Department of Health and Human Services

OFFICE OF INSPECTOR GENERAL

HOSPITALS LARGELY REPORTED ADDRESSING REQUIREMENTS FOR EHR CONTINGENCY PLANS

Daniel R. Levinson
Inspector General

July 2016
OEI-01-14-00570

EXECUTIVE SUMMARY: HOSPITALS LARGELY REPORTED ADDRESSING REQUIREMENTS FOR EHR CONTINGENCY PLANS
OEI-01-14-00570

WHY WE DID THIS STUDY

Disruptions, such as natural disasters or technical malfunctions, can make electronic health records (EHRs) unavailable to hospital staff. Prior OIG work found, for example, that hospitals experienced substantial challenges responding to the effects of Superstorm Sandy, which included damage to health information systems and curtailed access to patient medical records. More recently, cyberattacks on hospitals have similarly prevented or limited access to EHRs. The Office for Civil Rights (OCR) enforces the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, which requires all covered entities to have a contingency plan for responding to disruptions to electronic health information systems. Contingency plans specify processes to recover EHR systems and access backup copies of EHR data in the event of a disruption. This evaluation provides information about the status of hospitals' contingency plans in light of evolving threats to their electronic health information systems.

HOW WE DID THIS STUDY

We sent a questionnaire to a projectable sample of 400 hospitals that received Medicare incentive payments for using a certified EHR system as of September 2014. We asked hospitals about their EHR contingency plans in relation to the following: HIPAA requirements, the practices for contingency planning recommended by two Federal agencies, and hospitals' experiences with EHR disruptions. To gain a deeper knowledge of hospital EHR contingency plans and experiences, we also conducted site visits at six hospitals, where we interviewed hospital staff and reviewed EHR contingency plans and related documents.

WHAT WE FOUND

Almost all hospitals reported having written EHR contingency plans, and about two-thirds reported that their contingency plans addressed the four HIPAA requirements we reviewed, i.e., having a data backup plan, having a disaster recovery plan, having an emergency-mode operations plan, and having testing and revision procedures. Most hospitals also reported implementing recommended practices, such as maintaining backup copies of EHR data offsite, supplying paper medical record forms for use when the EHR is unavailable, and training and testing staff on contingency plans. Over half of hospitals reported an unplanned EHR disruption, and about a quarter of those experienced delays in patient care as a result. Finally, we found that OCR considers HIPAA compliance broadly and does not target EHRs when reviewing a covered entity's contingency plans.

WHAT WE CONCLUDE

Persistent and evolving threats to electronic health information reinforce the need for EHR contingency plans. This review and cyberattacks that have occurred since 2014 underscore our previous recommendation that OCR fully implement a permanent audit program for compliance with HIPAA.

TABLE OF CONTENTS

OBJECTIVES

1. To determine the extent to which hospitals report that their electronic health record (EHR) contingency plans complied with the Health Insurance Portability and Accountability Act (HIPAA).
2. To determine the extent to which hospitals implemented recommended practices related to EHR contingency plans.
3. To describe hospitals' experiences activating their EHR contingency plans.
4. To describe how Office for Civil Rights (OCR) oversight of HIPAA identified and addressed concerns with EHR contingency plans.

BACKGROUND

Disruptions, both planned and unplanned, may make EHRs unavailable to hospital clinicians and other staff for day-to-day business operations. For example, prior OIG work found that hospitals experienced substantial challenges responding to Superstorm Sandy, including damage to health information systems and problems accessing patients' medical records.[1]

More recently, cyberattacks on hospitals have posed a new threat to EHRs. In 2014, Boston Children's Hospital suffered a distributed denial of service attack. Though no data were lost and no patient harm occurred, some of the hospital's systems lost Internet-based functionality. The hospital relied on its contingency planning and work arounds to continue operating.[2] In January 2016, a hospital in California reported that it suffered a ransomware attack that disabled its network and EHR system for about a week, leading to delayed patient care and the need to divert patients to other facilities.[3] In March 2016, MedStar Health reported a suspected ransomware attack that forced it to take computer systems offline throughout its entire system, including 10 hospitals.[4,5]

Planned disruptions occur when hospitals are updating or replacing hardware or software or conducting tests. Unplanned disruptions result from natural disasters,

---

[1] OIG, *Hospital Emergency Preparedness and Response During Superstorm Sandy*, OEI-06-13-00260 (September 2014).
[2] Daniel J. Nigrin, "When 'Hacktivists' Target Your Hospital," *New England Journal of Medicine*, 371, 393-395 (2014).
[3] Richard Winton, "Hollywood Hospital Pays $17,000 in Bitcoin to Hackers; FBI Investigating," *Los Angeles Times*, February 18, 2016.
[4] John W. Cox, "MedStar Health Turns Away Patients After Likely Ransomware Cyberattack," *Washington Post*, March 29, 2016.
[5] Ransomware is a type of malware that prevents or limits users from accessing their systems. This type of malware forces its victims to pay a ransom to access to their systems or retrieve their data.

power outages, technical malfunctions, or malicious actions, among other events. Contingency plans specify processes to recover EHR systems and access backup copies of EHR data in the event of a disruption.[6] They also outline processes to minimize EHR disruptions and ensure the continuity of care when disruptions occur.[7] Hospitals may maintain their contingency plans in a single plan or may describe them across multiple plans, each covering a specific unit, department, or information system.

Health Insurance Portability and Accountability Act

The HIPAA Security Rule establishes various safeguards to ensure the confidentiality, integrity, and availability of individuals' electronic protected health information. EHRs are one of many applications that store such information. Others include computerized order-entry systems for physicians; claims processing applications; and radiology, pharmacy, and laboratory systems. The HIPAA Security Rule applies both to covered entities (i.e., health plans, health care clearinghouses, and most health care providers) and their business associates (generally, vendors or contractors that store or transmit electronic protected health information).[8, 9]

HIPAA Requirements for Contingency Planning

The HIPAA Security Rule requires that each covered entity have a contingency plan for responding to events that disrupt systems containing electronic health information.[10] HIPAA requirements are not prescriptive in how covered entities develop and use contingency plans. However, contingency plans must include policies and procedures in the following five areas:

- a data backup plan for creating and storing copies of electronic health information (required);
- a disaster recovery plan for restoring lost data (required);
- an emergency mode operations plan for continuing critical business processes during emergencies (required);
- testing and revising of contingency plans (addressable); and

---

[6] Office of the National Coordinator for Health Information Technology (ONC), *SAFER Self-Assessment Guide: Contingency Planning* (January 2014). Accessed at http://www.healthit.gov/safer/sites/safer/files/guides/safer_contingencyplanning_sg003_form_0.pdf on Nov. 5, 2014.
[7] Ibid.
[8] 45 CFR pts. 160 and 164, subpts. A, C, and E.
[9] The Health Information Technology for Economic and Clinical Health Act (HITECH) of 2009 further strengthened the civil enforcement of the HIPAA rules. HITECH § 13410.
[10] 45 CFR § 164.308(a)(7).

- an applications and criticality assessment (addressable).[11]

Recommended Practices for Contingency Planning

Two Federal agencies have recommended practices for contingency planning. The National Institute for Standards and Technology (NIST) offers a comprehensive guide on contingency planning for information systems. The Office of the National Coordinator for Health Information Technology (ONC) provides a contingency planning guide with recommendations specific to EHRs.

NIST's guide on contingency planning outlines a seven-step process to develop and maintain contingency plans for information systems. The guide includes numerous approaches for recovering information system services after a disruption.[12] Although NIST guidance applies only to Federal information systems, it is an accepted source of recommended practices by the wider information-systems industry.

ONC produced a series of Safety Assurance Factors for EHR Resilience (SAFER) guides to help hospitals mitigate patient-safety risks related to EHRs; one addresses contingency planning. Unlike NIST's guide, which applies generally to information systems, ONC tailored its guide to hospitals' EHR systems. ONC's contingency planning guide describes 10 recommended practices for minimizing and reducing the effects of EHR disruptions. It also provides a rationale and advice for implementing those recommendations.[13]

For example, the HIPAA requirement for a data backup plan states that a covered entity or business associate must "establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information," yet it does not offer specific practices for meeting that requirement.[14] However, the NIST- and ONC-recommended practices that align with this requirement offer specific actions, such as maintaining backup copies, storing backup data offsite, and having a read-only system. See Appendix A for NIST's and ONC's recommended practices for contingency planning and Appendix B for a table that shows how they relate to HIPAA requirements.

---

[11] "Addressable" implementation specifications provide covered entities additional flexibility in determining whether these are reasonable and appropriate security measures to apply within their particular security frameworks.
[12] NIST, *Contingency Planning Guide for Federal Information Systems* (May 2010).
[13] ONC, *SAFER Self-Assessment: Contingency Planning* (January 2014).
[14] 45 CFR § 164.308(a)(7)(ii)(A).

Office for Civil Rights Enforcement of the HIPAA Security Rule

Since 2009, OCR has been responsible for enforcing the HIPAA Security Rule.[15] OCR enforces and administers the HIPAA Security Rule in several ways:

- investigating complaints, which could result in corrective action, payment of a resolution amount, or civil money penalties;
- performing compliance reviews in response to breach notifications or other events; and
- providing education and outreach. [16]

The HITECH Act requires the Department of Health and Human Services (HHS) to perform periodic audits of covered entities' and business associates' compliance with HIPAA.[17] OCR made progress toward meeting the requirement by launching a pilot audit program and evaluating the program's results.[18] In March 2016, OCR announced that phase 2 of that program was underway. In these audits, OCR will review the policies and procedures adopted and employed to meet selected standards and implementation specifications of the Privacy, Security, and Breach Notification Rules.[19]

Related Office of Inspector General Work

In 2015, the Office of Inspector General (OIG) released two reports as part of its body of work on the security of health information. One report found that OCR investigated possible noncompliance with privacy standards primarily in response to complaints and had not fully implemented the audit program required by the HITECH Act to proactively identify possible noncompliance by covered entities.[20] The second report found that OCR investigated all large breaches, as required by its policy, but it did not record small-breach information in its case tracking system, limiting its ability to track and identify covered entities with multiple small breaches.[21] Those reports made a number of recommendations to OCR,

---

[15] In 2003, HHS delegated the authority to enforce the HIPAA Security Rule to the Centers for Medicare & Medicaid Services (CMS). In 2009, it transferred this responsibility to OCR.
[16] OCR Enforcement of Privacy and Security Rules. Accessed at http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/enforcement-process/index.html on December 21, 2015.
[17] HITECH Act, §§ 13411.
[18] OCR, *Audit Program*. Accessed at http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/ on March 10, 2016.
[19] OCR, *Audit Program*. Accessed at http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/index.html on June 2, 2016.
[20] OIG, *OCR Should Strengthen Its Oversight of Covered Entities' Compliance With the HIPAA Privacy Standards*, OEI-09-10-00510 (September. 2015).
[21] OIG, *OCR Should Strengthen Its Followup of Breaches of Patient Health Information Reported by Covered Entities*, OEI-09-10-00511 (September 2015).

including that it fully implement a permanent audit program, improve its case tracking system, and expand education and outreach.

In 2014, an OIG evaluation found that most hospitals experienced substantial challenges in responding to Superstorm Sandy, including damage to health information systems and problems accessing patient medical records. Hospitals reported that their prior emergency planning was valuable during the storm, but that they subsequently revised their plans as a result of lessons learned.[22]

METHODOLOGY

Scope

This inspection is limited to contingency plans for protected electronic health information stored in hospitals' EHRs. We limited our population to hospitals that have received EHR incentive payments from CMS to ensure that hospitals had begun using EHRs to record and provide care. Our evaluation used four HIPAA-required criteria as well as NIST- and ONC-recommended practices that we determined were relevant and appropriate to hospitals' EHR systems. Although HIPAA requires hospitals to include criticality assessments in their contingency plans, we did not ask about these assessments because we focused on one information system—EHRs—that we presume to be critical. Covered entities are not required to implement recommended practices from NIST and ONC to be compliant with the HIPAA Security Rule.

Data Sources

Sample Selection: We used CMS's National Level Repository database to identify all hospitals that received Medicare incentive payments for using a certified EHR as of September 2014 (3,949 hospitals). We then stratified our population by hospital size, using bed count data from CMS's Certification and Survey Provider Enhanced Reporting (CASPER) system. The first stratum included 1,221 hospitals with 50 or fewer beds (small hospitals). The second stratum included 2,728 hospitals with more than 50 beds (large hospitals). From this population, we randomly selected 200 hospitals from each stratum for a total sample size of 400.

Hospital Questionnaire: We administered an online questionnaire to our sampled hospitals between May and July 2015 to learn whether hospitals had contingency plans for their EHR systems, as required by HIPAA. Because HIPAA requirements do not prescribe how providers should meet the requirements for contingency planning, we asked hospitals whether they implemented practices

---

[22] OIG, *Hospital Emergency Preparedness and Response During Superstorm Sandy*, OEI-06-13-00260 (Sept. 2014).

recommended by NIST and ONC for EHRs. We used this information to learn how hospitals were carrying out contingency planning and to help substantiate their self-reported HIPAA compliance. The questionnaire also asked about hospitals' experiences activating their contingency plans in the year preceding our questionnaire. We obtained an 86-percent overall weighted response rate. The response rate for small hospitals was 84 percent and the response rate for large hospitals was 87 percent. We analyzed the questionnaire results as a whole and by strata. We also determined whether the difference in the point estimates were statistically significant between strata by using independent group t-tests. See Appendix C for point estimates, 95 percent confidence intervals, and results of these statistical tests.

Hospital Site Visits: To further our understanding of EHR contingency plans, we chose six hospitals for site visits on the basis of geographic diversity, bed count, and experience activating their contingency plans, as reported in their questionnaire responses. While onsite, we interviewed hospital staff knowledgeable about their hospitals' EHR contingency plans, including the Chief Information Officer, Chief Technology Officer, Director of Information Technology (IT), Chief Information Security Officer, facilities managers, IT analysts, and nursing informaticists.[23] We reviewed the hospitals' EHR contingency plans and related documentation such as reports assessing testing and training for those plans. We conducted these site visits in June and July 2015.

OCR Interviews: We interviewed OCR staff about their policies and procedures for investigations and compliance reviews. We also asked staff about the status of the HIPAA audit program.

Limitations

Our analysis used self-reported data from hospitals. We did not independently verify their responses. We did not require hospitals to submit copies of their contingency plans to support their questionnaire responses, for several reasons. For example, hospitals may not consolidate contingency plans into a single document; a hospital may maintain plans for each unit, department, or information system. We also note that hospitals that were not compliant with HIPAA contingency planning requirements may have been less likely to respond to our questionnaire.

---

[23] Nursing informatics is the specialty that integrates nursing science with multiple information-management and analytical sciences to identify, define, manage, and communicate data, information, knowledge, and wisdom in nursing practice. Accessed at http://www.himss.org/resourcelibrary/TopicList.aspx?MetaDataID=767 on June 2, 2016.

Standards

This study was conducted in accordance with the *Quality Standards for Inspection and Evaluation* issued by the Council of the Inspectors General on Integrity and Efficiency.

FINDINGS

Almost all hospitals reported that they had written EHR contingency plans, and about two-thirds of hospitals reported that their contingency plans addressed all four HIPAA requirements that we reviewed

Ninety-five percent of hospitals reported that the written policies and procedures in their EHR contingency plans specify how to respond to EHR disruptions.[24] The other 5 percent of hospitals reported that they did not have EHR contingency plans. Some of the hospitals without contingency plans noted in their responses that they were developing contingency plans at the time of our questionnaire because they had only recently adopted EHR systems. Other hospitals noted that they had implemented practices related to contingency plans but did not document those practices in policies or procedures.

Most hospitals' contingency plans addressed three of the four specific HIPAA requirements to have a data backup plan, a disaster recovery plan, and an emergency mode operations plan (see Table 1). Less than three-quarters of hospitals reported that their EHR contingency plans or equivalent alternative plans addressed testing and revision procedures. HIPAA allows hospitals to address testing and revision in their EHR contingency plans or in an equivalent alternative.[25] That may explain why fewer hospitals addressed it in their plans. Sixty-eight percent of hospitals' contingency plans addressed all four HIPAA requirements.

Table 1. Hospitals That Reported Having Written Contingency Plans Addressing HIPAA Requirements

HIPAA Requirement*	Percentage of Hospitals
Data backup plan	83%
Disaster recovery plan	95%
Emergency mode operations plan	95%
Testing and revision procedures	73%

Source: OIG analysis of hospitals' responses to EHR contingency plan questionnaire, 2015.

* The HIPAA requirement of criticality assessment procedures was outside the scope of this evaluation and not included in this analysis.

[24] The scope of our analysis is limited to hospitals that received Medicare incentive payments for using a certified EHR as of September 2014.

[25] 45 CFR § 164.306(d)(3).

Large hospitals were more likely to report having a written EHR contingency plan than small hospitals (see Appendix C for details).

Most hospitals reported implementing recommended practices related to data backup and emergency mode operations

Hospitals reported taking actions to implement practices recommended by NIST and ONC for each of the four HIPAA requirements for contingency plans that we reviewed: data backup, disaster recovery, emergency mode operations, and testing and revision. Recommended practices related to backing up, storing, and maintaining data; using paper records; and having alternative power sources (e.g., generators) were among the most commonly implemented (reported by 90-100 percent of hospitals). The recommended practices of NIST and ONC are not required under the HIPAA Security Rule, but they are sources of best practices relied upon by government and industry.

For certain recommended practices, the percentage of hospitals reporting having implemented them sometimes exceeded the percentage of hospitals reporting having written contingency plans. This may be because hospitals carry out certain recommended practices, but not under a formal contingency plan. For example, in our questionnaire, two hospitals explained that although they did not have detailed, written EHR contingency plans, each department has processes it follows in the event of a disruption to the EHR system.

Data Backup:

During EHR disruptions, hospitals rely on backup copies to restore EHR systems with minimal data loss. Backup copies also allow clinical staff to view EHR data when they cannot access their primary EHR system.

Nearly all hospitals reported that they maintained backup copies of their EHR data. Of the hospitals that maintained backup copies, almost all reported implementing the recommended practice to back up data at least once per day. Hospitals may rely on multiple methods to back up data. For example, one hospital we visited told us that it replicated data on a secondary server continuously and backed up data to media—either a tape or disk—every 4 hours.

Just over half of hospitals reported that they had read-only systems that display backup EHR data. Hospitals we visited told us that during EHR disruptions, staff may access read-only systems on dedicated computer terminals or through icons that information technology (IT) staff enable on normal computer workstations. However, only 32 percent of hospitals reported that their read-only system was visually differentiated from their fully operational system. These visual clues are intended to help staff instantly recognize that the hospital has activated its

contingency plan. See Table 2 for the recommended practices that hospitals reported implementing for data backup.

Table 2: **Hospitals That Reported Implementing Recommended Practices for Data Backup**

Recommended Practice from NIST and ONC	Percentage of Hospitals
Maintain backup copies	99%
Store backup data offsite	92%
Back up data daily, or more frequently	91%
Have a read-only EHR system *	57%
Visually differentiate read-only system *	32%

Source: OIG analysis of hospitals' responses to EHR contingency plan questionnaire, 2015.

* Indicates that large hospitals are more likely to include the recommended practice than small hospitals.

Disaster Recovery: Hospitals can mitigate technology failures by having duplicate EHR hardware at an alternate site. Hospitals can also minimize EHR disruptions by duplicating their Internet connections.

About three-quarters of hospitals reported having alternate sites, and more than half implemented the recommended practice of having "warm" or "hot" sites to operate their EHR systems when their primary EHR systems malfunction.[26] Almost half of hospitals with alternate sites reported that they can transfer EHR operations within the recommended 8 hours. One hospital that we visited told us that it requires a formal decision process before transferring to an alternate site. This hospital reported that it took about 2 hours to transfer to its alternate site and about 2 hours to switch back to the primary EHR system. Only about a quarter of hospitals reported testing their alternate systems at least every 3 months. See Table 3 for the recommended practices that hospitals reported implementing for disaster recovery.

[26] A "hot" site is an alternate facility appropriately sized to support EHR system requirements and configured with the necessary system hardware, supporting infrastructure, and support personnel. A "warm" site is a partially equipped alternate office space that contains some or all of the EHR system hardware, software, telecommunications, and power sources. A "cold" site is an alternate facility with adequate space and infrastructure (electric power, telecommunication connections, and environmental controls) to support EHR system recovery activities.

Table 3: **Hospitals That Reported Implementing Recommended Practices for Disaster Recovery**

Recommended Practice from NIST and ONC	Percentage of Hospitals
Determine a strategy to replace damaged equipment	87%
Have at least two Internet paths *	78%
Have at least two Internet providers *	67%
Have a "warm" or "hot" alternate site *	56%
Transfer operations to the alternate site within 8 hours *	46%
Locate the alternate site 50 miles from the primary site	31%
Test the alternate site at least quarterly	25%

Source: OIG analysis of hospitals' responses to EHR contingency plan questionnaire, 2015.

* Indicates that large hospitals are more likely to include the recommended practice than small hospitals

Finally, as with written EHR contingency plans, more large hospitals than small hospitals reported having alternate sites. One hospital we visited told us that the cost associated with duplicate hardware and software was challenging to support, particularly because it had not experienced a disruption that would have called for such an investment.

Emergency Mode Operations:

When EHRs or the supporting infrastructure goes down, hospitals can take steps to keep operating until systems can be restored. Generators can provide electricity to sustain EHRs during a power failure. Additionally, paper forms can replace key EHR functions during EHR disruptions, such as registering new patients, documenting patients' vital signs, or ordering medications.

Nearly all hospitals reported supplying staff with paper forms to document care during EHR disruptions. About three-quarters of hospitals reported meeting the recommended practice to maintain enough paper forms to last at least 8 hours. See Table 4 for the recommended practices that hospitals reported implementing for emergency mode operations.

Nearly all hospitals also reported having generators and uninterruptible power systems. About three-quarters of hospitals reported maintaining fuel supplies to power their generators for at least 2 days. The hospitals we visited told us that they contracted with local fuel companies to replenish their fuel supplies as

needed. One hospital that we visited relied on a mix of fuels to ensure a ready supply, storing a week's worth of diesel fuel onsite and connecting directly to a natural gas pipeline.

Table 4: **Hospitals That Reported Implementing Recommended Practices for Emergency Mode Operations**

Recommended Practice from NIST and ONC	Percentage of Hospitals
Supply paper forms	100%
Maintain an electric generator	98%
Have processes to reconcile paper forms	96%
Use a communication strategy that does not rely on computing infrastructure *	96%
Maintain an uninterruptible power supply *	94%
Test the generator at least monthly	89%
Have forms available to last 8 hours	77%
Maintain at least 2 days of fuel onsite	73%
Test the uninterruptible power supply at least monthly	58%

Source: OIG analysis of hospitals' responses to EHR contingency plan questionnaire, 2015.

* Indicates that large hospitals are more likely to include the recommended practice than small hospitals

Testing and Revision:

By testing their contingency plans, hospitals can identify gaps and other problems in a controlled environment, enabling them to make improvements. Hospitals can also train staff so they are familiar with activating contingency plans and operating under them.

Most hospitals reported reviewing their contingency plans regularly to remain current with system or organizational changes. Eighty-eight percent reported reviewing their EHR contingency plans within the preceding 2 years for any reason, including as part of a regularly scheduled review. Hospitals also reported regularly training staff on how to operate during EHR disruptions. Although most hospitals trained staff on EHR contingency plans in the year preceding our questionnaire, 45 percent of hospitals reported training staff through recommended drills on how to deal with EHR system downtime. One hospital we visited told us that it avoids drills because of the risk to patient safety from

unnecessarily shutting down EHR systems. See Table 5 for the percentages of hospitals that reported having policies following the recommended practices for testing and revision.

Table 5: **Hospitals That Reported Implementing Recommended Practices for Testing and Revision**

Recommended Practice from NIST and ONC	Percentage of Hospitals
Update contingency plans regularly to remain current with system enhancements and organizational changes *	85%
Train and test staff on contingency plans *	81%
Validate the contingency plan with testing and exercises	45%

Source: OIG analysis of hospitals' responses to EHR contingency plan questionnaire, 2015.

* Indicates that large hospitals are more likely to include the recommended practice than small hospitals

Over half of hospitals reported an unplanned EHR disruption, and a quarter of those experienced delays in patient care as a result

For the year preceding our questionnaire, 59 percent of hospitals reported unplanned EHR disruptions that made their EHR system unavailable to hospital staff.[27] The majority (74 percent) of these hospitals reported three or fewer disruptions within 1 year. One-fifth of hospitals with unplanned disruptions reported disruptions that lasted more than 8 hours.

Hospitals reported that hardware malfunctions accounted for the largest percentage of EHR disruptions, followed by Internet connectivity problems. See Table 6 for the causes of unplanned EHR disruptions that hospitals reported.

[27] Hospitals completed our questionnaire between May and July 2015.

Table 6: Reported Causes of Unplanned EHR Disruptions

Cause	Percentage of Hospitals*
Hardware malfunction or failure	59%
Internet connectivity problem	44%
Power failure	33%
Natural disaster	4%
Hacking incident	1%

Source: OIG analysis of hospitals' responses to EHR contingency plan questionnaire, 2015.

* Each hospital may have identified more than one cause of unplanned EHR disruptions

Of those hospitals that reported an unplanned disruption, about one-quarter reported an outcome of delayed patient care, while 1 percent of hospitals reported having lost records. See Table 7 for the outcomes from unplanned EHR disruptions that hospitals reported.

Table 7: Reported Outcomes from Unplanned EHR disruptions

Outcomes	Percentage of Hospitals*
Delayed patient care	24%
Rerouted patient care	15%
Loss of records	1%
Data breach	0%

Source: OIG analysis of hospitals' responses to EHR contingency plan questionnaire, 2015.

* Each hospital may have identified more than one outcome from unplanned EHR disruptions.

To minimize the effects of EHR disruptions on clinical care and business operations, three of the six hospitals that we visited told us that the backup controls in their contingency plans helped to maintain EHR functions. For example, if these backup controls work appropriately, clinical staff were unlikely to notice any disruption to the EHR system at all. In addition, in our questionnaire, 40 percent of hospitals that activated their contingency plans reported having no disruption to patient care or adverse events as one of their top successes.

Hospitals reported using planned and unplanned disruptions to improve their contingency plans and better prepare staff for future disruptions

More than half of hospitals reported having policies to review their contingency plans after each planned or unplanned EHR disruption. EHR disruptions allow hospitals to test whether their contingency plans are effective and identify opportunities to improve them. For example, as a result of activating and reviewing EHR contingency plans, some hospitals reported that they recognized the need to improve communication during EHR disruptions.

Some hospitals also reported that EHR disruptions allow both clinical and IT staff to become more familiar with EHR contingency plans. For example, during EHR disruptions, clinical staff could practice accessing a read-only system or documenting care on paper records. IT staff could practice transferring the EHR system to an alternate site and bringing the primary system back to functioning status.

Staff gained experience responding to both planned and unplanned EHR disruptions. In fact, hospitals we visited noted that they relied on planned disruptions to train staff on EHR contingency plans. In their responses to questionnaires, hospitals also noted that they may schedule planned EHR disruptions for system upgrades, maintenance, or testing.

OCR does not target EHR contingency plans for review

In our interviews with OCR staff, they noted that when performing a compliance review in response to a breach or other problem, OCR considers HIPAA compliance broadly. In fact, HIPAA requirements do not prescribe how covered entities should develop or use contingency plans. If warranted by the problem to which it is responding, OCR may include EHR contingency plans in its compliance review. OCR staff also told us that they have not received complaints that would prompt an investigation specific to EHR contingency plans through OCR's complaint investigation channels. In March 2016, OCR launched Phase 2 of its audit program to ensure covered entities' compliance with HIPAA privacy and security requirements. OCR's audit protocol for Phase 2 assesses compliance with questions that address each HIPAA requirement for contingency planning.[28]

---

[28] OCR, *Audit Program Protocol*. Accessed at http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol-current/index.html on June 2, 2016.

CONCLUSION

In our review, almost all hospitals that received a Medicare incentive payment for using certified EHRs reported that they maintain EHR contingency plans as required by HIPAA, and two-thirds of hospitals addressed all four HIPAA requirements that we reviewed. In addition, hospitals generally implemented many practices recommended by ONC and NIST for EHR contingency plans. Recommended practices related to backing up, storing, and maintaining data; using paper records; and having alternative power sources (e.g., generators) were among the most commonly implemented (reported by 90-100 percent of hospitals).

Oversight of HIPAA compliance generally is triggered when OCR becomes aware of problems, such as breaches and complaints, at covered entities. OCR does not review a covered entity's contingency plans unless it believes the problem to which it is responding warrants it. In March 2016, OCR began Phase 2 of its audit program that addresses EHR contingency plans through both desk and onsite audits of covered entities.

Persistent and evolving threats to electronic health information reinforce the need for EHR contingency plans. Since we administered this review's hospital questionnaire in 2015, awareness of cybersecurity threats to health information technology has grown. Stakeholders in government, health care, and information technology sectors have raised concerns about vulnerabilities in networked medical devices that may put hospital networks and EHR systems at risk. In January 2016, a hospital in California reported that it suffered a ransomware attack that disabled its network and EHR system for about a week, leading to delayed patient care and the need to divert patients to other facilities. Disruptions to EHRs from these and other threats can present significant safety risks to patients. Contingency plans are crucial because they are designed to minimize the occurrence and effects of such disruptions.

OIG previously recommended that OCR fully implement a permanent audit program to assess compliance with HIPAA requirements, and recent events underscore the importance of this recommendation. This review provides baseline information on hospitals' EHR contingency plans and reflects our continued attention to this issue.

APPENDIX A

Practices Recommended by NIST and ONC

Table A-1: Practices Recommended by NIST

NIST 7 Step Contingency Planning Process
Step 1: Develop the contingency planning policy statement
Step 2: Conduct the business impact analysis
Step 3: Identify preventive controls
Step 4: Create contingency strategies
Step 5: Develop an information system contingency plan
Step 6: Ensure plan testing, training, and exercises
Step 7: Ensure plan maintenance

Table A-2: Practices Recommended by ONC

SAFER 10 Recommended Practices
Practice 1: Hardware that runs applications critical to the organization's operation is duplicated.
Practice 2: An electric generator and sufficient fuel are available to support the EHR during an extended power outage.
Practice 3: Paper forms are available to replace key EHR functions during downtimes.
Practice 4: Patient data and software application configurations critical to the organization's operations are backed up.
Practice 5: Policies and procedures are in place to ensure accurate patient identification when preparing for, during, and after downtimes.
Practice 6: Staff are trained and tested on downtime and recovery procedures.
Practice 7: A communication strategy that does not rely on the computing infrastructure exists for downtime and recovery periods.
Practice 8: Written policies and procedures on EHR downtimes and recovery processes ensure continuity of operations with regard to safe patient care and critical business operations.
Practice 9: The user interface of the locally maintained backup, read-only EHR system is clearly differentiated from the live/production EHR system.
Practice 10: There is a comprehensive testing and monitoring strategy in place to prevent and manage EHR downtime events.

APPENDIX B

HIPAA Requirements and Practices Recommended by NIST and ONC for Contingency Planning

HIPAA requirement	Recommended Practice	NIST's Guide	ONC's Guide
Data backup plan 164.308 (a)(7)(ii)(A)	• Maintain backup copies • Back up data daily, or more frequently	Step 4 Section 3.4.2	Practice 4
	• Store backup data offsite • Have a read-only EHR system	Step 4 Section 3.4.2	
	• Visually differentiate read-only system	-	Practice 9
Disaster recovery plan 164.308 (a)(7)(ii)(B)	• Have at least 2 Internet paths • Have at least 2 Internet providers • Have a "warm" or "hot" alternate site • Locate the alternate site 50 miles from primary site • Test the alternate site at least quarterly • Transfer operations to the alternate site within 8 hours	Step 4 Section 3.4.3	Practice 1
	• Determine a strategy to replace damaged equipment	Step 4 Section 3.4.4	-
Emergency mode operations plan 164.308 (a)(7)(ii)(C)	• Maintain an electric generator • Test the generator monthly • Maintain at least 2 days of fuel onsite • Maintain an uninterruptible power source • Test the uninterruptible power supply at least monthly	Step 3 Section 3.3	Practice 2
	• Supply paper forms • Have forms available to last 8 hours	-	Practice 3
	• Processes to reconcile paper forms	-	Practice 5
	• Use a communication strategy that does not rely on computing infrastructure	-	Practice 7
Testing and revision procedures 164.308 (a)(7)(ii)(D)	• Train and test staff on contingency plans	Step 6 Section 3.5.2	Practice 6
	• Validate the contingency plan with testing and exercises	Step 6 Sections 3.5.1 & 3.5.3	-
	• Update contingency plans regularly to remain current with system enhancements and organizational changes	Step 7 Section 3.6	Practice 8
Criticality assessment procedures* 164.308 (a)(7)(ii)(E)	• Conduct a business impact analysis to prioritize contingency planning for the information systems critical to the organization's operation	Step 2 Section 3.2	-

Source for NIST: NIST, *Special Publication 800-34: Contingency Planning Guide for Federal Information Systems* (May 2010)

Source for ONC: ONC, *SAFER Self-Assessment: Contingency Planning* (Jan. 2014).

Source for HIPAA Requirement: OIG Analysis.

* HIPAA requirement of criticality assessment procedures was outside the scope of this evaluation and was not included in this analysis.

APPENDIX C

Point Estimates, Confidence Intervals, and Results of Independent T-Tests

Table C-1: Point Estimates and Confidence Intervals

Description	Sample Size	Percentage of Hospitals (95-Percent Confidence Interval)
Hospitals with written contingency plans	342	95.4% (93.1%−96.9%)
Hospitals without written contingency plans	342	4.6% (3.1−6.9%)
Hospitals with contingency plans that address all four HIPAA requirements	342	67.7% (62.5%−72.5%)
Hospitals with a data backup plan	342	83.4% (79.1%−86.9%)
Hospitals with a disaster recovery plan	342	94.7% (92.3%-96.3%)
Hospitals with an emergency-mode operations plan	342	95.2% (92.9%-96.8%)
Hospitals with testing and revision procedures	342	73.1% (68.2%-77.6%)
Hospitals that maintain backup copies	342	99.4% (97.6%-99.9%)
Hospitals that store backup data offsite	340	92.0% (88.6%-94.5%)
Hospitals that back up data daily or more frequently	204	90.9% (86.1%-94.1%)
Hospitals with a read-only EHR system	342	57.0% (51.6%-62.2%)
Hospitals that visually differentiate their read-only systems	342	32.2% (27.3%-37.6%)

Description	Sample Size	Percentage of Hospitals (95-Percent Confidence Interval)
Hospitals that determine a strategy to replace damaged equipment	342	86.9% (82.9%-90.1%)
Hospitals with at least two Internet paths	342	77.7% (73.3%-81.6%)
Hospitals with at least two Internet carriers	342	67.2% (62.2%-71.9%)
Hospitals with a “warm” or “hot” alternate site	342	56.0% (50.7%-61.2%)
Hospitals that transfer operations to the alternate site within 8 hours	342	45.6% (40.3%-51.1%)
Hospitals that locate the alternate site within 50 miles of the primary site	342	31.1% (26.3%-36.4%)
Hospitals that test the alternate site quarterly	196	24.5% (19.1%-31.0%)
Hospitals that supply paper forms	342	99.6% (98.7%-99.9%)
Hospitals that maintain an electric generator	342	98.4% (96.2%-99.4%)
Hospitals that have processes to reconcile paper forms	342	96.3% (93.7%-97.9%)
Hospitals that use a communication strategy that does not rely on computing infrastructure	342	95.9% (93.5%-97.4%)
Hospitals that maintain an uninterruptible power supply	342	93.6% (90.6%-95.6%)
Hospitals that test their generators at least monthly	342	89.4% (85.6%-92.3%)
Hospitals that have forms available to last 8 hours	342	77.1% (72.3%-81.3%)

Description	Sample Size	Percentage of Hospitals (95-Percent Confidence Interval)
Hospitals that maintain at least 2 days of fuel onsite	342	73.0% (67.9%-77.5%)
Hospitals that test the uninterruptible power supply at least monthly	342	57.9% (52.6%-63.1%)
Hospitals that update contingency plans regularly	342	84.9% (80.8%-88.3%)
Hospitals that train and test staff on contingency plans	342	81.5% (77.1%-85.2%)
Hospitals that validate contingency plans with training and exercises	342	45.2% (39.8%-50.6%)
Hospitals with an unplanned EHR disruption in the year preceding our questionnaire	342	58.8% (53.4%-64.1%)
Hospitals with three or fewer unplanned disruptions	196	73.9% (67.3%-79.7%)
Hospitals with an unplanned disruption caused by a hardware malfunction or failure	196	59.3% (52.2%-66.0%)
Hospitals with an unplanned disruption caused an Internet connectivity problem	196	44.3% (37.5%-51.3%)
Hospitals with an unplanned disruption caused by a power failure	196	32.7% (26.5%-39.5%)
Hospitals with an unplanned disruption caused by a natural disaster	196	4.3% (2.2%-8.5%)
Hospitals with an unplanned disruption caused by a hacking incident	196	0.7% (0.1%-4.4%)
Hospitals with an unplanned disruption that resulted in delayed patient care	204	24.5% (18.9%-31.1%)
Hospitals with an unplanned disruption that resulted in rerouted patient care	204	15.2% (10.7%-21.0%)

Description	Sample Size	Percentage of Hospitals (95-Percent Confidence Interval)
Hospitals with an unplanned disruption that resulted in loss of records	204	1.0% (0.2%-4.0%)
Hospitals with an unplanned disruption that resulted in a data breach	204	0.0% (0%-4.4%)
Hospitals with an unplanned disruption that resulted in adverse events	204	0.0% (0%-4.4%)
Hospitals that review contingency plans after each disruption	320	54.0% (48.4%-59.5%)
Hospitals with an unplanned disruption that exceeded 8 hours	204	19.9% (15.0%-26.0%)
Hospitals that listed communication as a way to improve response after activating contingency plans	169	39.5% (32.2%-47.3%)
Hospitals that listed as a success staff familiarity with contingency plans after the plans were activated	171	23.3% (17.4%-30.3%)
Hospitals that listed as one of their top successes no disruption to patient care or no adverse events after contingency plans were activated	171	39.7% (32.4%-47.4%)
Hospitals that reviewed their contingency plans in the last 2 years	342	88.2% (84.6%-91.1%)

Source: OIG questionnaire of hospitals, 2015.

Table C2: Results of Independent Group T-Tests for Hospitals by Stratum

Factor	Stratum	Point Estimates	P-Value
Difference in hospitals with EHR contingency plans	Large Small	98.3% 88.7%	0.0004
Difference in hospitals with contingency plans that cover all four HIPAA requirements	Large Small	60.7% 70.7%	0.0521
Difference in hospitals that maintain backup copies	Large Small	99.4% 99.4%	0.9802
Difference in hospitals with read-only EHR systems	Large Small	62.1% 45.2%	0.0017
Difference in hospitals that visually differentiate read-only systems	Large Small	35.6% 24.4%	0.0236
Difference in hospitals with at least two Internet paths	Large Small	85.1% 60.7%	0.0001
Difference in hospitals with at least two Internet carriers	Large Small	74.1% 51.1%	0.0001
Difference in hospitals with a “warm” or “hot” alternate site	Large Small	63.2% 39.3%	0.0001
Difference in hospitals that transfer operations to the alternate site within 8 hours	Large Small	48.9% 38.1%	0.0451
Difference in hospitals that locate the alternate site within 50 miles of the primary site	Large Small	32.8% 27.4%	0.2798
Difference in hospitals that test the alternate site quarterly	Large Small	21.2% 35.4%	0.0261

Factor	Stratum	Point Estimates	P-Value
Difference in hospitals that supply paper forms	Large Small	100.0% 98.8%	0.1498
Difference in hospitals that maintain an electric generator	Large Small	98.3% 98.8%	0.6811
Difference in hospitals that have processes to reconcile paper forms	Large Small	96.6% 95.8%	0.7293
Difference in hospitals that use a communication strategy that does not rely on computing infrastructure	Large Small	97.7% 91.7%	0.0134
Difference in hospitals that maintain an uninterruptible power supply	Large Small	95.4% 89.3%	0.0342
Difference in hospitals that test the generator at least monthly	Large Small	90.2% 87.5%	0.4234
Difference in hospitals that have forms available to last 8 hours	Large Small	79.3% 72.0%	0.1168
Difference in hospitals that maintain at least 2 days of fuel onsite	Large Small	74.1% 70.2%	0.4223
Difference in hospitals that test the uninterruptible power supply at least monthly	Large Small	62.6% 47.0%	0.0036
Difference in hospitals that train and test staff on contingency plans	Large Small	85.1% 73.2%	0.0071
Difference in hospitals that validate contingency plans with training and exercises	Large Small	47.8% 39.3%	0.1173
Difference in hospitals that duplicate hardware and infrastructure	Large Small	82.8% 66.1%	0.0004

Source: OIG questionnaire of hospitals, 2015.

ACKNOWLEDGMENTS

This report was prepared under the direction of Joyce Greenleaf, Regional Inspector General for Evaluation and Inspections in the Boston regional office, and Kenneth Price, Deputy Regional Inspector General.

Danielle Fletcher served as team leader for this study. Alyson Cooper served as lead analyst for this study. Central office staff who provided support include Lucia Fort, Althea Hosein, and Joanne Legomsky.

Office of Inspector General

http://oig.hhs.gov

The mission of the Office of Inspector General (OIG), as mandated by Public Law 95452, as amended, is to protect the integrity of the Department of Health and Human Services (HHS) programs, as well as the health and welfare of individuals served by those programs. This statutory mission is carried out through a nationwide network of audits, investigations, and inspections conducted by the following operating components:

Office of Audit Services

The Office of Audit Services (OAS) provides auditing services for HHS, either by conducting audits with its own audit resources or by overseeing audit work done by others. Audits examine the performance of HHS programs and/or its grantees and contractors in carrying out their respective responsibilities and are intended to provide independent assessments of HHS programs and operations. These assessments help reduce waste, abuse, and mismanagement and promote economy and efficiency throughout HHS.

Office of Evaluation and Inspections

The Office of Evaluation and Inspections (OEI) conducts national evaluations to provide HHS, Congress, and the public with timely, useful, and reliable information on significant issues. These evaluations focus on preventing fraud, waste, or abuse and promoting economy, efficiency, and effectiveness of departmental programs. To promote impact, OEI reports also present practical recommendations for improving program operations.

Office of Investigations

The Office of Investigations (OI) conducts criminal, civil, and administrative investigations of fraud and misconduct related to HHS programs, operations, and individuals. With investigators working in all 50 States and the District of Columbia, OI utilizes its resources by actively coordinating with the Department of Justice and other Federal, State, and local law enforcement authorities. The investigative efforts of OI often lead to criminal convictions, administrative sanctions, and/or civil monetary penalties.

Office of Counsel to the Inspector General

The Office of Counsel to the Inspector General (OCIG) provides general legal services to OIG, rendering advice and opinions on HHS programs and operations and providing all legal support for OIG's internal operations. OCIG represents OIG in all civil and administrative fraud and abuse cases involving HHS programs, including False Claims Act, program exclusion, and civil monetary penalty cases. In connection with these cases, OCIG also negotiates and monitors corporate integrity agreements. OCIG renders advisory opinions, issues compliance program guidance, publishes fraud alerts, and provides other guidance to the health care industry concerning the anti-kickback statute and other OIG enforcement authorities.