Journal of AHIMA, Roundtable Article

September 2018 Feature Article

Lessons Learned During EHR Downtime

Moderator: **Debra Primeau, MA, RHIA, FAHIMA, President, Primeau Consulting Group, Torrance, CA**

Panelists: Maria Castillo, Health Information Management Director/Privacy Officer, Redlands Community Hospital, Redlands, CA

Stephen Giles, MBA, Chief Information Officer, Hollywood Presbyterian Medical Center, Los Angeles

Gloria Ruiz, MBA, RHIA, CPHA, Former Executive Director, Quality Professional Services, Pacific Alliance Medical Center, Los Angeles

In May 2016, the Office of the National Coordinator for Health Information Technology (ONC) published *ONC Data Brief 35*, which reported 96 percent of U.S. non-Federal acute care hospitals were in possession of a certified EHR.[i] Two months later, in July 2016, the Office of the Inspector General (OIG) issued a report on its study regarding contingency plans for EHRs. OIG surveyed 400 hospitals that had received Medicare incentive payments for a certified EHR as of September 2014.[ii] The hospitals were asked about written EHR contingency plans in relation to the following four HIPAA requirements:

- Data backup plan
- Disaster recovery plan
- Emergency-mode operations plan
- Testing and revision procedures

Nearly all hospitals reported having written EHR contingency plans, and about two-thirds of those plans addressed the four HIPAA requirements reviewed. Over half the surveyed hospitals reported unplanned downtimes, a quarter of which resulted in patient care delays.

In this article, three HIM leaders offer lessons learned during EHR downtime. In May 2018, these HIM professionals participated in a virtual roundtable to share experiences and best practices for managing unplanned or extended downtime. The discussion was moderated by Debra Primeau, MA, RHIA, FAHIMA, president of Primeau Consulting Group.

Primeau: What was the reason for your most recent downtime? How long did it last?

Maria Castillo, health information management director/privacy officer, Redlands Community Hospital (RCH): RCH is a 229-bed, community-based, not-for-profit acute care hospital. Annually, we average 14,000 discharges, 7,000 surgeries, 53,000 emergency visits, and 50,000 clinic encounters.

Our transcription service vendor fell subject to a cyberattack on June 27, 2017, rendering dictation and transcription services completely nonfunctional and inaccessible. One month later, July 28, the vendor

reactivated our servers and recovered all untranscribed dictations. Within four days, the vendor completed the transcription of reports that had been dictated prior to the date of the attack.

Stephen Giles, MBA, chief information officer, Hollywood Presbyterian Medical Center (HPMC), Los Angeles: HPMC is a 424-bed facility averaging approximately 12,000 annual admissions.

Recently, HPMC's system was down for 36 hours with the exception of intermittent two-to-four-hour periods when the system was online and operational. This was a result of a major upgrade that was expected to take 16 to 18 hours. At that time, it seemed we might be back online within a couple hours. As it turned out, HPMC's primary EMR/HIS system was down for 38 hours.

Gloria Ruiz, MBA, RHIA, CPHQ, former executive director of Quality Professional Services at Pacific Alliance Medical Center, Los Angeles: Pacific Alliance Medical Center was a 138-licensed-bed facility in Los Angeles. Annually, the hospital averaged approximately 6,000 inpatient discharges and 22,000 outpatients. The facility officially closed on November 30, 2017 due to massive costs required to retrofit the building to meet California seismic standards—an effort that was financially unfeasible.

On June 14, 2017, Pacific Alliance Medical Center was a target of a ransomware attack that caused certain files on some of its networked servers to become inaccessible when the attacker installed a computer virus that began encrypting files. As a precautionary measure, IT shut down all the networked hospital computer systems, including the primary electronic health record system.

The hospital's primary EHR was affected, as were most interfacing systems, including OB/NB, pharmacy, radiology, and other systems throughout the hospital.

Though some of the primary EHR applications were brought up nine days after the attack, it took an entire month to fully restore operations.

Primeau: How was the downtime identified and communicated to the organization?

Castillo: At 6:34 a.m. on June 27, 2017, the RCH HIM transcription liaison found that the transcription vendor platform was not accessible. By 8:58 a.m. that same day, the vendor's client development executive contacted us to report network problems with their systems. An estimated time of service restoration could not be provided.

Giles: The downtime was intended to upgrade the primary EHR/HIS system and was expected to last 16 to 18 hours. It was scheduled to start at 12:01 a.m. on May 15 and be back up and operational that afternoon or evening. The downtime was planned for that period of time and was communicated accordingly. Unfortunately, the system ended up being down for more than 24 hours.

When the system came back up it ran fine for approximately three to four hours, but then crashed. Using email and phone communications, Information Systems (IS) advised all departments and personnel to resume downtime procedures. The system came back up and stayed up for another hour or so before crashing again at 8 a.m. IS immediately announced across the hospital for all to resume downtime procedures. As of 12 p.m. on May 16, we were still waiting for the system to come back online.

Ruiz: The IT team was alerted by several hospital employees who were unable to access certain files on their workstations. As a precautionary measure, the IT team took prompt action to contain the incident and mitigate associated risks by shutting down all networked hospital computer systems. Internal Triage was called, and departments began their downtime procedures.

Primeau: Does your organization have a formal downtime procedure in place? If so, how frequently do you practice downtime procedures?

Castillo: Yes. We shift to downtime procedures and processes whenever we undergo scheduled system maintenance downtime.

Giles: Yes, we practice downtime once a month during a planned outage for Windows patching of servers and other minor maintenance.

Ruiz: The hospital had a formal downtime procedure as well as many department-specific downtime procedures used during system upgrades. However, after we experienced the days-long downtime, the need for more frequent downtime practices was evident, including periodic practices for longer periods of downtime. Another issue was that hospital departments did not know each other's downtime roles and processes and how they impacted each other.

Primeau: Can you describe the key points of the downtime procedure?

Castillo: Every nursing unit and clinical service maintains a "downtime" box, cabinet, or drawer. The paper-based template of every EHR document for that particular unit/service is in that container. Clinical staff make photocopies of each template as needed. Training for downtime events is an integral part of our new-hire orientation and annual compliance training.

Giles: Downtime is basically a return to a complete paper environment. The most critical point is the sequence of tasks to bring the system back online. Catching up all inpatient ADT activity incurred during downtime is priority number one. Emergency department registration starts up simultaneously for concurrent visits while also catching up ED registrations. Also, we direct pharmacy to catch up entering all medication orders incurred during downtime. All other orders and documentation are scanned into the electronic document management system without catching up on the EMR/HIS primary system. This strategy has proven successful for us and is followed religiously.

Ruiz: Based on our experience, I recommend the following:

- Outline steps to take for various types of downtime—when the entire EHR system is down or when the EHR is available but an important interface may be down.
- Clearly define the assigned roles of the clinical and ancillary departments to ensure proper awareness of procedures.
- Identify departments that will support clinicians by assisting on the units to ensure uninterrupted patient care and safety.
- Outline documentation requirements for managing paper-based records, as many employees have only used the electronic system.

Primeau: What, if any, unanticipated issues did you encounter during the downtime?

Castillo: The non-functionality of transcription services forced physicians to manually write or type their patients' reports. In addition, the options of using speech recognition and electronic documentation templates were strongly encouraged. The unanticipated backlog of untranscribed dictations significantly delayed the clinical documentation, coding, and billing processes, which resulted in our DNFC, DNFB, and AR days tripling.

Giles: The only unanticipated issues we experienced were related to the software upgrade.

Ruiz: The hospital did not anticipate that it would take nine days to a month to bring up all applications and systems.

Primeau: How long did it take to become fully functional post-downtime? What was the process to come back online?

Castillo: On June 29, 2017—48 hours after downtime occurred—we engaged an alternate vendor to immediately provide transcription services. Transcription services were fully functional on August 2, 2017.

Giles: For the typical monthly Windows patching, the time to come back from downtime is usually one hour. Our recent downtime situation extended well beyond that.

Ruiz: Based on the prioritization established by leadership, it took up to one month to become fully functional. The process to come back online involved prioritizing the main patient care applications and systems first, then all remaining EHR applications, all interfaced systems into the EHR, and finally all other systems.

Primeau: Please share your downtime recommendations/best practices.

Castillo: After this experience, the hospital committed to minimizing future risk by engaging more than one vendor for any given contracted service line. This practice allows us to have backup services immediately available at all times for any contracted outsourced service.

Ruiz: Communication is absolutely necessary during extended downtimes. Daily updates are essential to communicate the current status and any new situation developments.

Hospital Recommendations

- Conduct frequent drills on downtime procedures for extended periods of time.
- Practice by calling an internal drill for longer than two to four hours to fully appreciate and understand the impact if the system were to stay down for some time. Include your emergency management team in this drill and critique for improvement opportunities.
- Ensure you have a hospital-wide downtime procedure policy that makes all departments aware of their own responsibilities and those of others.
- If you have a cloud-based or other backup system, do not include it on the hospital network. If the network is taken down, that system will not be accessible.
- Centralize forms control at all units. Since an electronic repository may not be accessible, ensure availability of manual forms.
- Ensure access to Wi-Fi for web-based applications.
- Provide additional department laptops and encrypted USBs.
- Ensure access to a paper-based copy of all policies and procedures in case intranet access is unavailable.

HIM Recommendations

- Design templates and create patient labels for downtime paper-based patient records.

- Dispense an allotment of downtime medical record numbers (MRNs) to the Admitting Department.
- Request that providers dictate their reports. Remind them to check the paper record daily for deficiency completion.
- Routinely print certain HIM reports as backup—such as incomplete records list, ROI pending request reports.
- Be prepared to institute manual processes such as the following:
    - Assemble discharged records into paper folders.
    - Analyze incomplete records manually and organize deficiencies by provider name.
- For Coding/Abstracting, the coders will need to:
    - Obtain paper records and leave out-guides in place of the record.
    - Use paper coding downtime templates and be ready to enter in abstracting system when online.
- For clinical documentation, the CDI specialists will need to:
    - Use paper query templates and chart in the inpatient binder and/or query physicians directly.
    - Ensure the physicians document responses on the paper-based progress note forms.
- Establish post-downtime procedures to:
    - Ensure the accuracy of all manual processes.
    - Update the electronic record system once it becomes available.
- Schedule staff as needed, flexing per department needs.

[i] https://dashboard.healthit.gov/evaluations/data-briefs/non-federal-acute-care-hospital-ehr-adoption-2008-2015.php#appendix

[ii] https://oig.hhs.gov/oei/reports/oei-01-14-00570.pdf

Bio for Debi Primeau, MA, RHIA, FAHIMA

As Primeau Consulting Group's Founder and President, Debi Primeau, MA, RHIA, FAHIMA collaborates with experienced and professional health information professionals to provide documentation and coding audits, health information and project management, information governance and privacy and security consulting services. She has a degree in business management, in addition to a graduate degree in organizational management.