Lessons Learned from an Electronic Health Record Downtime

by Patricia S. Coffey, RHIA, CPHIMS; Susan Postal, DNP, RN-BC; Susan M. Houston, RN-BC, PMP, CPHIMS, FHIMSS; and Jon W. McKeeby, DSc, MBA, CPHIMS

Abstract

Unexpected downtime of an electronic health record (EHR) system poses a risk to patient safety and can result in loss or compromise of data. This article reviews a downtime of the National Institutes of Health Clinical Center EHR system and presents the methodology of the review process, a description of the event, lessons learned, and potential process and policy improvements that can improve a facility's response to unexpected downtime and facilitate smooth transitions to downtime procedures during planned outages.

Keywords: EHR; downtime; IT

Introduction

Electronic Health Record Downtime

An electronic health record (EHR) has many integrated components from the data center to the end user. Each component needs to be working at capacity to ensure that the entire system is available to all users. A failure anywhere along this path will affect performance or access. Because of this scenario, one should not ask *if* a downtime will occur, but *when* it will occur, and what effect it will have on the organization and patient care.[1, 2]

The immediate effect of any unexpected downtime of a clinical system is the risk to patient safety. Information may be lost or compromised, and care providers must revert to a system of manually reporting patient data. For example, during system downtime, orders are handwritten and transcribed into a manual system, and test results are called to the floor or delivered by a messenger. Without the electronic guidance provided by an order form, critical information such as a patient's allergies or medication lists can often be overlooked. Therefore, side effects of system downtime include disruption to clinical workflow, limited access to patient data, increases in patient wait time, staff overtime hours related to reentry of data, and frustration of staff and patients.

Because downtimes are inevitable and lengthy ones can be catastrophic, it is important to have policies, processes, and procedures in place both for the information technology (IT) staff to recover from the downtime and for the clinical staff to continue to provide appropriate care during the downtime. In addition, it is important to have processes and controls in place to reduce the potential of similar system unavailability to occur in the future.

Clinical Research Information System

The National Institutes of Health Clinical Center (NIH/CC) is commonly referred to as America's research hospital. It is exclusively devoted to clinical research, and provides care and services to patients, principal investigators, and research care teams that are a part of the NIH Intramural Research Program. The NIH/CC maintains an EHR system called the Clinical Research Information System (CRIS). CRIS supports approximately 3,200 users and interfaces with all of the typical ancillary systems (e.g., laboratory information system, radiology information system). The Department of Clinical Research Informatics (DCRI) follows a project management methodology that follows the processes published by the Project Management Institute in the fifth edition of *A Guide to the Project Management Body of Knowledge (PMBOK® Guide)*.[3]

Methodology

Healthcare organizations use the lessons-learned approach to identify, review, and communicate experiences within an organization.[4] This process consists of identification of lessons learned from an event. After-action review, change management, or a similar continuous quality improvement process can be used to assess key events to identify areas that can be improved in the future. The process of gathering and documenting lessons learned after an event is an important step for continuous improvement. Something can be learned from every event, whether the event is big or small, unscheduled or scheduled. The intent of the exercise is to identify what went right as well as where improvements can be made. These lessons should feed into future planning or even become part of a standard process.

After the event, the team that was involved is brought together to discuss the lessons from the team members' perspective. While no comment is dismissed, the facilitator has the important role of keeping the meeting in a positive direction. Since this review is retrospective and the focus is on learning for the future, the process should not involve finger pointing or assigning of blame. The basic approach is to be honest and fair without regard to who was involved.[5, 6]

During the meeting, the facilitator may need to rephrase comments to ensure that they are understood and have a positive focus and to clarify why they are important. The lessons-learned documents may be reviewed years later and by staff not involved in the original event, so including the effect will help to define the context of a comment.

> *Original comment:* I never heard from Jane so I wasn't sure when I was needed or what was going on.
>
> *Rephrased comment*: Sending out regular status reports, including the estimated timeline, during the event and to all affected staff will ensure that everyone is aware of progress and schedule.

The comments should include a description of the lesson or recommendation and its effect or importance. The extended downtime of the NIC/CC EHR resulted in many lessons learned that were used to change multiple processes. Both technical staff and users have noticed the improvements.

The Event

On May 13, 2010, the NIH/CC's EHR went down unexpectedly. The cause was a hardware failure that caused corruption in the primary and backup databases. The event resulted in a sudden loss of access to clinical information for all patients in the Clinical Center with a potential effect on patient care and patient safety.

The system components and logs were reviewed, a conference line was opened, and key resources were brought in to assist. Over the next few hours, several attempts were made to restart the system without success. To resolve the hardware failure, a replacement part had to be ordered. After the replacement part was received and installed, the system was restored using the last trusted backup and transaction logs up to the last log, which had possible corrupted data.

The database with the last transaction log was restored to a separate server so that the team could compare the data and identify any missing data that would require manual reentry. Reports were generated to assist users in completing the entry of missing data.

Interface messages from all ancillary systems were then rerun from the time of the downtime. After validation of all components of the system, it was turned over to the end users approximately 33 hours after the failure.

Existing downtime policies at the time were followed during the event. These policies included documentation and communication of results, orders, vital signs, medication administration, and other clinical documentation as well as patient admissions, discharges, and transfers. Reentering the information collected during the extensive downtime was labor intensive and required more than one week. Daily meetings were held with department leadership and quality assurance officers to ensure that all concerns and issues of data reentry were addressed.

The Environment at the Time of the Event

The NIH/CC maintains a primary and secondary data center, each with fully redundant power, network, and cooling with multiple high-bandwidth fiber connections, allowing production systems to run seamlessly on servers in either location. The EHR continuity plan was available but did not address the scenario of both the primary and secondary (replicated) databases being corrupt.

The continuity plan was reviewed regularly, but an actual test was never performed because of the difficulty of coordinating the interruption with the user community. Although actual testing of the failover to the remote storage-area network never occurred, many other elements of the EHR business continuity plan were tested regularly as part of normal business operations. For example, restoring the database and creating a new environment occurred regularly as part of release management and failover of services across servers.

Lessons Learned

Both technical and organizational processes needed to be reviewed and updated where appropriate. Organizational and technical lessons-learned meetings were held after the downtime to address what worked well and what areas needed improvement. As a result of these meetings, multiple committees were created to promote downtime process improvement.

Participation and broad support for these process improvement initiatives extended from the executive level to the user community. Those involved were in agreement that communication was a key focus for improvement and needed to be both effective and timely.[7] The committees addressed the communication of planned and unplanned system downtime, revision of the downtime policy, and the creation of a downtime toolkit.

The main committee formed was the multidisciplinary Downtime Communication, Education, and Training (DCET) committee. The DCET committee met routinely for one year to address improving the communication and education of staff about downtime processes and procedures. The committee continues to meet biannually to review and update the downtime policies and the contents of the toolkits, including the forms, to determine if any modifications are necessary.

Process Improvement from Lessons Learned

Communication

During the downtime, overhead announcements were made within the hospital and e-mails were sent updating the community on the system's status. A command center was set up for executive leadership, which provided centralized communication for the technical team and stakeholders. Clinical and technical staff members made rounds to the patient care and ancillary areas, meeting with the stakeholders to assist with downtime procedures and providing the status of the situation and the plan of action. Minghella[8] recognizes the importance of staff seeing the support of the leadership team visiting the patient care areas.

Downtime Policy Revision

Activities to support unplanned system downtime were reviewed. Processes and actions identified by stakeholders as having been useful during the downtime were added to the policy. Downtime communication templates were updated by subject matter experts to ensure that key information was included if not already captured. These templates addressed various downtimes in a standardized format and identified user and system effects.

Downtime Toolkit

Users had become so accustomed to solely utilizing and documenting in the EHR that they were no longer aware of what paper forms were still applicable for use in a downtime situation.[9] The forms were available on the Health Information Management Department's website; however, they were not grouped in a manner that would make it easy for users to locate them quickly. In addition, since the majority of documentation was being completed within the EHR, the forms had not been reviewed or updated in years.

During a DCET committee meeting, the concept of creating a downtime toolkit was introduced. Paper downtime forms were reviewed and revised by the Clinical Information Management Committee. The downtime toolkit is a plastic storage bin with file folders grouped by category (e.g., orders, progress notes, nursing care, vital signs, input/output, medication administration, and consultation reports) with the appropriate forms for each category included in the folders.

An inpatient unit toolkit and an outpatient clinic toolkit were created. Toolkits were disseminated to all patient care areas. Each area is expected to maintain/restock their toolkit as needed and may contact the Health Information Management Department to replenish the supply of forms. Education has continued with downtime drills scheduled quarterly as a good way to assess staff readiness.[10, 11]

Prepare for Handling Incidents

A DCRI incident response team was created to respond to unexpected system unavailability. A communication plan was created to address activities that should occur before, during, and after the incident. Pre-incident activities include identification by section supervisors of on-call designations for their teams and the creation of downtime contingency plans, checklists, and disaster recovery documents. Documentation is reviewed regularly and stored on a common site.

Activities during the incident include the following: The Systems and Monitoring team notifies the DCRI executive on call of the issue; contacts appropriate teams; notifies the user community and, when possible, provides an estimated time for resolution via e-mail and an overhead page; and opens up a conference phone line. For major unplanned downtime, the Project Management Office documents the incident and the response as tasks in a project plan. The DCRI executive communicates the severity of the downtime to various levels of NIH/CC executive leadership.

Postincident activities are as follows: The Systems and Monitoring team notifies the user community of system availability via e-mail and an overhead page; a technical point of contact documents the downtime; the Project Management Office develops an incident response report, which is reviewed by the Technical Review Board; and the Technical Review Board completes a root-cause analysis, which is presented to the chief information officer.

Manage System Availability

From a user and executive management perspective, a 99.999-percent system availability target is desired. The current system availability target is 99.9 percent, which means approximately nine hours per year of both planned and unplanned downtimes across all components of the EHR system. The target system availability, including the risks and controls, should be determined and reviewed with executive leadership of the organization.[12–14] The target will depend on many factors. A target of 99.9 percent is acceptable in the NIH/CC because it has no emergency room or labor and delivery department.

To maintain the current target at the NIH/CC, the extended downtime demonstrated the need to focus on managing system availability as part of all system operations and projects. New processes were also implemented to ensure that the EHR continuity plan is reviewed prior to any planned system change. System changes and updates go through a formal change management process, while upgrades and new modules go through the project management process.

Backup Systems

The review of the continuity plan revealed the need to have an additional backup system available for planned and unplanned interruptions. It was determined that the Clinical Center needed two new environments: a read-only system and a warm site. The read-only system would be available for any scheduled downtime and would provide an option for use in instances of unscheduled downtime, depending on the expected duration.

A project team was formed to work with the vendor and outline different technical options for the read-only system. Each option was evaluated and documented, including a description, effects, advantages, and disadvantages. The final decision was to utilize log shipping in the short term and evaluate moving to mirroring or another technology in the future. The read-only system, and the process of activation and restoration, is validated with each upgrade of the EHR system.

The decision on when this system would be made available was based on the duration of the work required to make it active for the users. The read-only system requires approximately 90 minutes to be made available. This system is utilized for any scheduled downtime longer than two hours or unscheduled interruptions that may extend that long.

Another decision that had a huge effect on the end users was how to distinguish the view-only system from the production environment EHR. The same icon was used, but with a black and white color scheme and a different name. The icon was also made to be viewable only at the end of the tasks required to activate the system.

The warm site is a fully redundant system for use in the event of a long unplanned interruption. The process of log shipping was also used for the warm site, which is made available to users during any unscheduled interruption that is expected to last longer than four hours.

This warm site does not share any hardware with the production system and has no direct link to the production database. This setup is to avoid any effect on the backup system of a failure of any or all of the primary system. Full testing of the warm site remains a challenge because of the potential of a longer-than-expected downtime and the risk of outage. These risks need to be balanced with the need for confidence in system design and recovery procedures; however, production system uptime was deemed most important.

Future Technical Enhancements

The system availability goal for 2016 is 99.99 percent. To reach this goal, Microsoft SQL Always On technology is being implemented with an expected activation in the spring of 2016. This technology provides improved functionality for failover and redundancy. The architecture design has been reviewed, documented, and approved. A full failover test is planned prior to the activation, and the process will be fully documented.

Virtualization of all components of the EHR system except for the database component is scheduled to be implemented with the new architecture mentioned above. Virtualization will enhance the ability to restore an environment in a different location quickly.

Conclusion

The NIH/CC utilized the opportunity of this extensive system downtime to thoroughly evaluate policies and procedures and conduct a thorough lessons-learned exercise. Downtime procedures are continually reviewed and enhanced on a regular basis and as system functionality changes. While no additional extensive system downtimes such as the one described in this article have occurred, staff are

now thoroughly familiar with downtime procedures and can execute smooth transitions to downtime procedures during planned outages. Ng states: "Downtime events are here to stay and while it is irrefutable that unplanned ones are not desired, planned ones will always be required."[15] Downtimes affect all organizations; however, it is important to maintain technology to reduce system downtime and to maintain a robust IT infrastructure. Maintaining a strong infrastructure, monitoring tools, ensuring a culture of high system availability, conducting frequent reviews of the business continuity documentation, and testing procedures at regularly scheduled intervals are keys to meeting a high target level of system availability.

Acknowledgment

The authors would like to acknowledge the contributions of Tim Maloney, Alex Gregg, Tom Dawson, Barrett Grieb, Steve Bergstrom, and John Kocher to this paper.

Patricia S. Coffey, RHIA, CPHIMS, is the chief of the Health Information Management Department at the National Institutes of Health Clinical Center in Bethesda, MD.

Susan Postal, DNP, RN-BC, is the supervisory nurse consultant in the Department of Clinical Research Informatics at the National Institutes of Health Clinical Center in Bethesda, MD.

Susan M. Houston, RN-BC, PMP, CPHIMS, FHIMSS, is chief of the Portfolio Office in the Department of Clinical Research Informatics at the National Institutes of Health Clinical Center in Bethesda, MD.

Jon W. McKeeby, DSc, MBA, CPHIMS, is the chief information officer at the National Institutes of Health Clinical Center in Bethesda, MD.

Notes

1. Ng, S. "Meet an Informaticist: Downtimes Are . . . Inevitable." HIMSS News. February 10, 2014. Available at http://www.himss.org/News/NewsDetail.aspx?ItemNumber=28123.
2. Nelson, N. C. "Downtime Procedures for a Clinical Information System: A Critical Issue." *Journal of Critical Care* 22, no. 1 (2007): 45–50.
3. Project Management Institute. *A Guide to the Project Management Body of Knowledge (PMBOK® Guide)*. 5th ed. Philadelphia, PA: Project Management Institute, 2013.
4. Savoia, E., F. Agboola, and P. D. Biddinger. "Use of After Action Reports (AARs) to Promote Organizational and Systems Learning in Emergency Preparedness." *International Journal of Environmental Research and Public Health* 9, no. 8 (2012): 2949–63.
5. Ibid.
6. Aiello, B., and L. Sachs. *Configuration Management Best Practices: Practical Methods That Work in the Real World*. Upper Saddle River, NJ: Addison-Wesley, 2011, p. 166.
7. Fahrenholz, C. G., L. J. Smith, K. Tucker, and D. Warner. "Plan B: A Practical Approach to Downtime Planning in Medical Practices." *Journal of AHIMA* 80, no. 11 (2009): 34–38.
8. Minghella, L. "Be Prepared: Lessons from an Extended Outage of a Hospital's EHR System." Healthcare Informatics. August 30, 2013. Available at http://www.healthcare-informatics.com/article/be-prepared-lessons-extended-outage-hospital-s-ehr-system.
9. Kilbridge, P. "Computer Crash—Lessons from a System Failure." *New England Journal of Medicine* 348, no. 10 (2003): 881–82. Available at http://ehealthecon.hsinetwork.com/NEJM_downtime_2003-03-06.pdf.
10. Nelson, N. C. "Downtime Procedures for a Clinical Information System: A Critical Issue."
11. Fahrenholz, C. G., L. J. Smith, K. Tucker, and D. Warner. "Plan B: A Practical Approach to Downtime Planning in Medical Practices."
12. Nelson, N. C. "Downtime Procedures for a Clinical Information System: A Critical Issue."
13. Fahrenholz, C. G., L. J. Smith, K. Tucker, and D. Warner. "Plan B: A Practical Approach to Downtime Planning in Medical Practices."
14. Minghella, L. "Be Prepared: Lessons from an Extended Outage of a Hospital's EHR System."
15. Ng, S. "Meet an Informaticist: Downtimes Are . . . Inevitable," p. 4.