DEPARTMENT OF HEALTH & HUMAN SERVICES **Office of Inspector General**

Washington, D.C. 20201

May 16, 2011

TO: Georgina Verdugo
Director
Office for Civil Rights

FROM: /Daniel R. Levinson/
Inspector General

SUBJECT: Nationwide Rollup Review of the Centers for Medicare & Medicaid Services Health Insurance Portability and Accountability Act of 1996 Oversight (A-04-08-05069)

The attached final report provides the results of our nationwide rollup review of the Centers for Medicare & Medicaid Services oversight of the Health Insurance Portability and Accountability Act of 1996.

Section 8L of the Inspector General Act, 5 U.S.C. App., requires that the Office of Inspector General (OIG) post its publicly available reports on the OIG Web site. Accordingly, this report will be posted at http://oig.hhs.gov.

If you have any questions or comments about this report, please do not hesitate to call me, or your staff may contact Lori S. Pilcher, Assistant Inspector General for Grants, Internal Activities, and Information Technology Audits, at (202) 619-1175 or through email at Lori.Pilcher@oig.hhs.gov. We look forward to receiving your final management decision within 6 months. Please refer to report number A-04-08-05069 in all correspondence.

Attachment

Department of Health & Human Services

OFFICE OF INSPECTOR GENERAL

NATIONWIDE ROLLUP REVIEW OF THE CENTERS FOR MEDICARE & MEDICAID SERVICES HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 OVERSIGHT

Daniel R. Levinson
Inspector General

May 2011
A-04-08-05069

Office of Inspector General

http://oig.hhs.gov

The mission of the Office of Inspector General (OIG), as mandated by Public Law 95-452, as amended, is to protect the integrity of the Department of Health & Human Services (HHS) programs, as well as the health and welfare of beneficiaries 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 beneficiaries. 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.

Notices

THIS REPORT IS AVAILABLE TO THE PUBLIC

at http://oig.hhs.gov

Section 8L of the Inspector General Act, 5 U.S.C. App., requires that OIG post its publicly available reports on the OIG Web site.

OFFICE OF AUDIT SERVICES FINDINGS AND OPINIONS

The designation of financial or management practices as questionable, a recommendation for the disallowance of costs incurred or claimed, and any other conclusions and recommendations in this report represent the findings and opinions of OAS. Authorized officials of the HHS operating divisions will make final determination on these matters.

EXECUTIVE SUMMARY

BACKGROUND

Health Insurance Portability and Accountability Act of 1996 Security Rule

On August 21, 1996, Congress enacted P.L. No. 104-191, the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Sections 261 and 262 of HIPAA established national standards that protect the confidentiality and integrity of electronic protected health information (ePHI) while it is being stored or transmitted between entities.

The HIPAA Administrative Simplification was codified in sections 1171 through 1179 of the Social Security Act (the Act). The HIPAA Security Rule (Security Rule) is a component of the HIPAA Administrative Simplification security standards and is incorporated into 45 CFR parts 160, 162, and 164. Both the Act and the Security Rule require a covered entity, defined as a (1) health plan, (2) health care clearinghouse, or (3) health care provider that transmits any health information in electronic form (45 CFR § 160.103), to (1) ensure the confidentiality, integrity, and availability of the information; (2) protect against any reasonably anticipated threats or risks to the security or integrity of the information; and (3) protect against unauthorized uses or disclosures of the information.

On February 17, 2009, Congress enacted P.L. No. 111-5, the American Recovery and Reinvestment Act of 2009 (Recovery Act). The Recovery Act contains the Health Information Technology for Economic and Clinical Health Act (HITECH Act). (See P.L. No. 111-5, Title XIII § 13001(a).) The HITECH Act at section 13001 added section 3009 to the Public Health Service Act (42 U.S.C. § 201 et seq.). This section requires the Department of Health & Human Services (HHS) to adopt health information technology standards and implementation specifications that "take into account the requirements of HIPAA privacy and security law." (See Public Health Service Act § 3009(a)(1)(B).)

Delegation of Authority To Administer the Health Insurance Portability and Accountability Act of 1996 Security Rule

On October 7, 2003, HHS delegated to the Centers for Medicare & Medicaid Services (CMS) the authority to enforce compliance with the Security Rule and to impose civil monetary penalties on covered entities that violate it. The Final Rule for enforcement of the Security Rule became effective on March 16, 2006.

CMS developed and published the Security Rule and guidance for covered entities. CMS also published a series of security papers designed to explain the Security Rule to covered entities and provide assistance with implementation of the security standards. These security papers explain specific requirements, the rationale behind those requirements, and possible ways to meet them.

Delegation of Authority to the Office for Civil Rights

On July 27, 2009, HHS delegated to the Office for Civil Rights (OCR) (1) the authority and responsibility to interpret, implement, and enforce the Security Rule; (2) the authority to conduct compliance reviews and to investigate and resolve complaints of Security Rule noncompliance; and (3) the authority to impose civil monetary penalties for a covered entity's failure to comply with the Security Rule.

Prior Office of Inspector General Reports on the Health Insurance Portability and Accountability Act of 1996 Security Rule

In October 2008, we issued a report to CMS based on our audit of CMS's implementation and enforcement of the Security Rule. (See Appendix A for a list of our prior audit locations and report issue dates.) We reported that CMS had taken limited actions to ensure that covered entities complied with the standards, implementation specifications, or other requirements of the Security Rule. At the time of our report, CMS had not conducted any Security Rule compliance reviews of covered entities and had not established any policies or procedures for conducting them. In the report, we recommended that CMS establish specific policies and procedures for conducting compliance reviews of covered entities.

We conducted additional audits at seven covered entities (hospitals) in California, Georgia, Illinois, Massachusetts, Missouri, New York, and Texas. Collectively, these audits assessed CMS's oversight and enforcement of the hospitals' implementations of the Security Rule. These audits disclosed numerous internal control weaknesses at the hospitals and further demonstrated the need for greater oversight by CMS.

The Centers for Medicare & Medicaid Services' Efforts To Address Prior Office of Inspector General Findings

After our 2008 audit, CMS performed reviews of 10 covered entities to verify compliance with the Security Rule. However, these reviews were limited to entities that had complaints filed against them, were identified in the media as potentially violating the Security Rule, or were recommended by OCR. Covered entities that had not otherwise been identified were not subject to CMS review.

In 2009, before delegation to OCR, CMS scheduled six compliance reviews of covered entities and did not limit its selection to covered entities with filed complaints.

OBJECTIVE

Our objective was to determine the sufficiency of CMS's oversight and enforcement actions pertaining to hospitals' implementation of the Security Rule.

SUMMARY OF FINDINGS

CMS's oversight and enforcement actions were not sufficient to ensure that covered entities, such as hospitals, effectively implemented the Security Rule. As a result, CMS had limited assurance that controls were in place and operating as intended to protect ePHI, thereby leaving ePHI vulnerable to attack and compromise.

Specifically, our audits of 7 hospitals throughout the Nation identified 151 vulnerabilities in the systems and controls intended to protect ePHI, of which 124 were categorized as high impact. These vulnerabilities placed the confidentiality, integrity, and availability of ePHI at risk. Outsiders or employees at some hospitals could have accessed, and at one hospital did access, systems and beneficiaries' personal data and performed unauthorized acts without the hospitals' knowledge.

RECOMMENDATIONS

We recommend that OCR continue the compliance review process that CMS began in 2009 and implement procedures for conducting compliance reviews to ensure that Security Rule controls are in place and operating as intended to protect ePHI at covered entities.

OFFICE FOR CIVIL RIGHTS COMMENTS AND OFFICE OF INSPECTOR GENERAL RESPONSE

In its response to our draft report, OCR did not comment on our specific findings and stated that it had considered our recommendations to continue the compliance process begun by CMS in 2009 and to implement procedures for the performance of compliance reviews.

OCR also noted in its response that it maintains a process for initiating covered entity compliance reviews in the absence of complaints and that it had used this process to open compliance reviews as a result of our seven hospital audits. It also stated that it performs compliance reviews of covered entities in response to breaches of unsecured protected health information affecting 500 or more individuals.

OCR also provided technical comments, which we addressed as appropriate. As a reference for its technical comments, OCR included excerpts from our executive summary and report body. OCR's comments, excluding its technical comments and references, are included as Appendix D.

Although OCR stated that it maintains a process for initiating covered entity compliance reviews in the absence of complaints, it provided no evidence that it had actually done so. The only reviews OCR mentioned were related to our hospital audits. In the absence of evidence of a more expansive review process, we encourage OCR to continue the compliance review process begun by CMS in 2009.

TABLE OF CONTENTS

APPENDIXES

INTRODUCTION

BACKGROUND

Health Insurance Portability and Accountability Act of 1996 Security Rule

On August 21, 1996, Congress enacted P.L. No. 104-191, the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Sections 261 and 262 of HIPAA established national standards that protect the confidentiality and integrity of electronic protected health information (ePHI) while it is being stored or transmitted between entities.

The HIPAA Administrative Simplification was codified in sections 1171 through 1179 of the Social Security Act (the Act). The HIPAA Security Rule (Security Rule) is a component of the HIPAA Administrative Simplification security standards and is incorporated into 45 CFR parts 160, 162, and 164. Both the Act and the Security Rule require a covered entity, defined as a (1) health plan, (2) health care clearinghouse, or (3) health care provider that transmits any health information in electronic form (45 CFR § 160.103), to (1) ensure the confidentiality, integrity, and availability of the information; (2) protect against any reasonably anticipated threats or risks to the security or integrity of the information; and (3) protect against unauthorized uses or disclosures of the information.

On February 17, 2009, Congress enacted P.L. No. 111-5, the American Recovery and Reinvestment Act of 2009 (Recovery Act). The Recovery Act contains the Health Information Technology for Economic and Clinical Health Act (HITECH Act). (See P.L. No. 111-5, Title XIII § 13001(a).) The HITECH Act at section 13001 added section 3009 to the Public Health Service Act (42 U.S.C. § 201 et seq.). This section requires the Department of Health & Human Services (HHS) to adopt health information technology standards and implementation specifications that "take into account the requirements of HIPAA privacy and security law." (See Public Health Service Act § 3009(a)(1)(B).)

Delegation of Authority To Administer the Health Insurance Portability and Accountability Act of 1996 Security Rule

On October 7, 2003, HHS delegated to the Centers for Medicare & Medicaid Services (CMS) the authority to enforce compliance with the Security Rule and to impose civil monetary penalties on covered entities that violate it. The Final Rule for enforcement of the Security Rule became effective on March 16, 2006.

CMS developed and published the Security Rule and guidance for covered entities. Examples of guidance include the March 25, 2005, *Federal Register* notice on how to file a complaint. CMS also published a series of security papers designed to explain the Security Rule to covered entities and provide assistance with implementation of the security standards. These security papers explain specific requirements, the rationale behind those requirements, and possible ways to meet them.

Delegation of Authority to the Office for Civil Rights

On July 27, 2009, HHS delegated to the Office for Civil Rights (OCR) (1) the authority and responsibility to interpret, implement, and enforce the Security Rule; (2) the authority to conduct compliance reviews and to investigate and resolve complaints of Security Rule noncompliance; and (3) the authority to impose civil monetary penalties for a covered entity's failure to comply with the Security Rule provisions.

OCR also enforces the HIPAA Privacy Rule, which is intended to protect the privacy of individually identifiable health information, and the confidentiality provisions of the Patient Safety Rule, which protect the confidentiality of identifiable information that is used to analyze patient safety events and improve patient safety.

Prior Office of Inspector General Reports on the Health Insurance Portability and Accountability Act of 1996 Security Rule

In October 2008, we issued a report to CMS based on our audit of CMS's implementation and enforcement of the Security Rule. (See Appendix A for a list of our prior audit locations and report issue dates.) We reported that CMS had taken limited actions to ensure that covered entities complied with the standards, implementation specifications, or other requirements of the Security Rule. At the time of our report, CMS had not conducted any Security Rule compliance reviews of covered entities and had not established any policies or procedures for conducting them. In the report, we recommended that CMS establish specific policies and procedures for conducting compliance reviews of covered entities.

We conducted additional audits at seven covered entities (hospitals) in California, Georgia, Illinois, Massachusetts, Missouri, New York, and Texas. These audits focused primarily on the hospitals' implementation of (1) the wireless electronic communications network or security measures the security management staff implemented in its computerized information systems (technical safeguards); (2) the physical access to electronic information systems and the facilities in which they are housed (physical safeguards); and (3) the policies and procedures developed and implemented for the security measures to protect the confidentiality, integrity, and availability of ePHI (administrative safeguards).

Collectively, these audits assessed CMS's oversight and enforcement of the hospitals' implementations of the Security Rule.[1] These audits disclosed numerous internal control weaknesses at the hospitals and further demonstrated the need for greater oversight by CMS.

[1] We are also conducting an audit in Pennsylvania.

OBJECTIVE, SCOPE, AND METHODOLOGY

Objective

Our objective was to determine the sufficiency of CMS's oversight and enforcement actions pertaining to hospitals' implementation of the Security Rule.

Scope

We conducted our audit at CMS in Baltimore, Maryland, and seven hospitals in California, Georgia, Illinois, Massachusetts, Missouri, New York, and Texas.

Methodology

To accomplish our objective, we focused on the findings and recommendations categorized as high impact from the eight reports resulting from the CMS and seven hospital audits.

Magnitude of Impact Definitions

To determine the impact of our findings, we used the "Magnitude of Impact Definitions" of the National Institute of Standards and Technology Special Publication 800-30. These definitions describe the consequences of not properly safeguarding ePHI in terms of high, medium, and low impacts, as quoted below:

- High—Exercise of the vulnerability (1) may result in the highly costly loss of major tangible assets or resources; (2) may significantly violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human death or serious injury.

- Medium—Exercise of the vulnerability (1) may result in the costly loss of tangible assets or resources; (2) may violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human injury.

- Low—Exercise of the vulnerability (1) may result in the loss of some tangible assets or resources or (2) may noticeably affect an organization's mission, reputation, or interest.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

FINDINGS AND RECOMMENDATIONS

CMS's oversight and enforcement actions were not sufficient to ensure that covered entities, such as hospitals, effectively implemented the Security Rule. As a result, CMS had limited assurance that controls were in place and operating as intended to protect ePHI, thereby leaving ePHI vulnerable to attack and compromise.

Specifically, our audits of 7 hospitals throughout the Nation identified 151 vulnerabilities in the systems and controls intended to protect ePHI, of which 124 were categorized as high impact. These vulnerabilities placed the confidentiality, integrity, and availability of ePHI at risk. Outsiders or employees at some hospitals could have accessed, and at one hospital did access, systems and beneficiaries' personal data and performed unauthorized acts without the hospitals' knowledge.[2]

SECURITY STANDARDS FOR THE PROTECTION OF ELECTRONIC PROTECTED HEALTH INFORMATION

Regulations at 45 CFR § 164.306(a) define general requirements for covered entities, which include hospitals, as quoted below.

> Covered entities must do the following: (1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits. (2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information. (3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part. (4) Ensure compliance with this subpart by its workforce.

HIGH-IMPACT VULNERABILITIES FOUND AT HOSPITALS

Although each of the seven hospitals had implemented some controls, policies, and procedures to protect ePHI from improper alteration or destruction, none had sufficiently implemented the administrative, technical, and physical safeguard provisions of the Security Rule.

Our audits identified 151 vulnerabilities, of which we determined 124 to be high impact, 24 to be medium impact, and 3 to be low impact.

The table on the following page summarizes the vulnerabilities found at the hospitals grouped by impact and HIPAA security standards. The table is followed by summaries of the high-impact vulnerabilities.

We provide details of the high-impact vulnerabilities in Appendix B. We also define some of the information technology terminology used throughout the report in Appendix C.

[2] One of the hospitals we audited reported a breach in which two employees accessed confidential patient information from the hospital's systems and allegedly opened credit card accounts using this information.

SUMMARY OF SECURITY RULE VULNERABILITIES IDENTIFIED AT SEVEN HOSPITALS NATIONWIDE

SECURITY RULE VULNERABILITIES	HIGH IMPACT		MEDIUM IMPACT		LOW IMPACT		TOTAL
	Findings	Hospitals Affected	Findings	Hospitals Affected	Findings	Hospitals Affected	
TECHNICAL VULNERABILITIES							
Wireless Access	15	5					15
Access Control	38	7					38
Audit Control	9	5	2	2			11
Integrity Control	21	7					21
Person or Entity Authentication	9	4	1	1			10
Transmission Security	14	4			1	1	15
TOTAL TECHNICAL	**106**		**3**		**1**		**110**
PHYSICAL VULNERABILITIES							
Facility Access Control	2	1	10	3	2	1	14
Device and Media Control	5	2	2	1			7
TOTAL PHYSICAL	**7**		**12**		**2**		**21**
ADMINISTRATIVE VULNERABILITIES							
Security Management Process	2	2	1	1			3
Workforce Security	2	2					2
Security Incident Procedures	1	1					1
Contingency Plan	6	3	2	1			8
Business Associate Contracts			6	6			6
TOTAL ADMINISTRATIVE	**11**		**9**				**20**
TOTAL VULNERABILITIES	**124**		**24**		**3**		**151**

Wireless Access Vulnerabilities

Five hospitals had fifteen wireless access vulnerabilities, including ineffective encryption, rogue wireless access points, no firewall separating wireless from internal wired networks, broadcasted service set identifiers (SSID)[3] from hospital access points, no authentication required to enter the

[3] An SSID is a code attached to all data packets on the wireless network that identifies each packet as part of that network. Only authorized users should know the SSID because the SSID identifies a wireless network. Broadcasting the SSID allows any computer with wireless capabilities to identify and potentially access the network.

wireless network, the inability to detect rogue devices intruding on the wireless network, and no procedures for continuously monitoring the wireless networks.

These vulnerabilities exposed the hospitals to known threats, such as unauthorized, unlimited, and undetected access into an organization's network and unauthorized access to ePHI.

Access Control Vulnerabilities

Seven hospitals had thirty-eight access control vulnerabilities involving domain controllers, servers, workstations, and mass storage media used to receive, maintain, or transmit ePHI. The vulnerabilities included inadequate password settings, computers that did not log users off after periods of inactivity, unencrypted laptops containing ePHI, and excessive access to root folders.

As a result, unauthorized individuals could have viewed or altered ePHI data on nonclinical workstations that were not automatically logged off after a period of inactivity; ePHI could have been compromised on lost or stolen unencrypted laptops; and unauthorized users could have circumvented system controls and modified, executed, and deleted system files.

Audit Control Vulnerabilities

Five hospitals had nine audit control vulnerabilities involving their servers, routers, firewalls, databases, and wireless access points containing or transmitting ePHI. The five hospitals had audit logging disabled for one or all of the above. In addition, their network administrators did not routinely review operating system and application audit logs, either manually or by using automated log-monitoring tools.

These vulnerabilities hindered the hospitals' abilities to investigate suspicious or malicious activity, including attempts to hack into the hospitals' networks and compromise the confidentiality, integrity, and availability of ePHI.

Integrity Control Vulnerabilities

Seven hospitals had twenty-one integrity control vulnerabilities on personal computers and servers containing ePHI. Examples of those vulnerabilities were uninstalled critical security patches, outdated antivirus updates, operating systems no longer supported by the manufacturer, and unrestricted Internet access.

By not applying critical security patches in a timely fashion, hospital network administrators exposed ePHI to a higher risk of improper alteration or destruction. It takes only one missing patch to create a vulnerability. Without the most current antivirus definitions and scan engines, hospitals could not fully protect their networks against current virus attacks. When operating system vendors no longer provide support for their products, the system software is no longer updated to guard against new security risks. Because some hospitals used unsupported operating systems, they had no assurance that ePHI would be protected from improper alteration or destruction. Unauthorized software downloaded from the Internet could have exposed hospital networks to malicious code that could have significantly harmed the hospital systems. Such

software could also have made the networks vulnerable to hackers, who could have penetrated connecting systems.

Person or Entity Authentication Vulnerabilities

Four hospitals had nine person or entity authentication vulnerabilities, such as inappropriate sharing of administrator accounts and unchanged default user identifiers (ID) and passwords.

Sharing administrator accounts limited the hospitals' ability to determine which individuals made changes to the hospitals' systems. User identification and authentication is critical to security and provides a foundation for organizations to control access and establish accountability. Default user names and default passwords are available in user manuals, as well as on the Internet. Failure to change vendor defaults allows any network user with the knowledge of the default user name and default password to anonymously access the administration console and alter the configuration and security features.

Transmission Security Vulnerabilities

Four hospitals had fourteen transmission security control vulnerabilities involving network devices, including routers and switches used for transmitting ePHI. These vulnerabilities were the result of using inappropriate plain text remote administration tools (e.g., Simple Network Management Protocol version 1 and the Telnet protocol); no email encryption; unsecure switch port connections; and unnecessary and unsecure network services.

When users connect to a remote host using these plain text remote administration protocols, sensitive information (e.g., device configuration settings, user IDs, and passwords) could be intercepted and compromised as it travels across the network. Remote connections and misconfigured routers could subject sensitive information to "man-in-the-middle" attacks or prevent access to the information through denial-of-service attacks. Sending emails containing unencrypted ePHI could enable ePHI confidentiality and integrity to be compromised by unauthorized recipients intercepting it en route. The interceptor could modify the ePHI before sending the email message to its original destination. Finally, running unsecure services can leave a system vulnerable to security-related risks. Unnecessary services should be turned off because they create security vulnerabilities.

Facility Access Control Vulnerabilities

One hospital had two facility access vulnerabilities involving unsecured physical access to ePHI in its data center and radiology data backup room. The hospital data center had large open shelves and an unsecured indoor window located between an external hallway and the data center's main entrance. In addition, the radiology data backup room's back door lock had been taped over.

Unauthorized personnel could have gained access to the data center by climbing through the open shelves or the unlocked window. We observed a maintenance employee enter the data backup room through the back door with the taped lock. In both areas, ePHI was vulnerable.

Device and Media Control Vulnerabilities

Two hospitals had five device and media control vulnerabilities, involving no inventory system to track computer equipment containing ePHI, no documented plans for or evidence of removal of ePHI from media before disposal, no password protection for computers on portable carts, and no encryption on backup tapes containing ePHI.

Without a tracking system to alert appropriate personnel of missing equipment containing ePHI, the loss of ePHI could have gone undetected. Insufficient disposal safeguards to remove or destroy ePHI before equipment left the facility compromised the confidentiality of the ePHI stored on electronic media. Insufficient password protection for computers on portable carts risked the exposure of ePHI to anyone with physical access to the computer. The confidentiality and integrity of ePHI were not protected on unencrypted backup media that were moved into, out of, or within the facilities.

Security Management Process

Two hospitals each had a security management process vulnerability. One had incomplete risk assessments of hospital systems that created, received, maintained, or transmitted ePHI. The other had no policies and procedures for risk analysis.

An inadequate security management process could have resulted in inadequate or inconsistently applied security controls, improperly implemented security responsibilities, insufficient protection of information technology resources, and inappropriate disclosures of ePHI.

Workforce Security Vulnerabilities

Two hospitals each had one workforce security vulnerability. One hospital's insufficient policies and procedures resulted in 36 employee user accounts with inappropriate access to its network and ePHI. Another hospital informed its network management department of employee terminations at the end of each 2-week pay period, thus allowing former employees' network IDs to remain active with inappropriate network access for up to 2 weeks after the employees no longer worked for the hospital.

Security Incident Procedure Vulnerabilities

One hospital had a security incident response vulnerability involving a lack of procedures to identify, respond to, or document actions taken in response to security incidents. As a result, when the hospital had a security incident involving a workstation and a laptop, the hospital did not confiscate either for inspection until 3 days after the incident occurred.

Contingency Plan Vulnerabilities

Three hospitals had six contingency plan vulnerabilities, such as incomplete contingency plans, incomplete disaster recovery plans, unsafe storage of backup tapes, and network security

disruptions. For example, one hospital did not complete a contingency plan for a system that provided ready access to patient health care records and test results.

Contingency plan vulnerabilities risk the loss of ability to process, retrieve, or protect information electronically, which could have significantly affected the hospitals' ability to accomplish their missions and provide patient care. Even minor interruptions could have resulted in lost or incorrectly processed data, expensive recovery efforts, and inaccurate or incomplete ePHI.

INSUFFICIENT OVERSIGHT AND ENFORCEMENT ACTIONS

CMS's oversight and enforcement actions were not sufficient to ensure that covered entities, such as hospitals, effectively implemented the Security Rule. Before our October 27, 2008, audit report, CMS had not established any policies or procedures for conducting compliance reviews at covered entities, nor had it conducted any Security Rule compliance reviews of covered entities. CMS emphasized voluntary compliance and provided guidance for implementing the Security Rule.

The Centers for Medicare & Medicaid Services' Efforts To Address Prior Office of Inspector General Findings

After our 2008 audit, CMS performed reviews of 10 covered entities to verify compliance with the HIPAA Security Rule. However, these reviews were limited to entities that had had complaints filed against them, were identified in the media as potentially violating the Security Rule, or were recommended by OCR.[4] Covered entities that had not otherwise been identified or recommended were not subject to CMS review.

In 2009, before delegation to OCR, CMS scheduled six compliance reviews of covered entities and did not limit its selection of covered entities to those that had had complaints filed against them.

RECOMMENDATIONS

We recommend that OCR continue the compliance review process that CMS began in 2009 and implement procedures for conducting compliance reviews to ensure that Security Rule controls are in place and operating as intended to protect ePHI at covered entities.

OFFICE FOR CIVIL RIGHTS COMMENTS AND OFFICE OF INSPECTOR GENERAL REPONSE

In its response to our draft report, OCR did not comment on our specific findings and stated that it had considered our recommendations to continue the compliance process begun by CMS in 2009 and to implement procedures for the performance of compliance reviews.

[4] CMS Office of E-Health Standards and Services, *HIPAA Compliance Review Analysis and Summary of Results*, 2008.

OCR also noted in its response that it maintains a process for initiating covered entity compliance reviews in the absence of complaints and that it had used this process to open compliance reviews as a result of our seven hospital audits. It also stated that it performs compliance reviews of covered entities in response to breaches of unsecured protected health information affecting 500 or more individuals.

OCR also provided technical comments, which we addressed as appropriate. As a reference for its technical comments, OCR included excerpts from our executive summary and report body. OCR's comments, excluding its technical comments and references, are included as Appendix D.

Although OCR stated that it maintains a process for initiating covered entity compliance reviews in the absence of complaints, it provided no evidence that it had actually done so. The only reviews OCR mentioned were related to our hospital audits. In the absence of evidence of a more expansive review process, we encourage OCR to continue the compliance review process begun by CMS in 2009.

APPENDIXES

APPENDIX A: PRIOR OFFICE OF INSPECTOR GENERAL REPORTS ON THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 SECURITY RULE [1]

Audit Location	Report Issue Date
Centers for Medicare & Medicaid Services	October 27, 2008
California	August 24, 2009
Georgia	October 16, 2008
Illinois	March 2, 2010
Massachusetts	November 10, 2009
Missouri	February 27, 2009
New York	September 1, 2009
Texas	March 15, 2010

[1] We included only the State name, not the individual hospital names or the report numbers, because the reports contained restricted, sensitive information that may be exempt from release under the Freedom of Information Act, 5 U.S.C. § 552. The hospital reports were not posted on the Internet.

APPENDIX B: DETAILS OF HIGH-IMPACT VULNERABILITIES

We categorized the 124 high-impact vulnerabilities from the 7 hospital reports according to their Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule definitions of technical,[1] physical,[2] and administrative[3] safeguards as follows:

- 106 technical safeguard vulnerabilities related to the wireless electronic communications network and to other security measures management implemented in their computerized information systems;

- 7 physical safeguard vulnerabilities involving physical access to electronic information systems and the facilities in which they are housed; and

- 11 administrative safeguard vulnerabilities related to the hospitals' policies and procedures for protecting the confidentiality, integrity, and availability of electronic protected health information (ePHI).

WIRELESS NETWORK AND TECHNICAL VULNERABILITIES

Our audit of the hospitals' implementation of the technical safeguards identified 15 high-impact wireless network vulnerabilities at 5 hospitals and 91 other high-impact technical safeguard vulnerabilities at 7 hospitals.

Wireless Access Vulnerabilities

Federal regulations state that covered entities must "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4)" (45 CFR § 164.312(a)(1)). Covered entities also must "[i]mplement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network" (45 CFR § 164.312(e)(1)) and must, if reasonable and appropriate, "[i]mplement a mechanism to encrypt and decrypt electronic protected health information" (45 CFR § 164.312(a)(2)(iv)).

---

[1] The Security Rule defines technical safeguards in 45 CFR § 164.304 as "the technology and the policy and procedures for its use that protect electronic protected health information and control access to it."

[2] The Security Rule defines physical safeguards in 45 CFR § 164.304 as "physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion."

[3] The Security Rule defines administrative safeguards in 45 CFR § 164.304 as "administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information."

Ineffective Wireless Network Encryption

Four hospitals used Wired Equivalent Privacy (WEP)[4] encryption to secure the data on their access points. Because WEP encryption uses a flawed algorithm, a hacker could quickly break into the wireless system. Since 2003, experts have questioned the use of WEP as a secure protocol. The Institute of Electrical and Electronics Engineers (IEEE) originally developed the WEP standard. In June 2003, IEEE recommended that the wireless encryption standard move from WEP to Wi-Fi Protected Access.[5]

Because of WEP's vulnerability, two hospitals used WEP encryption together with Cisco's Lightweight Extensible Authentication Protocol (LEAP)[6] to secure the transmission of data between their access points. LEAP uses a stronger authentication method than WEP. However, LEAP is susceptible to "man-in-the-middle" attacks, in which an unauthorized party intercepts traffic between an authorized computer and a wireless access point and uses that information to do something malicious, such as hijacking future traffic. Also, the LEAP authentication mechanism potentially compromises password security.

Rogue Access Points

Three hospitals had rogue access points. A rogue access point is a wireless access point that is installed on a network but is not authorized for operation on that network and is not under the management of the network administrator. Because rogue access points often do not conform to wireless local area network (LAN) security policies, they can allow unauthorized access to an organization's network.

No Firewall Separating Wireless Network From Internal Wired Network

Three hospitals' network configurations did not include firewalls to protect the internal wired network from the wireless network. After compromising the wireless network encryption, an unauthorized individual could have gained immediate and unlimited access to a hospital's entire network of computer processing systems located on the wired network. To add a level of security and prevent network intrusion, firewalls should separate wireless from wired networks.

Broadcasted Service Set Identifiers

Two hospitals publicly broadcasted their service set identifier (SSID) from their access points. In a Wi-Fi Wireless LAN, an SSID is a code attached to all data packets on the wireless network that identifies each packet as part of that network. Only authorized users should know the SSID

[4] WEP is a security protocol used to encrypt wireless transmissions.

[5] Wi-Fi Protected Access is a class of systems to secure wireless (Wi-Fi) computer networks developed to remedy serious weaknesses in WEP.

[6] LEAP is a wireless encryption protocol.

because the SSID identifies a wireless network. Publicly broadcasting the SSID enables any computer with wireless capabilities to identify, and potentially access, the network.

Inability To Detect Rogue Devices

One hospital's wireless monitoring and control system had not been configured to detect intrusion by unauthorized wireless devices. The hospital used Cisco's Wireless Control System (WCS) as its foundation for administering and monitoring its wireless networks. The hospital was not able to deploy WCS to detect intrusion by unauthorized wireless devices because it had not completed an accurate access control list of electronic equipment authorized to access the wireless network. Without the access control list, the hospital could not recognize rogue devices that connected or attempted to connect to the wireless network.

No Wireless Monitoring Policies and Procedures

One hospital had not established a procedure for continuously monitoring its wireless networks or the overall wireless control environment. In addition, the same hospital had not established a procedure for conducting periodic wireless walkthrough scans of the facility to compensate for its wireless network monitoring deficiencies. Without appropriate policies and procedures, the hospital could not ensure that staff had implemented effective actions to continuously monitor wireless networks and to maintain effective network security.

Access Control Vulnerabilities

Federal regulations state that covered entities must, if reasonable and appropriate, "[i]mplement electronic procedures that terminate an electronic session after a predetermined time of inactivity" (45 CFR § 164.312(a)(2)(iii)) and must "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4)" (45 CFR § 164.312(a)(1)). Additionally, 45 CFR § 164.316(a) requires the implementation of reasonable and appropriate policies and procedures to comply with the standards.

Inadequate Password Settings

Five hospitals did not properly configure password settings on their domain controllers and servers used to receive, maintain, or transmit ePHI. The domain controllers and servers had minimum password lengths and ages and histories set to zero. In addition, maximum password ages were set to "none" and other password settings did not meet recommended guidelines. As a result, those accounts with passwords did not have to change them or could immediately change them back, thus making the domain controller and server vulnerable to intrusion.

No Automatic Logoff

Four hospitals did not use the automatic logoff setting on computers connected to the network to terminate user sessions after a predetermined period of inactivity. These vulnerabilities increased the likelihood that an unauthorized individual could have gained access to hospital networks and viewed or altered ePHI data on a nonclinical workstation, especially if the workstation were in an unsecure location.

Insufficient Remote Access Control

One hospital did not promptly terminate remote network access when it was no longer required. Remote access to the network could potentially allow a former employee to obtain, alter, or destroy ePHI.

No Laptop Hard Drive Encryption

Five hospitals did not encrypt employee laptop hard drives containing ePHI. Failure to encrypt laptop hard drives increases the risk that unauthorized individuals could access ePHI on lost or stolen laptops.

Excessive Access to Root Folders

One hospital allowed the "everyone" group on servers unrestricted access to the root folder. Only the "administrator" group should have unrestricted access to the root folder. Users with unrestricted access can modify, execute, and delete system files.

Audit Control Vulnerabilities

Federal regulations require covered entities to "[i]mplement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information" (45 CFR § 164.312(b)) and also to "[i]mplement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart ..." (45 CFR § 164.316(a)).

Improper Audit Policy Settings

Three hospitals had audit logging disabled on various servers or network devices. The audit trails that logs create can assist network and system administrators in detecting security violations and performance problems that pose a threat to a network. Without audit trails, those hospitals could not have investigated suspicious or malicious activity, including attempts to hack into their networks or compromise the confidentiality, integrity, and availability of their ePHI.

Audit Logs Not Monitored

Four hospitals' network and system administrators did not routinely review audit logs, either manually or by using automated log-monitoring tools. System administrators use audit trails to

help ensure that systems have not been harmed by hackers, insiders, or technical problems. Not monitoring audit logs hindered these hospitals' ability to investigate suspicious or malicious activity, including attempts to hack into their networks or compromise the confidentiality, integrity, and availability of ePHI.

Integrity Control Vulnerabilities

Federal regulations (45 CFR § 164.312(a)(1)) state that covered entities must "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4)." Covered entities must also "[i]mplement policies and procedures to protect electronic protected health information from improper alteration or destruction" (45 CFR § 164.312(c)(1)). In addition, covered entities must "[e]nsure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits" (45 CFR § 164.306(a)(1)). Finally, covered entities must "[p]rotect against any reasonably anticipated threats or hazards to the security or integrity of such information" (45 CFR § 164.306(a)(2)).

Uninstalled Critical Security Patches

Six hospitals did not have the latest security patches installed on personal computers and servers. Security patches are a collection of updates, fixes, and enhancements distributed by the operating system (OS) manufacturer, e.g., Microsoft or Linux, in a single installable package that promotes system reliability, program compatibility, and security. By not applying these patches expeditiously, hospital system administrators exposed ePHI to a higher risk of improper alteration or destruction. It takes only one missing patch to create a vulnerability.

Outdated Antivirus Updates

Six hospitals did not have the most current antivirus definitions, the most current antivirus scan engines, or both on workstations connected to their networks. Without current antivirus updates, antivirus software could not fully protect these hospitals' networks against current viruses.

Operating Systems Unsupported by Manufacturer

Three hospitals used unsupported OSs on domain controllers and data servers containing ePHI. The hospitals used these unsupported OSs: Windows NT 4.0, UNIX/AIX 4.3.3, Novell 5.0, and Novell 5.1. When an OS vendor no longer supports its products, the system software is no longer updated to guard against new security risks. Because the hospitals used unsupported OSs, they had no assurance that ePHI would be protected from improper alteration or destruction.

Unrestricted Internet Activity Access

Two hospitals had workstations, console computers, or domain controllers with unrestricted Internet access. Unauthorized software downloaded from the Internet could have exposed hospital networks to malicious code. Such software also could have made the network

vulnerable to hackers using the software to penetrate and compromise connecting systems. At one of the hospitals, the console computers connected to the Internet posed an even greater risk because they were also connected to the servers and mainframe computers at the hospital's data center, which housed the majority of the hospital's ePHI. Domain controllers, which are used to authenticate users when they log onto hospital networks, connected to the Internet could enable malware to be downloaded and compromise user authentication. Best practices recommend using a Web server rather than a domain controller to connect to the Internet.

Person or Entity Authentication Vulnerabilities

Federal regulations state that covered entities must "[i]mplement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed" (45 CFR § 164.312(d)). Covered entities also must "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4)" (45 CFR § 164.312(a)(1)) and "[a]ssign a unique name and/or number for identifying and tracking user identity" (45 CFR § 164.312(a)(2)(i)).

Inappropriate Sharing of Administrator Accounts

Three hospitals had network administrators who shared the same administrator account with a single logon identification (ID) and password to gain access to group servers. The hospitals used this authentication method to enable any individual from a group to make emergency changes. However, allowing individuals in administrator groups to share the same account limited the hospitals' ability to determine which individuals made changes to the hospitals' systems. User ID and authentication is critical to security and to controlling access and establishing accountability.

Unchanged Default User Identification and Passwords

Two hospitals had network administrators that did not change or remove the Virtual Private Network (VPN) manufacturer's default user ID and password. The VPN is used to access the network remotely in a secure manner by encrypting data being transmitted. This default user name and default password information is available in user manuals and on the Internet. Failure to change the vendor defaults allows any network user with the knowledge of the default user name and default password to anonymously alter the configuration and security features and add, modify, or delete user names on the VPN.

Transmission Security Vulnerabilities

Federal regulations state that covered entities must "[i]mplement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network" (45 CFR § 164.312(e)(1)) and also must "[i]mplement a mechanism to encrypt electronic protected health information whenever deemed appropriate" (45 CFR § 164.312(e)(2)(ii)).

Plain Text Remote Adminstration Tools

Three hospitals had network administrators that used plain text remote transmission protocols, including Simple Network Management Protocol version 1 and the Telnet protocol, to monitor and manage the hospital internal networks and to provide remote command-based access to a variety of network devices. When network administrators connect to a remote host using these protocols, sensitive information, such as device configuration settings and user IDs and passwords, could be intercepted and compromised as it travels across the network in unencrypted plain text. This vulnerability makes it easier for unscrupulous individuals connected to the network to monitor and obtain network administrator user IDs and passwords, as well as device configuration settings.

Lack of Email Encryption

One hospital did not enforce its policies and procedures for encrypting email messages containing ePHI. Without encryption, anyone that received an email message from the hospital, including those who received it in error or maliciously intercepted it, would have been able to see ePHI in clear text. The lack of encryption could have compromised not only the ePHI's confidentiality but also its integrity if the interceptor had modified the ePHI before sending the email message to its original destination.

Unsecure Switch Port Connections

One hospital did not disable switch port trunking. Cisco switch devices can create connections called trunks for transferring information to different network devices, but trunks can create serious security issues. An attacker could create a trunk and gain direct access to all the virtual LANs associated with the switch, thus breaching security.

Unnecessary and Unsecure Network Services

One hospital was running unnecessary and unsecure network services that should have been turned off because they created unnecessary security vulnerabilities.

PHYSICAL VULNERABILITIES

We identified seven high-impact physical safeguard vulnerabilities at three hospitals.

Facility Access Control Vulnerabilities

Federal regulations state that covered entities must "[e]nsure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits." (45 CFR § 164.306(a)(1)) and also must "[i]mplement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed" (45 CFR § 164.310(a)(1)). In addition, if reasonable and appropriate, covered entities must "[i]mplement policies and procedures to safeguard the facility and the equipment therein from

unauthorized physical access, tampering, and theft" (45 CFR § 164.310(a)(2)(ii)) and "[i]mplement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision" (45 CFR § 164.310(a)(2)(iii)).

Unsecured Data Center Access

One hospital had two facility access vulnerabilities in its data center and radiology data backup room. The hospital data center had large open shelves and an unsecured indoor window located between an external hallway and the data center's main entrance. In addition, the door lock to the radiology data backup room had been taped over.

Unauthorized personnel could have gained access to the data center by climbing through the open shelves or the unlocked window. Office of Inspector General auditors observed a maintenance employee using the door with the taped lock to access the radiology data backup room. In both areas, ePHI was vulnerable.

Device and Media Control Vulnerabilities

Federal regulations state that covered entities must "[i]mplement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility" (45 CFR § 164.310(d)(1)). In addition, covered entities must "[i]mplement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored" (45 CFR § 164.310(d)(2)(i)) and, if reasonable and appropriate, recommend that covered entities "maintain a record of the movements of hardware and electronic media ..." (45 CFR § 164.310(d)(2)(iii)).

No Computer Equipment Inventory

Two hospitals did not have a process for tracking or inventorying computer equipment that might have contained ePHI. Equipment containing ePHI could have been stolen, lost, or misplaced. Without a tracking system to alert the appropriate personnel of such an incident, loss of ePHI could have gone undetected.

No Written Plan for Media Disposal

One hospital did not document its procedures for disposing of computer tapes and hard drives containing ePHI. Hospital management said that it would retain the media until it developed and implemented an action plan for proper disposal.

No Password Protection for Computers on Portable Carts

One hospital used a portable computer in a public area as an electronic medication administration record cart. The portable computer stored a Windows temporary file containing ePHI that could have been accessed by unauthorized personnel. Management believed that ePHI was secured

because computer applications on the PC required a user ID and password for access. However, the stored memory, which was in an OS folder, was accessible without using password-protected applications or any other security measures.

Unencrypted Backup Tapes

One hospital transferred unencrypted backup tapes containing ePHI to and from its data center. The confidentiality and integrity of ePHI were not protected on unencrypted backup media that were moved into, out of, or within the facilities.

ADMINISTRATIVE VULNERABILITIES

We identified 11 high-impact administrative vulnerabilities at four hospitals.

Security Management Process Vulnerabilities

Federal regulations state that covered entities must "[i]mplement policies and procedures to prevent, detect, contain, and correct security violations" (45 CFR § 164.308(a)(1)(i)). In addition, covered entities must "[c]onduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information …" and the implementation of "… security measures to reduce risks and vulnerabilities identified during the risk analysis to a reasonable and appropriate level ..." (45 CFR §164.308(a)(1)(ii)(A) and (B)).

Incomplete Risk Assessments

One hospital did not perform risk assessments on its systems that created, received, maintained, or transmitted ePHI. Because the hospital had limited resources to conduct risk assessments, it gave priority to systems that had the greatest effect on hospital operations and finances. Using these priorities, hospitals may not have defined as critical those systems creating, receiving, maintaining, or transmitting ePHI.

Not including systems that create, receive, maintain, or transmit ePHI in the hospital's risk assessments could have resulted in inadequate or inconsistently applied security controls, improperly implemented security responsibilities, insufficient protection of information technology resources, and inappropriate disclosures of ePHI.

No Risk Analysis Policies and Procedures

Another hospital's risk analysis policies and procedures were not established, nor was a hospitalwide risk assessment conducted to identify risks to ePHI. The hospital had not implemented a formal process for conducting periodic risk assessments that could identify potential vulnerabilities affecting ePHI. Instead, the hospital performed an initial ePHI risk assessment with a consultant, but the assessment addressed only the hospital's major applications. The hospital also instituted a policy to address HIPAA Security Rule compliance when new systems are implemented.

Workforce Security Vulnerabilities

Federal regulations state that covered entities must "[i]mplement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information" (45 CFR § 164.308(a)(3)(i)). In addition, Federal regulations state that covered entities must, if reasonable and appropriate, "[i]mplement procedures for terminating access to electronic protected health information when the employment of a workforce member ends …" (45 CFR § 164.308(a)(3)(ii)(C)).

Inappropriate Network Access

One hospital's insufficient policies and procedures resulted in 36 network user accounts with inappropriate access to the hospital's network. The user accounts belonged to employees on long-term disability. Three of these individuals had accessed ePHI while on long-term disability. The hospital did not have adequate policies and procedures to terminate network access for employees on long-term disability. Allowing network access to those who no longer needed it placed ePHI at unnecessary risk.

Delayed Termination of Employee Network Access

One hospital's Human Resources Department notified the Management Information Systems Department of all employees who no longer worked for the hospital at the end of each 2-week pay period. This created a period of up to 2 weeks during which former employee network IDs remained active, thus allowing former employees inappropriate network access.

Security Incident Procedures Vulnerabilities

Federal regulations state that covered entities must "... [i]dentify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes" (45 CFR §164.308(a)(6)(ii)).

Inadequate Incident Response Plan

One hospital's incident response plan did not address what actions needed to be taken during security incidents or breaches. As a result, when a workstation and laptop were involved in a security incident, they were not confiscated for inspection until 3 days after the security incident occurred.

Contingency Plan Vulnerabilities

Federal regulations state that covered entities must "[e]stablish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (e.g., fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic

protected health information" (45 CFR § 164.308(a)(7)(i)), "[e]stablish and implement procedures to create and maintain retrievable exact copies of electronic protected health information ..." (45 CFR § 164.308(a)(7)(ii)(A)), and "[e]stablish (and implement as needed) procedures to restore any loss of data ..." (45 CFR § 164.308(a)(7)(ii)(B)). In addition, covered entities must "[e]stablish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode" (45 CFR § 164.308(a)(7)(ii)(C)).

Incomplete Contingency Plans

One hospital's contingency plans for its systems that created, received, maintained, or transmitted ePHI were not completed. Furthermore, the hospital did not have a complete listing of these systems.

Without completed contingency plans, the hospital could have lost the ability to process, retrieve, or protect information electronically, which could have significantly affected the hospital's ability to accomplish its mission and provide patient care. Even minor interruptions could have resulted in lost or incorrectly processed data, expensive recovery efforts, and inaccurate or incomplete ePHI. For example, the hospital did not complete a contingency plan for its system that provides ready access to patient health care records and test results. Damage to this system could have negatively affected the integrity and availability of the ePHI it contained, thereby negatively affecting the hospital's ability to deliver quality patient care.

Incomplete Disaster Recovery Plan

Two hospitals did not have a comprehensive disaster recovery plan that included information systems that contained or transmitted ePHI. In addition, the documentation that one hospital provided as its business continuity plan did not include the critical elements required by its own policy, e.g., information regarding arrangements for prolonged unavailability of critical information resources, key personnel, telecommunications, office accommodations, and managed services.

Unsafe Backup Tape Storage

One hospital kept daily incremental backup tapes containing ePHI in its data center and sent full backup tapes to an offsite storage facility only once a week. A disaster at the data center could have placed 6 days' worth of data at risk, resulting in considerable cost to the hospital and making it difficult for patients to replace medical procedure history and other patient ePHI. Moving the daily backup tapes to a location distant from the data center and suitable for storage of magnetic media is an industry best practice. Also, the hospital did not send the catalog tape specifying the content of the backup tapes to an offsite storage facility. If a disaster had occurred, the hospital might not have been able to locate and recover ePHI data because it would have been unable to determine the contents of the backup tapes.

No Procedures for Unscheduled System Interruptions

One hospital had not documented procedures on how to replace the functions of its Web-based primary ePHI viewing system during unscheduled interruptions. Instead, the hospital relied on a screen that listed help desk and various hospital department contact phone numbers that appeared when the viewing system was unavailable.

APPENDIX C: INFORMATION TECHNOLOGY TERMINOLOGY

Computer Resources	Computer resources are: (1) An aggregate of computer equipment, programs, documentation, services, facilities, and personnel available for a given purpose: devices such as printers and disk drives are resources; memory is also a resource. (2) In many OSs, including Microsoft Windows and the Macintosh OSs, the term "resource" refers specifically to data or routines that are available to programs. These data or routines are also called system resources.
Domain Controller	A domain controller is a type of server that authenticates user names and passwords when users log onto the network.
Operating System	The OS is the most important program that runs on a computer. Every general-purpose computer must have an OS to run other programs. OSs perform basic tasks, such as recognizing input from the keyboard; sending output to the display screen; keeping track of files and directories on the disk; and controlling peripheral devices, such as disk drives and printers.
Router	A router is a device that forwards data packets along networks. A router normally connects at least two networks, commonly two LANs or wide area networks or a LAN and its Internet Service Provider's network. Routers are located at gateways, the places where two or more networks connect.
Server	A server is a computer or device on a network that manages network resources. For example, a file server is a computer and storage device dedicated to storing files. Any user on the network can store files on the server. A print server is a computer that manages one or more printers, and a network server is a computer that manages network traffic. A database server is a computer system that processes database queries.
Software	Software is the instructions executed by a computer, as opposed to the physical device on which they run (the "hardware"). Software can be computer instructions or data. Software is often divided into two categories: • systems software, which includes the OS and all the utilities that enable the computer to function, and • applications software, which includes programs that do real work for users, such as word processors, spreadsheets, and database management systems.

System Administrator	A system administrator is an individual responsible for maintaining a multiuser computer system, including a LAN. Typical duties include: adding and configuring new workstations, setting up user accounts, installing systemwide software, performing procedures to prevent the spread of viruses, and allocating mass storage space. Small organizations may have just one system administrator, whereas larger ones usually have a team of system administrators.
System Configuration	System Configuration is the way a system is set up or the assortment of components that make up the system. "Configuration" can refer to hardware, software, or the combination of both. For instance, a typical configuration for a personal computer consists of the main memory, a floppy drive, a hard disk, a modem, a network card, a CD-ROM drive, a monitor, and the OS.
Windows	Microsoft Windows is a family of OSs for computers.
Wireless Access Point	A wireless access point is a hardware device or a computer's software that acts as a communication hub for users of a wireless device to connect to a wired LAN. Access points are important because they connect users to heightened wireless security and extend the physical range of service.
Wireless Network Scan	A wireless network scan is the act of driving or walking around with a laptop computer, an antenna, and an 802.11 wireless LAN adapter to detect existing wireless networks. Set on promiscuous mode, the wireless adapter (typically a Network Interface Card) receives packets within its range. Wireless network scans detect wireless networks that have ranges that extend outside the perimeter of buildings to identify configuration weaknesses that might enable individuals to gain free Internet access or unauthorized access to an organization's data.

APPENDIX D: OFFICE FOR CIVIL RIGHTS COMMENTS

DEPARTMENT OF HEALTH & HUMAN SERVICES

Office of the Secretary

Director
Office for Civil Rights
Washington, DC 20201

March 18, 2011

To: Daniel R. Levinson
Inspector General

From: Georgina Verdugo
Director, Office for Civil Rights

Subject: Nationwide Rollup Review of the Centers for Medicare & Medicaid Services Health Insurance Portability and Accountability Act of 1996 (HIPAA) Oversight (Report #: A-04-08-05069)

Thank you for the opportunity to review the subject draft report. The Office for Civil Rights (OCR) appreciates the efforts and recommendations of the Office of the Inspector General (OIG). OCR cannot comment on the specific findings contained in the report as OCR was not involved in the selection of the covered entities for review or the establishment of the criteria for review. Further, OCR received only summaries that did not contain specific evidence that would permit evaluation of the findings.

As a general comment, we caution against drawing conclusions about the state of compliance of all covered entities based on the small sample of narrowly focused audits performed in the review of CMS oversight. [redacted]

- [redacted]
- [redacted]

We have considered the recommendation to OCR to continue the compliance review process that CMS began in 2009, and to have a process and implement procedures for the performance of compliance reviews to ensure that Security Rule controls are in place and operating as intended

Office of Inspector General Note -- Technical comments in OCR's response to the draft have been omitted from the final report and all appropriate changes have been made.

to protect electronic protected health information. We note that under the HIPAA Enforcement Rule, OCR maintains a process to initiate compliance reviews of covered entities in the absence of a complaint, through which we investigate for non-compliance and seek corrective action. We have used this process to open compliance reviews as a result of the seven hospital audits conducted by the OIG. As part of each review, OCR has developed a corrective action plan to be completed by the covered entity to ensure the vulnerabilities identified by the OIG are mitigated and corrected. When the covered entity completes the corrective action in a manner satisfactory to OCR, the compliance review is closed.

In addition, OCR performs compliance reviews of covered entities when they report a breach of unsecured protected health information affecting 500 or more individuals, pursuant to the Breach Notification Rule. See 45 CFR Part 164, subpart D. These reviews by OCR seek the root cause of the unauthorized disclosure and, where the disclosure involved electronic protected health information, broadly examine whether the covered entity has appropriate safeguards in place to protect the confidentiality, availability, and integrity of electronic protected health information to satisfy the requirements of the Security Rule.

Thank you again for the opportunity to review the draft report. Please do not hesitate to contact me with any questions.