12 months) Confidentiality Agreement on file for each member of the cleaning crew that cleans your office?
122	If current agreements are not on file for the cleaning crew, explain:
123	Were current (signed within the last 12 months) Confidentiality Agreements on file for vendors who visit regularly? (Snack vendor, copier repair, etc.)?
124	If current agreements are not on file for regular visitors, explain:
125	As required by policy are all visitors, including McKesson employees from another location, given a badge that identifies them as a visitor?
	CONCLUDING QUESTIONS
126	How long did it take you to complete this checklist?
127	What additional question would you like to see on this questionnaire?
128	Please enter any comments about any of your answers.
129	When was the last time BPS Compliance visited your location?
130	What was the nature of the visit?
131	How can the Compliance Department better assist your office in the next year?

Change Healthcare
General Compliance, Billing Compliance and Privacy Policy Manual

Table of Contents Effective June 1, 2016
(Last Revision Date in Parenthesis)

Guide to Billing Compliance Policy Numbering

The Billing Compliance Policy (BCP) Manual Numbering System consists of a divisional defined section (Physician Compliance which appears as PHYSN-CMPL) and a Category code represented by letters, and a digit classification number. For example, for BCP "Release of Billing Compliance and HIPAA Policies," it is listed under the General Policies section (GP) and the digit policy number is 03.01, therefore it appears as PHYSN-CMPL-GP.03.01.

SECTION 1	
General Policies (GP)	**Policy Number**
Change Healthcare Code of Conduct	N/A
Preventing Retaliation	N/A
Compliance with Policies (6/1/15)	PHYSN-CMPL-GP.01.02
Compliance Training (6/1/15)	PHYSN-CMPL-GP.02.02
Release of Billing Compliance and HIPAA Policies (6/1/16)	PHYSN-CMPL-GP.03.02
Record Retention, Storage and Destruction Within BPS Offices (6/1/14)	PHYSN-CMPL-GP.04.01
Anti-Trust Compliance Client/Payer Negotiation Guidelines (10/1/08)	PHYSN-CMPL-GP.05.0
SECTION 2	
Billing Compliance Policies (BCP)	
General Billing (GB)	**Policy Number**
Discount Arrangements (6/1/14)	PHYSN-CMPL-GB.01.02
New Business Claim Review (6/1/15)	PHYSN-CMPL-GB.02.02
Requests for Medical Records - Legal (6/1/16)	PHYSN-CMPL-GB.03.01
Requests for Medical Records – Audit (6/1/16)	PHYSN-CMPL-GB.04.01
Charges for Medical Record Copying (6/1/16)	PHYSN-CMPL-GB.05.03
Signing Paper Medical Claim Forms (6/1/12)	PHYSN-CMPL-GB.06.0
Alternate Tax ID Request (6/1/15)	PHYSN-CMPL-GB.07.02
Completion of Online Provider Enrollment Forms (6/1/16)	PHYSN-CMPL-GB.08.02
Purchased Services – Anti-Mark Up Provisions (6/1/13)	PHYSN-CMPL-GB.09.01
Health Professional Shortage Areas (HPSA) (6/1/15)	PHYSN-CMPL-GB.10.01

CMS Claim Jurisdiction Rules (6/1/15)	PHYSN-CMPL-GB.11.02
Supplies, Global Services and Technical Component (6/1/15)	PHYSN-CMPL-GB.12.03
Medical Coding General (MCG)	
Diagnosis Coding (6/1/16)	PHYSN-CMPL-MCG.01.03
Procedural Coding (6/1/16)	PHYSN-CMPL-MCG.02.02
Non-Physician Practitioners (6/1/16)	PHYSN-CMPL-MCG.03.03
Consultation Services (6/1/16)	PHYSN-CMPL-MCG.04.01
Locum Tenens and Reciprocal Billing (6/1/14)	PHYSN-CMPL-MCG.05.01
Coding Reference Tools (6/1/16)	PHYSN-CMPL-MCG.06.03
Contract Coding (6/1/16)	PHYSN-CMPL-MCG.07.02
Teaching Physicians (6/1/16)	PHYSN-CMPL-MCG.08.01
Specialty Coding Certification (SCC)- Production Coding Personnel Qualifications (6/1/16)	PHYSN-CMPL-MCG.09.03
Specialty Coding Certification (SCC)- Non-Production Coding Personnel Qualifications (6/1/16)	PHYSN-CMPL-MCG.10.03
Hospice (6/1/14)	PHYSN-CMPL-MCG.11.01
Medical Coding Anesthesia/Pain Management (MCAPM)	
Post-Operative Pain Management (6/1/14)	PHYSN-CMPL-MCAPM.01.01
Medical Direction and Supervision (6/1/16)	PHYSN-CMPL-MCAPM.02.02
Medical Coding Radiology (MCR)	
Mammography (6/1/16)	PHYSN-CMPL-MCR.01.02
Medical Coding Pathology (MCP)	
Pap Smears (6/1/16)	PHYSN-CMPL-MCP.01.03
Professional Component of Clinical Pathology (PCCP) (6/1/15)	PHYSN-CMPL-MCP.02.01
Medical Coding Emergency Medicine (MCE)	
Ambulance (EMS) Services (6/1/13)	PHYSN-CMPL-MCE.01.0
Charge Processing (CP)	
Duplicate Charges (6/1/16)	PHYSN-CMPL-CP.01.02
Claims Resubmission (6/1/14)	PHYSN-CMPL-CP.02.01
Fee Schedule (6/1/15)	PHYSN-CMPL-CP.03.02
Receipt of Government Funds (6/1/13)	PHYSN-CMPL-CP.04.0
Payment Processing (PP)	

Credit Balances and Refunds (6/1/16)	PHYSN-CMPL-PP.01.03
Credit Balance Reporting Criteria (6/1/15)	PHYSN-CMPL-PP.02.02
Medicare Secondary Payer (6/1/12)	PHYSN-CMPL-PP.03.0
Non-Routine Refunds and Disclosures (6/1/15)	PHYSN-CMPL-PP.04.03
A/R Follow-Up (ARF)	
Workers' Compensation (6/1/15)	PHYSN-CMPL-ARF.01.01
Balance Billing Prohibitions (Medicare and Individual State Law) (6/1/16)	PHYSN-CMPL-ARF.02.02
Advance Beneficiary Notice (6/1/16)	PHYSN-CMPL-ARF.03.0
Small Balance Write Off-Credit (6/1/15)	PHYSN-CMPL-ARF.04.03
Small Balance Write Off-Debit (6/1/15)	PHYSN-CMPL-ARF.05.02
FORMS	
ECRU General Compliance, Billing and Privacy Policies Review	N/A
Billing Compliance and HIPAA Policy Confidentiality Agreement Release Form	N/A
Combined Application for Billing Supplies, Global, Technical or Purchased Services, POS	N/A
Combined Application for Billing Supplies, Global, Technical or Purchased Services, POS (Hospital Laboratory Client ONLY)	N/A
Client Discount Arrangement Directive	N/A
RETIRED BCP POLICIES	
Physician Scarcity Area (PSA) (Retired Policy10/1/08)	PHYSN-CMPL-2114.0
Medical Coding Certification (MCC) (Retired Policy 9/30/08)	PHYSN-CMPL-602.3
Coder Productivity Standards (Retired Policy 4/1/10)	PHYSN-CMPL-218.1
Evaluation and Management Services (Retired Policy 4/1/10)	PHYSN-CMPL-215.4
Red Flag Rules (Retired Policy 6/1/11)	PHYSN-CMPL-106.1
SECTION 3	
Privacy Policies and Procedures	**Policy/Procedure Number**
BPS HIPAA Privacy Policy	
Procedure: HIPAA Privacy Structure	PHYSN-HIPAA PRIV-CMPL-02.6
Procedure: Privacy Questions, Complaints and Incidents	PHYSN-HIPAA PRIV-CMPL-03.5
Procedure: Accounting Of Disclosures	PHYSN-HIPAA PRIV-CMPL-

	04.5
Procedure: Electronic Transmission of PHI and Confidential Information – Email	PHYSN-HIPAA PRIV-CMPL-05.6
Procedure: Electronic Transmission of PHI – Faxing	PHYSN-HIPAA PRIV-CMPL-06.6
Procedure: PHI Outside of Change Healthcare Controlled Facilities	PHYSN-HIPAA PRIV-CMPL-07.5
Procedure: Media Management	PHYSN-HIPAA PRIV-CMPL-08.5
Procedure: Physical Access	PHYSN-HIPAA PRIV-CMPL-10.6
Procedure: Business Associates	PHYSN-HIPAA PRIV-CMPL-11.5
Procedure: Handling a Patient's Request for Confidential Communications	PHYSN-HIPAA PRIV-CMPL-13.4
Procedure: Handling a Patient's Request for Restrictions to Protect Their Healthcare Information	PHYSN-HIPAA PRIV-CMPL-14.4
Procedure: Communicating with Patients and Patient's Representatives	PHYSN-HIPAA PRIV-CMPL-15.5
Procedure: Minimum Necessary	PHYSN-HIPAA PRIV-CMPL-17.5
Procedure: External Communication of HIPAA Policies	PHYSN-HIPAA PRIV-CMPL-18.4
Procedure: Storage of Work in Process that Contains Confidential Information, Including Personally Identifiable Information (PII) & Protected Health Information (PHI)	PHYSN-CMPL-HIPAA-PRIV-21.1
Procedure: Working Remotely	PHYSN-HIPAA PRIV-CMPL-22.1
Document Destruction Post Scanning	PHYSN-HIPAA SEC-CMPL- 01.2
Non-Change Healthcare or Non-Business Unit Employees Co-Located in and BPS Office Space	PHYSN-HIPAA SEC-CMPL- 02
Protection of Bank Account Information: The Security of Banking Information Belonging to Change Healthcare, Change Healthcare Clients, and Client's Patients	PHYSN-CMPL-GENERAL PRIV-01.1
Cell Phone Usage Where Confidential Information is Located	PHYSN-CMPL-GENERAL PRIV-02
Social Media and Networking Participation	PHYSN-CMPL-GENERAL-PRIV-0
Protecting Credit and Debit* Card Information	PHYSN-PCI-CMPL- 01.3