****

9B19E023

Midwest Health System: Information System Risks and Controls

Reza Espahbodi and Ganesh Vaidyanathan wrote this case solely to provide material for class discussion. The authors do not intend to illustrate either effective or ineffective handling of a managerial situation. The authors may have disguised certain names and other identifying information to protect confidentiality.

This publication may not be transmitted, photocopied, digitized, or otherwise reproduced in any form or by any means without the permission of the copyright holder. Reproduction of this material is not covered under authorization by any reproduction rights organization. To order copies or request permission to reproduce materials, contact Ivey Publishing, Ivey Business School, Western University, London, Ontario, Canada, N6G 0N1; (t) 519.661.3208; (e) cases@ivey.ca; www.iveycases.com. Our goal is to publish materials of the highest quality; submit any errata to publishcases@ivey.ca. i1v2e5y5pubs

Copyright © 2019, Ivey Business School Foundation Version: 2020-01-07

As Steve Nelson looked out of his office window onto a beautiful fall afternoon in November 2017, his focus drifted to his next meeting. Since 1996, Nelson had been with Midwest Health System (Midwest), climbing the ladder to become chief information officer (CIO). A major health care provider in a central town in the United States, Midwest was in the midst of implementing various new initiatives to satisfy the changes that were mandated by the Patient Protection and Affordable Care Act.[[1]](#footnote-1) The 2010 health care reforms had been the organization’s central focus. Midwest was in the process of providing wider health care coverage through public and private sector insurance programs, better access to health care specialists, and improved quality health care.

Nelson had scheduled the meeting with the information systems (IS) group and audit group to discuss and review risks related to information technology (IT) and the billing and collection process (the most critical process in terms of its impact on Midwest’s operations and financial statements), as well as the controls that were in place. The IS group, which consisted of veterans, including Carla Van Horde, Carmen Capriati, and Jeff Beckman, was eager to understand the risks more thoroughly and re-engineer the controls. Van Horde served as the privacy officer for the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the information security officer of the organization, Capriati was the business director of IS, and Beckman was her IS business manager, charged with responsibility for a group of analysts and programmers. Capriati and Beckman had a thorough knowledge of all the systems that were in place at Midwest. The audit group consisted of Tom Cavanaugh and Julie Stiles, who served as internal auditors for the organization.

Nelson knew that IS had generally demanded increasingly higher costs and efforts. Concerns regarding incorrect billing, data theft, waste, fraud, and abuse had risen over the years. Moreover, HIPAA compliance requirements had posed increasing challenges. Nelson wanted his team to revisit current processes, starting with the billing and collection process, and develop a list of significant risks and effective controls to mitigate those risks. He believed that better controls would enable Midwest to improve patient satisfaction and reduce loss of revenues due to incorrect billing, fraud, and other factors by establishing better security processes while ensuring compliance with HIPAA, the Gramm-Leach-Bliley Act, the International Organization for Standardization, the Sarbanes-Oxley Act of 2002, and the Payment Card Industry Data Security Standard. The IS and audit groups had expressed similar sentiments. As Van Horde stated,

The effectiveness of our controls impacts the accuracy of our revenues and thus our bond ratings. For example, incorrect billing could result in a potential understatement of revenues, which in turn would result in a decline in our bond rating. As applications and procedures change, we may have to re-evaluate the risks and implement new controls to mitigate new and existing risks. By improving our audit process, we are also ensuring the protection of our financial and clinical information.

These thoughts were shared by Cavanaugh: “We need to work effectively with our data owners. We have processes in place to ensure that all procedures are adhered to and followed and all data modifications are evaluated on a weekly basis. This is a critical part of our auditing process and continuous improvement.”

During the meeting, Nelson’s message to the IS and internal audit team was going to be clear: “We need to ensure that our practices meet federal, state, and industry regulations and compliance expectations. By placing better controls to meet those expectations, we can also improve our revenues and collection and decrease our operational costs.” Nelson’s plan was to implement important controls identified by the team as quickly as possible.

MIDWEST HEALTH SYSTEM

Founded over 100 years earlier, Midwest was a large regional hospital offering a range of services, including cardiac, cancer, childbirth, emergency medicine, and rehabilitation services. Midwest’s mission was to provide patient-focused care and to create an environment that promoted healing and wellness. To achieve its mission, Midwest had pursued innovation to improve patient satisfaction and service. For example, Midwest implemented an electronic medical records system to allow patients to consult with and receive treatment from different hospitals, patient care units, physicians, and surgeons without having to validate their information and records on every visit. Midwest employed more than 6,000 team members and volunteers, operated more than 1,000 hospital beds, and was staffed by nearly 1,000 physicians. As the second-largest employer in its county, Midwest provided stable jobs and compensation of over $100 million for more than 2,800 employees within the county. Moreover, the health care system supported hundreds of local suppliers, provided charity care, and served as a medical treatment centre for over 600 area physicians. The number of patient days served in 2016 totalled about 80,000, and total revenues exceeded $400 million (see Exhibit 1).

Health care INFORMATION SYSTEMS

Midwest had invested a significant amount of resources in IS (see Exhibit 2). The McKesson STAR system was the billing system for patient accounts. It was used for registering patients, coding patient services, collating patient medical records, and generating and processing all claims.

The Nebo Passport system was a claims management solution that imported claims from the McKesson STAR system. It checked for data integrity and captured bill edits and denials, automatically routing them to assigned staff for correction. This software solution reconciled claims against payments and automated the task of posting payment information from remittance and other billing information. In addition, the Nebo Passport system provided access to various commercial and government payers to verify a patient’s insurance coverage, co-pay amounts, and deductibles and to retrieve claim status. After financial counselling, information was sent to the Nebo Passport system, as were the results of insurance analysis from information obtained from patients during registration. If needed, advanced beneficiary notification was sent to Medicare.[[2]](#footnote-2) The billing department was notified electronically if any problems arose after advanced beneficiary notification.

As a patient received health care services, all information was entered into two systems: the McKesson STAR system and the Cerner computerized physician order entry (CPOE) system. CPOE ensured standardized, legible, and complete orders. When used in combination with clinical decision support systems, CPOE also provided default values for drug doses, routes, and frequencies, simultaneously checking for drug allergies, adverse drug-to-drug interactions, contraindicating laboratory values, and the need for corollary orders. CPOE patient management software was used to enter physician instructions for patient treatment. These orders were communicated over a computer network to medical staff or to various departments, such as pharmacy, laboratory, or radiology, which were responsible for fulfilling the orders. The benefits of CPOE included expediting order completion, reducing errors related to handwriting or transcription, allowing order entry at the point of care or off-site, checking for errors such as duplicate or incorrect doses or tests, and simplifying inventory and the posting of charges. Information on discharge and maintenance services was also entered in the CPOE system. Once orders were completed in the CPOE system, they were generated back in McKesson STAR, and from there the information was consolidated and prepared for billing. The McKesson STAR system validated and produced claims. Invoices were sent to insurance companies and patients by the EC2000 claims administrator module of the McKesson STAR system. Insurance companies typically sent their explanation of benefits to both Midwest and the involved patient. Insurance payments and payments received from the patients were posted in the McKesson STAR system.

Physician offices used two connected software programs similar to McKesson STAR. These programs, Professional Electronic Health Records and Professional Management, handled the financial and billing sides of all physician medical records. A “grouper,” otherwise known as a set of standards, and part of McKesson STAR, was used to include various diagnoses and procedures. Diagnosis-related groups (DRGs) classified various hospital services, used later for billing and reimbursement. DRGs were used in billing Medicare and Medicaid.[[3]](#footnote-3) They also estimated what health care organizations could anticipate in the form of reimbursement. If a patient had many items related to a visit, the grouper classified the most severe DRG. For example, if, after surgery, a patient had bleeding, the actual DRG would change. If a patient was readmitted to the hospital for the same issue within a 30-day period, the hospital had to write off the costs. The goal of this rule was to ensure that hospitals discharged patients when they were fully prepared and safe for home care. If a patient checked out of an emergency room and returned to the same hospital emergency room within 24 hours, the patient’s visit was considered the same. Another application, ProCon Contract Management (ProCon), was used for contract management.

To monitor radiation oncology services and maintain relevant records, Midwest used another software application, called Varian. McKesson STAR obtained this information from Varian in order to generate charges associated with treatment. PeopleSoft was used for general ledger, payroll, and inventory management. This financial application was connected to McKesson STAR and was also used in supply chain management and supply inventory management. Charge master data was used by McKesson STAR to generate the charges associated with each patient’s visit. The charges were typically built according to various transactions that took place during a patient’s visit, and the associated codes were generated as specifically outlined by HIPAA and insurance company policies.

Information Processing

Most patient information was entered into the McKesson STAR system at registration, whereas some was retrieved from previous visits or through pre-certification of patient insurance (see Exhibit 3). After all pertinent information was captured, the McKesson STAR system initiated a face sheet, which was used by the hospital, physicians, and other caregivers to record, view, and update the admitted patient’s health and medical requirements, as well as personal preferences, in an easy-to-use format (see Exhibit 4). Some of the information in the face sheet was passed on to the Nebo Passport system. The registration information was viewed by the financial counselling department to help the patient understand all the financial obligations and payment options. After the patient was formally admitted to the hospital, health care services were initiated. Information on patient care services rendered, discharge, and maintenance were entered into the CPOE, Varian, Professional Electronic Health Records, Professional Management, and McKesson STAR systems. The EC2000 system validated information pertaining to claims. The billing and collection process used the validated information collected from these dispersed systems. McKesson STAR fed the information into ProCON and received expected payments according to the contract with the payer. ProCON provided a validation check to ensure the reimbursement was correct. Information was also retrieved from the McKesson STAR system by the PeopleSoft system for supply chain management activities.

Data from the various applications mentioned above was fed into the respective financial components of PeopleSoft, either in real time or through a batch process. Middleware enabled communication and data management among the distributed applications. Triggers—procedural software codes that were automatically executed in response to events in the database—maintained data integrity. For example, if payment was received from a patient, the information was fed into the financial components, and a trigger was automatically executed to reconcile the patient account records.

Billing and Collection Process

Midwest provided services to three categories of patients: in-patient, outpatient, and emergency. Patient classification as in-patient or outpatient was determined by the physician’s order. The billing and collection process for the first two categories of patients (in-patient and outpatient) started at registration (see Exhibit 5). It was at the registration point that the patient’s identity and demographic and insurance information were captured. Because this information was used by the finance department to bill insurances and patients, accuracy of registration was fundamental for billing services.

Not all patients had insurance coverage. Of those with coverage, some carried private insurance, while others enjoyed Medicare and Medicaid benefits. For a patient with private insurance, the utilization review group contacted the patient’s insurance company to determine the payment criteria for scheduled services. Most medical insurance companies required advance authorization for scheduled in-patient procedures and some outpatient services. This pre-certification process was the responsibility of the patient or the patient’s family and had to be completed before registration. This ensured that the insurance company would cover payment for services performed. In the absence of pre-certification, the utilization review group checked eligibility during registration. This process was basically for claims analysis. For example, if a patient was getting registered for a computer tomography scan with contrast, the registration clerk checked for a pre-certification, as one was required for this particular procedure. If the pre-certification was generated, it was documented; if not, the registration clerk would advise the patient that it was their sole responsibility to bear the full amount. For a Medicare patient, the process was different. Medicare conducted an eligibility check and then informed the patient of their eligibility; this became an informed consent. The patient would be responsible for a large percentage of the bill, as the medical procedure fell outside of Medicare. Medicare and Medicaid published a list of services they covered. Patients with these insurances received an advanced beneficiary notice for services not covered. Financial counselling personnel offered patients who had difficulty making payments various payment options.

Patients could also pre-register at their convenience; doing so saved patients time and increased the accuracy of registration information during the admission process. The procedure for verifying patient information with the insurance company was the same for pre-registered patients. Patients whose insurance companies would not cover the cost of services in full went through a financial counselling process and were offered payment options at registration.

For the third category of patients, those who arrived through the emergency room (about 40 per cent of all patients), registration took place as soon as circumstances allowed or with the assistance of the patient’s companion. According to the Emergency Medical Treatment and Active Labor Act, hospitals had to treat every person that came through the emergency room; otherwise, they would lose the ability to accept Medicare and Medicaid patients.

Regardless of patient classification, if patients did not have insurance coverage, they were responsible for the charges. If requested by the patient, a financial assessment of a patient’s ability to pay was performed by a financial counsellor. If the patient was able to pay, the financial counsellor worked out a payment plan with the patient. If the patient qualified for a charity or another type of financial support, then the financial counsellor assisted the patient in securing it. Midwest had an established charity care policy—essentially a financial needs policy—which required the patient to fill out financial forms and submit documents such as tax returns and bank statements. Midwest then wrote off a portion, or all, of the charges, depending on the financial standing of the patient. The hospital documented these cases to demonstrate its care for the community and to support its not-for-profit status.

After registration and financial counselling, patients (with the exception of emergency patients) were provided the scheduled services. Charges for various services were entered at various times by means of different systems. Via the McKesson STAR system, room charges were automatically posted to the patient’s account at pre-specified rates based on midnight census, depending on type of room and level of care. The patient’s location prior to midnight was irrelevant. For example, if a patient spent time in an intensive-care unit (ICU) after surgery and was moved to a step-down or monitoring unit before midnight, the room charge was that of the step-down unit and not the ICU. There was a five-day cut-off period for entering late charges.

Most other charges were entered through the Cerner CPOE system. However, some charges, such as rehabilitation charges, were entered into the McKesson STAR system. Cerner interfaced with the McKesson STAR system, which meant that the charges entered in Cerner automatically transferred to the McKesson STAR system. An exception was radiology charges, which were first entered into Varian.

Physicians recorded all diagnosis and procedural information on the patient’s face sheet. Medical record personnel coded the bill using current procedural terminology (CPT). CPT coding provided uniform language with which to describe medical services among different parties. For Medicare and Medicaid, CPT and diagnosis codes were then entered into a software program (i.e., the DRG grouper system), which automatically determined the service’s DRG classification.

DRG codes produced by the grouper system determined what the hospital was paid from Medicare and Medicaid. The hospital’s primary payer on the basis of DRG was the government. Midwest relied on the software for the accuracy of such classifications. Once the coding was completed, the coder did multiple edits to ensure all required information had been captured. The coder then produced the claim and entered it into the claim editing system, which had additional edits based on the payer.

The physicians initiated the discharge process. For in-patients, a physician indicated in the face sheet that the patient was to be discharged. The status or mode of discharge was then entered into McKesson STAR. Instructions were sent home with the patient. Once the patient was put on discharge status, a trigger set the end-of-patient-care record. The medical records picked up the discharge information that signalled the medical records to perform abstracts. The abstracts ensured that all billing and other documents needed to bill the patient were present. If all documents were not present, a flag was set in the CPOE system for physicians to complete all documents. The physicians were usually given four to five days to do so. Once the documentation was ready, the flag was reset to proceed with the billing process. At this point, a coder in the medical system began to code the records. The coder looked at the diagnosis of the patient upon discharge and in the medical records. Documents sent to the coder for validation included primary documents dictated by physicians; transcribed surgical operation notes, discharge progress notes, and emergency physician reports; and any images and interpretations. The coder also validated all documents. Once all the deficiencies were remediated and coding was completed, the billing documentation was sent through groupers. Once all services were grouped, the bills were sent to the insurance payers, such as Medicare, Medicaid, workers’ compensation, and other private insurance companies, for payment.

Bills were sent out to insurance payers, the patient, or both, in either electronic or paper form, five days after the patient was discharged. There were three reasons for the five-day billing window: (1) one or more designated charge persons might have fallen behind and thus may not have had the time to enter the charges into the patient’s account; (2) pathology charges were normally received later and had to be manually keyed into the system; and (3) charges for non-standard supplies had to be entered manually. The five-day window allowed assigning charges to many and different patient records.

On occasion, errors would be detected, or charges would come in outside of the five-day window. In those cases, the patient’s bill was edited, and a corrected bill was sent to the insurance company, the patient, or both. After the payer had applied a contractual discount and sent payment to the hospital, the personnel in the patient accounts department posted the payment to the patient’s account against the claim. The revenue was recognized at the time when service was performed.

Roles and Responsibilities of Internal Auditors

Internal auditors were from the IS and finance departments and worked independently of the operations they audited. They had access to all relevant personnel and records. The internal audit group at Midwest reported to the corporate compliance and audit committee (CC&A committee), which met quarterly. It comprised the chief executive officer (CEO); the chief operating officer; the chief financial officer (CFO); the CIO; the president of various hospitals in the system; financial board members, one of whom was the chair of the CC&A committee; the director of corporate compliance; and the director of internal audit (see Exhibit 6). Both the CIO and CFO reported to the CEO administratively. The director of benefits and the director of compliance were heavily involved in the audit. The business director of IS, the HIPAA privacy officer, and the ISO were involved with security, privacy, and IT compliance issues.

The Midwest internal audit group was tasked with the following key responsibilities:

* Evaluate risks and design and implement controls to meet the goals and objectives of the organization with respect to
  + compliance with federal and state regulations;
  + the fair presentation of financial statement items, including revenues and receivables associated with billing and collection activities; and
  + improving the effectiveness and efficiency of operations.
* Conduct a HIPAA Security Rule Administrative Safeguards audit in cooperation with IS compliance and other personnel.
* Plan and complete audits to identify inadequate, inefficient, or ineffective internal controls and to ensure the accuracy of financial information, especially revenues and receivables.
* Manage information services application and infrastructure changes.
* Evaluate and authorize data fixes in data tables, missing data, enrolment files not properly updated, and claims data inaccuracies.
* Conduct critical incident responses, monitoring and remediating them as needed.
* Evaluate information security, privacy, and associated exposures related to HIPAA compliance.
* Participate in the pre-implementation audit of new application software with finance and information services management.
* Monitor the status of internal and external audit exceptions with finance and information services.
* Support anti-fraud programs.

MINUTES FROM THE FIRST MEETING: RISK AND CONTROLS

At the meeting, Nelson and his team agreed that the information system, in general, and the billing and collection process, in particular, posed numerous risks. They decided that both IT general controls (ITGCs) and application controls were needed to mitigate those risks. Instead of identifying specific risks and controls, however, Nelson and his team decided to use the meeting time to identify the general categories and areas of risks and to create a template. Then, over the next several days, each person would develop a comprehensive list of risks and potential controls (see Exhibit 7).

As the meeting ended, Nelson reminded everyone that each risk area could entail several risks and that many controls could be installed to mitigate them. He asked every team member to identify and list all significant risks and controls, expanding the table as needed, and to submit the completed template to him by the end of the week. He agreed to combine everyone’s input into one document, to discuss at the second meeting, scheduled for the following week. Identified risk categories and related controls are discussed below.

IT General Controls

ITGCs applied to all applications, including those related to billing and collection. IS management, systems acquisition and development, change management, access security, and business continuity were all part of ITGCs (see Appendix A).

While ineffective ITGCs by themselves did not translate to misstatements, they may have permitted application controls to fail and allowed misstatements to occur undetected. That is, ITGCs had an umbrella effect over all other controls; they affected the reliability of all information produced by Midwest’s systems and were an integral part of all systems. For example, a weakness in the ITGCs over access security could impede the effectiveness of application controls over billing and collection.

Application Controls

Application controls applied to individual applications. Such controls helped to ensure that transactions were valid, properly authorized, and accurately recorded, processed, stored, and reported. There were three categories of application controls: input, processing, and output. To ensure that all relevant data was captured for processing claims, the patient accounts department prepared a daily report comparing claims that were downloaded from PCON system to those that were imported from the McKesson STAR system. The department checked the totals daily and compared them with the number of claims. Every night, after the department had finished its daily claim routine, the information was sent to the clearing house for processing. The department compared its report for what had been sent with the balancing report of what the clearinghouse had received; this ensured that everything had been transferred correctly. The finance department audited general ledger outputs with supporting documentation.

MINUTES FROM THE SECOND MEETING: RESIDUAL RISKS AND TESTS OF CONTROLS

Nelson started the meeting by saying how impressed he was with the thoroughness and clarity of the lists of risks and possible controls. He wondered, though, if there were any residual risks remaining. In addition, Nelson asked if each team member could suggest at least one test for assessing the operating effectiveness of each control they recommended. The team agreed that this was a good idea. Van Horde noted that, although no system of internal controls would be perfect, thinking through residual risks could potentially identify other significant risks that could be mitigated at a reasonable cost. Cavanaugh added, “We have to make sure controls are operating as designed; otherwise our objectives, including that of reducing the loss of revenues due to incorrect billing, fraud, and other factors, would not materialize.” Beckman suggested that access security and change management were the only significant areas of concern in ITGCs (see Exhibit 8). The entire team seemed to agree.

At the meeting’s conclusion, Nelson asked everyone to submit their answers to him by the end of the week. He stated that there was no need for another face-to-face meeting and that he would collate everyone’s answers into one document and email the document to them for their review. Nelson emphasized that he intended to implement important controls as soon as possible.

SUMMARY

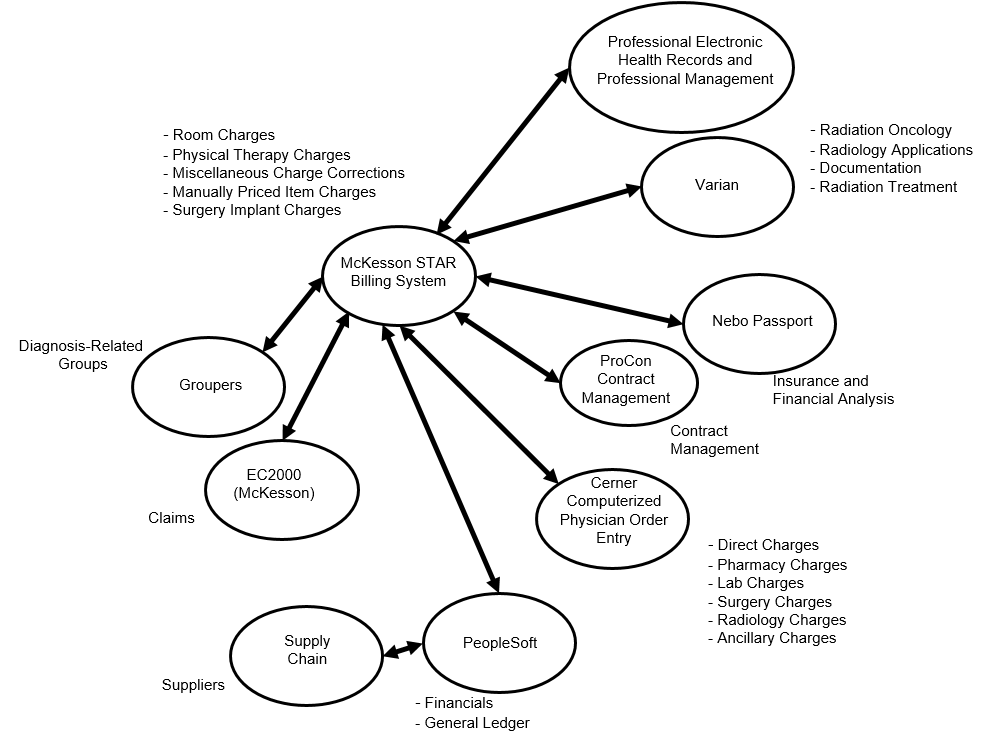
Nelson walked out of the meeting assured that the team would be able to identify all risks related to the billing and collection process, develop effective controls to mitigate those risks, and test them periodically to ensure that they were operating as designed. His confidence in Van Horde, Capriati, and Beckman had grown by the end of the second meeting. He was also satisfied with the work of Cavanaugh and Stiles. He thought that his vision for re-engineering the processes would be a success. The undertaking had the potential to reduce loss of revenues due to incorrect billing, fraud, and other factors by employing better security processes. It would also ensure that his organization was in compliance with HIPAA, the Gramm-Leach-Bliley Act, the International Organization for Standardization, the Sarbanes-Oxley Act of 2002, and the Payment Card Industry Data Security Standard.

Exhibit 1: Midwest Health System Revenues, 2012–2016 (in US dollars)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **2012** | **2013** | **2014** | **2015** | **2016** |
| Contributions and Grants | $1,966,424 | $2,628,344 | $2,795,351 | $3,440,928 | $3,220,079 |
| Program Service Revenue | $67,793,807 | $81,205,762 | $86,611,360 | $367,309,371 | $394,957,158 |
| Investment Revenue | $604,115 | $154,362 | $735,483 | ($1,354,540) | ($777,596) |
| Other Revenue | $2,403,293 | $1,383,530 | $1,116,609 | $29,268,775 | $21,237,837 |
| Total Revenue | $72,767,639 | $85,371,998 | $91,258,803 | $398,664,534 | $418,637,478 |

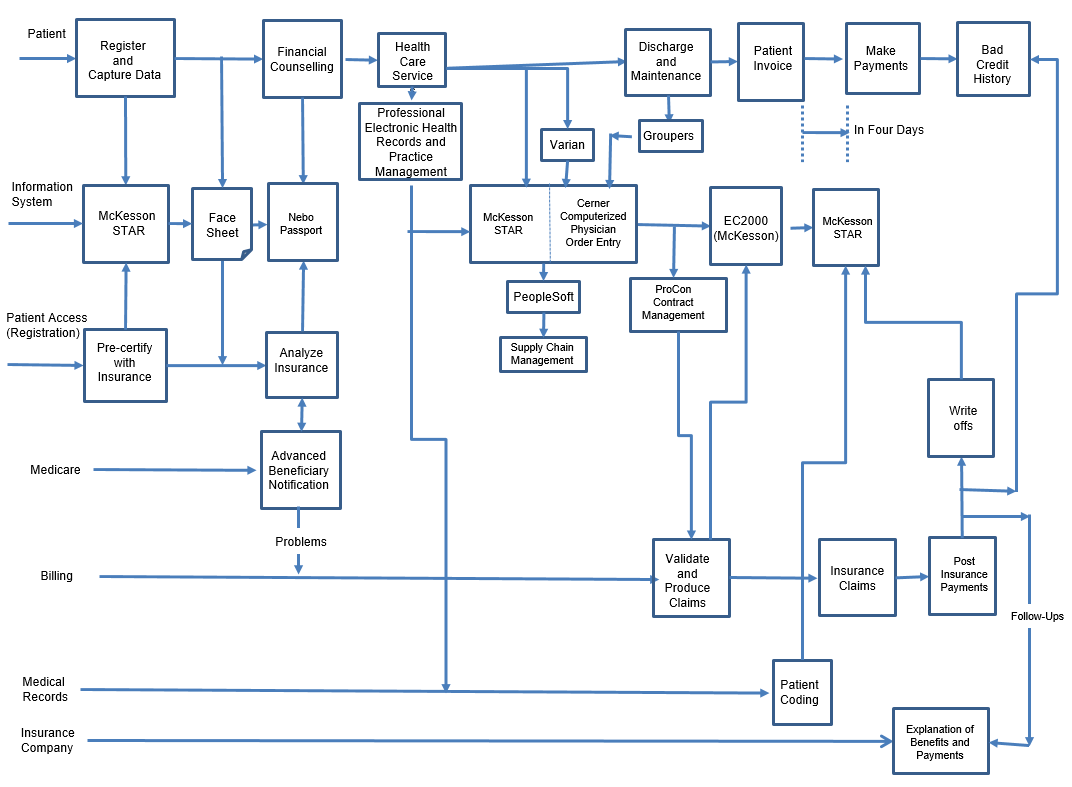
Source: Company files.

Exhibit 2: Enterprise Integration of Information Systems



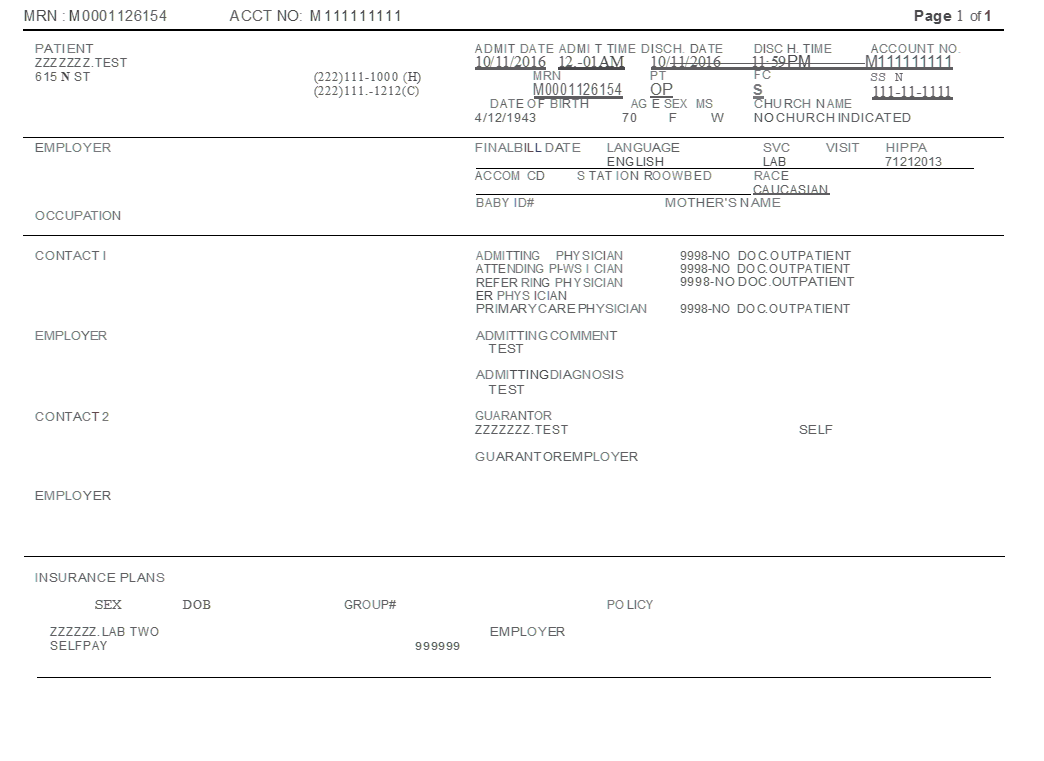
Source: Created by the authors using information supplied by Midwest Health Systems.

Exhibit 3: Information Systems Process Flow



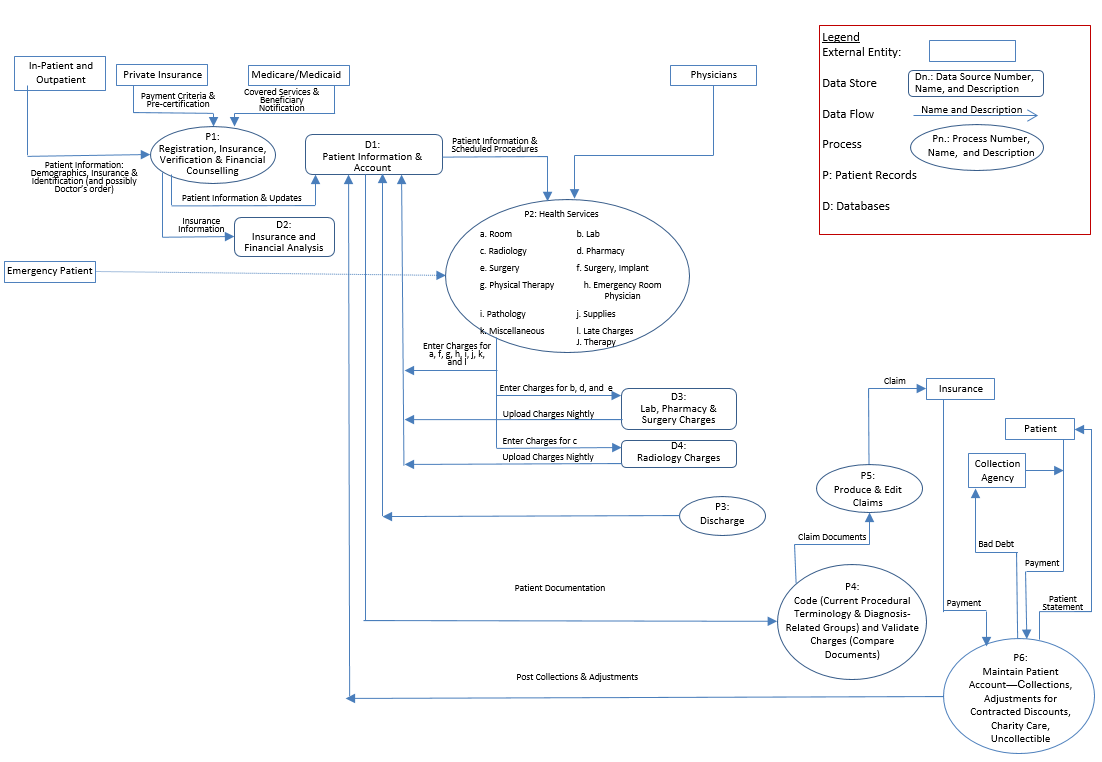
Source: Created by the authors using information supplied by Midwest Health System.

Exhibit 4: Example Face Sheet



Source: Company files.

Exhibit 5: Billing and Collection Process and Associated Data Flow



Source: Created by the authors using information supplied by Midwest Health System.

Exhibit 6: Corporate compliance and audit committee Structure

Chief Operating Officer

Chief Information Officer

Corporate

Compliance Committee

Chief Executive Officer

Presidents of

Various Hospitals

Chief Financial Officer/Controller

Health Insurance Portability and Accountability Act of 1996, Privacy Officer

Director, Internal Audit

Information Security Officer

Director, Corporate Compliance

Business Director, Information Systems

Source: Created by the authors.

Exhibit 7: Risks and Relevant Controls

|  |  |  |
| --- | --- | --- |
| **Area, Activity, or Process** | **Risks of Errors or Fraud** | **Possible Controls to Mitigate Risks** |
| IT general controls:  Overall security | Unauthorized access might affect data integrity (e.g., data could be changed) or data security (e.g., information could be stolen). | Ensure various processes and procedures are in place to authenticate users and limit their physical and logical access according to their responsibilities:  Ensure the data centre is located in an area with secured entry.  Ensure that intrusion detection systems monitor network and system activities for malicious activities and policy violations and produce logs and reports.  Enforce an active directory security policy:   * Logs and reports are reviewed by the system and/or data owners, who respond to those alerts. * The alerts are followed up by process owners and resolved. * Proactive security measures, including patching and anti-virus updates, are implemented regularly. * A PIX firewall is in place for host-based protection. |
| Application control registration | The provision of fake identification by a patient or errors by staff might result in inaccurate registration, inhibiting collection of patient accounts. | Ensure registration staff check patient identification, double check the information, including insurance information and pre-certification, and verbally verify the accuracy of the information with the patient.  Ensure the registration sheet is printed and given to the patient to verify the information.  Have the system retrieve stored information for returning patients. |

Exhibit 7 (CONTINUED)

|  |  |  |
| --- | --- | --- |
| **Area, Activity, or Process** | **Risks of Errors or Fraud** | **Possible Controls to Mitigate Risks** |
| Provision of services:  Pharmacy charges | An incorrect charge or no charge (e.g., medication was dispensed but was not charged, pharmacy charge was not removed if patient did not receive the medication, medication was charged to the wrong account). | Have the system automatically charge the patient’s account when the order is filled.  Ensure medication is dispensed only if there is a charge to the patient’s account.  Ensure the patient’s chart is reconciled with the charges. |
| Claim processing:  Claims were produced after a five-day waiting period and were filed in electronic and paper form | Edit routines might not be up to date.  Coding might be delayed beyond five days. | Independently verify that edit routines are updated on a timely basis.  Ensure that patient accounts billed after eight days following discharge are examined on a sample basis; underlying reasons are investigated. |
| Write-offs:  Uncollectable accounts were written off after unsuccessful attempt by collection agency | Accounts might be improperly written off, because remittances from the collection agency either were diverted or were incorrect. | Depending on the amount, require different levels of authorization to write off accounts.  Test write-off process on an annual basis. |

Note: IT = information technology.

Source: Created by the authors.

Exhibit 8: Risks, Controls, and Tests of Controls

|  |  |  |
| --- | --- | --- |
| **Risks of Errors or Fraud** | **Possible Controls to Mitigate Risks** | **Possible Tests of Controls** |
| Unauthorized access | Only two administrative passwords, with very strong login credentials, were employed. | Ask the information security officer, Van Horde, whether administrative passwords are limited and strong. |
| Failure to verify benefits or obtain pre-certification, which might prevent collection from third-party payers as well as the patient | The insurance benefits were verified, and 100 per cent of all scheduled admissions and procedures were pre-certified.  For patients who were admitted through the ER (e.g., a car wreck), financial counsellors verified benefits as soon as possible. | Ask registration staff about the verification process.  Using a sample, test whether insurance benefits and scheduled admissions were verified.  Observe financial counselling of patients admitted through the ER.  Using a sample of ER admissions, test whether financial counsellors verified benefits and the timing of verification. |

Note: ER = emergency room.

Source: Created by the authors.

Appendix A: Components of information technology Controls at Midwest Health System

Information Systems Management

Key elements in information systems (IS) management included the strategic position of a department within an organization; the alignment of IS goals with the strategic goals of the organization; the use of an IS steering committee; and the proper establishment of roles and responsibilities within an IS department to protect the assets of the organization. The executive team of Midwest Health System (Midwest), which consisted of the three chief medical information officers, the Health Insurance Portability and Accountability Act of 1996 privacy officer, the information security officer (ISO), and the chief information officer, developed IS policies and reviewed the overall operations of the IS department, upon recommendations from directors. Midwest had an IS strategy that was consistent with its corporate strategic plan. The IS strategic plan outlined the objectives and strategies that the IS group would implement to assist Midwest in meeting its overall business objectives.

System Acquisition and Development

The key elements of system acquisition and development were whether the acquisition of new systems or the development of major applications were mapped into the strategic plan; how the internal audit group was involved in those acquisitions and developments; how feasibility studies that reflected technical, financial, and strategic issues were conducted; how security and control features for networks and application were assessed; how pre- and post-implementation project reviews were performed; and whether the testing of developed applications was appropriate and adequate. Midwest mapped system acquisition and development into its strategic plan. The internal audit group was involved with the design, development, and implementation of new software projects. The group also performed post-implementation reviews on all significant projects. The IS department performed feasibility studies on major and important projects. Testing and security assessment and implementation processes were adequate.

Change Management

The key elements of change management included whether formal change management procedures existed; what authorizations and approvals were performed, and how; and how changes were adequately tested, documented, and reviewed by management and owners.

At Midwest, the IS business director was responsible for change management. For all application software changes, the software owner initiated a change request when needed, including required software upgrades. The IS business director’s department maintained a log of all changes and authorized and approved all changes with help from other departments that were involved with the change process. The project team made appropriate changes, and the IS business director approved them. The whole process was documented by the project manager, and the documentation was maintained by the IS business director. The new software was moved to production only after the software owner tested and approved the changes.

Access Security

Access security provided assurance that the computer equipment, programs, and data were physically safeguarded and that only authorized individuals had access to them. On the physical side, access security included physical access and environmental controls over the computer room and data centres. Midwest physically safeguarded its computer equipment, software, and data in a computer room with modern authorization and access protocols, including biometrics and chip access cards with passwords. The computer room was also equipped with modern fire suppression systems.

Appendix A (Continued)

On the logical side, access security included policies related to information security, access on a need-to-know basis, monitoring, and exception reporting. At Midwest, logical access to the system was managed via user profiles, which were based on employee job descriptions and responsibilities. Employees had access only to the software and data that they needed for performing their jobs. Ownership of various systems and the related data were assigned to the person responsible for the related function. For example, the controller owned the general ledger system, the director of material management owned the inventory system, and the director of patient accounts owned the accounts receivable system. Owners of systems signed off annually on who had access to their systems and what access they had. They also approved access and access rights for new employees. When employees were terminated or transferred to other jobs, their access to the system was terminated; in the case of transfer, the employee was granted access privileges for the new position almost immediately. In addition, Midwest security staff conducted a user audit every quarter. The appropriate department manager reviewed electronically submitted reports that listed each user’s profile, noted changes on the reports, and returned the reports to the ISO, who then made the appropriate modifications. When the internal auditors requested access to certain software, they needed to go through a documentation process that kept records of their request and use of the software.

Access to needed programs and data was granted through passwords. Each employee chose a password, which had to consist of alphanumeric characters and one special character, and which could not be a dictionary word. In addition, Midwest hired outside experts to try to find vulnerabilities and crack user passwords. Passwords expired after six months and had to be changed. Employees also had to sign an agreement promising that they would not share their passwords with others.

Business Continuity

Business continuity referred to an entity’s ability to timely recover its processing capability in case of a system failure or catastrophic event. The key elements of business continuity were a written business continuity plan, the plan’s currency, off-site storage of both the plan and data files, and testing the plan.

Midwest did not have a written business continuity or disaster recovery plan. Management believed that such a plan was cost-prohibitive for an organization of its size, and Midwest had never experienced any major business disruption. In case of disaster, the data centre manager would retrieve the most recent backup tapes stored off-site. The data files were incrementally backed up every day and stored in multiple secured places, both on-site and off-site. Midwest would use those stored files to restore its systems, if needed. The plan was last tested in 2016.

Source: Created by the authors using information from Midwest Health System’s personnel.

1. For further information, see “Patient Protection and Affordable Care Act,” HealthCare.gov, accessed September 4, 2019, www.healthcare.gov/glossary/patient-protection-and-affordable-care-act/. [↑](#footnote-ref-1)
2. Medicare was the federal health insurance program for people who were 65 years old or older, as well as for younger people with disabilities or end-stage renal disease (permanent kidney failure requiring dialysis or transplants, sometimes called ESRD). For further information, see “What’s Medicare?,” Medicare.gov, accessed September 4, 2019, www.medicare.gov/what-medicare-covers/your-medicare-coverage-choices/whats-medicare. [↑](#footnote-ref-2)
3. Medicaid provided health coverage to eligible low-income adults, children, pregnant women, elderly adults, and people with disabilities. Medicaid was administered by states, according to federal requirements. For further information, see “Medicaid,” Medicaid.gov, accessed September 4, 2019, www.medicaid.gov/medicaid/index.html. [↑](#footnote-ref-3)