Surviving a CMS Security Investigation: Oregon Facility Shares an Early Look at the Process

by **Judi Hofman,** CAP, CHP, CHSS

Hospitals and other healthcare organizations are expecting greater scrutiny of their HIPAA compliance programs in 2009. Last year the Centers for Medicare and Medicaid Services (CMS) announced plans to ramp up its HIPAA enforcement efforts even before an Office of Inspector General report chided it for ineffective oversight to date.[1]

So far, however, covered entities have had little indication of what new, more aggressive CMS oversight will look like.

Little has been heard of HIPAA audits or investigations since an audit of Piedmont Hospital in 2007. The description leaked from that investigation gave a glimpse of technical reviews that appeared to be hands-on testing of systems for security compliance, but this was never confirmed. So far, covered entities have lacked the opportunity to understand the audit and investigational process and learn from the experiences of others.

In August 2008 CMS conducted an on-site investigation at Cascade Healthcare Community in Oregon. This article offers some insights into that experience.

The Alleged Breach

Cascade Healthcare Community is a private, not-for-profit Oregon corporation with more than 3,000 caregivers in Bend, Redmond, and Prineville, OR. The incident involved a computer virus that caused the potential exposure of the names, addresses, and credit card numbers of more than 11,500 individuals who had donated to Cascade's hospital foundation and air transportation program. Cascade IT staff noticed suspicious system activity in late December, and after extensive investigation the organization reported possible exposure of data in February.

It was not initially clear whether any of the information was seen by individuals outside the hospital. Luckily, there was no evidence that patient health information was ever compromised or exposed.

Cascade worked quickly and diligently to provide all affected donors with free information and credit-monitoring service from a well-known agency. The details of the possible breach were reported in countless publications and Web sites such as the Breach Blog, the Privacy Rights Clearinghouse, Security Ratty, and *SC Magazine* .

The CMS Inquiry

On May 20, 2008, CMS contacted Cascade to inquire about the organization's compliance with the HIPAA security standards. The inquiry made reference to media reports that a virus had caused the organization to expose personally identifiable information inappropriately.

On July 1, 2008, Cascade received a letter from CMS's Office of E-Health Standards and Services announcing that it would be conducting a review to determine whether Cascade was compliant with areas of the HIPAA security rule related to the complaint under investigation and to the control of remote access and use.

While the inquiry identified only certain provisions of the security rule, it also raised general concerns about Cascade's overall level of HIPAA security compliance. Due in part to this broader concern, CMS elected to conduct an on-site investigation, and it hired PricewaterhouseCoopers (PwC) to conduct the on-site review.

The Investigation

CMS used a tracking form similar to the one shown in "Audit Checklist and Documentation Request Form" (see page 44). The form indicates the scope of the investigation and the documents requested. CMS requested applicable documents in electronic format and asked that Cascade provide the PwC investigation team with working space for three people for three to four business days.

To improve efficiency, Cascade created a secured online "drop box" into which staff dropped relevant documents. Investigation team members were given unique user names and passwords so that they could access the documents remotely.

The four days of the investigation were long and busy. The process required the entire organization's participation. Testing included the review of all relevant policies and procedures as well as targeted testing to verify that the controls outlined in the documents were operating effectively.

In addition to policy and procedural reviews, Cascade staff conducted many internal meetings to discuss the process, including the following:

- Pre-entrance meeting (July 25, 2008)
    - Conference call with investigating team from CMS, PwC, and Cascade (CEO, executives, and applicable department leadership)
- On-site meetings (August 4–7, 2008)
    - Incident overview and response (information security personnel and security incident response team)
    - Hiring, termination, and training policies and procedures (human resources staff)
    - IT environment overview (information security personnel)
    - Incident response and network monitoring (information security personnel)
    - Patch and antivirus management (IT senior leadership, IT technical team, information security personnel)
    - On-site exit conference (CEO, executives, and applicable department leadership)
- Exit meeting (August 20, 2008)
    - Conference call with investigating team from CMS, PwC, and Cascade (CEO, executives, and applicable department leadership)

Between August 18 and August 29, PwC submitted two drafts of the report, incorporating responses from Cascade. PwC delivered the final report to CMS on September 1, which included Cascade's responses.

The investigating team generated a list of the gaps identified between the HIPAA security requirements and Cascade's implementation of them and attached it to the summary report sent to CMS. Other attached reports provided detailed information on the observed gaps and recommended corrective actions. Additional recommendations included ways that the hospital could strengthen its security posture as recommended by NIST SP 800. An example from the gap analysis chart can be found on page 45.

Findings and Recommendations

Cascade's experience offers organizations several lessons on the CMS process. First and foremost, organizations should confirm that their formal, documented risk assessments are up to date. They should include individual risk assessments for each application that contains protected health information and personally identifiable information.

It may be helpful for organizations to prepare a list of current staff members broken out by those with less than a year of service and those with more than a year of service. CMS requested that Cascade provide documentation of HIPAA security education *prior* to access of any computer systems for staff who had been employed for less than a year. Cascade was required to provide documentation of yearly HIPAA security education for staff employed more than a year.

Organizations will also benefit by taking time and effort to understand and use the full capabilities of their antivirus solutions, specifically around centralized management. CMS asked Cascade to generate a list of all workstations (both desktops and

laptops) for a random audit of systems that included a check for individually activated firewalls.

An organization's security work comes down to developing appropriate policies and procedures and performing targeted testing to verify that the controls outlined in their written documents are operating effectively. The CMS investigation undergone by Cascade was as thorough and rigorous as the audits that other hospitals pay hefty sums to consulting companies to perform.

CMS indicated to Cascade legal counsel that the results of its investigation will be de-identified and disseminated to assist other facilities comply with the HIPAA security rule as a whole. CMS assured Cascade that it would protect sensitive or confidential information received during the on-site investigation to the full extent permitted by federal law. Such information, as indicated by CMS, is generally not available to the public under federal disclosure laws.

Cascade received the final report from CMS on December 22, 2008. CMS accepted all findings from PwC, with Cascade's corrective action measures set forth with completion dates for compliance. CMS requested written certification within 30 days of the full implementation of each corrective action with evidence of completion and continued performance of the documented measures.

The Investigation Timeline

February: Cascade announces the possible breach
May: CMS contacts Cascade to inquire about the organization's compliance with the HIPAA security standards
July 1: CMS's Office of E-Health Standards notifies Cascade that it will conduct an on-site investigation
August 4–7: Investigation
August 13: Requested items due from Cascade to PwC
August 18: First draft report from PwC to Cascade and CMS
August 20: Exit meeting and conference call with CMS, PwC, and Cascade
August 22: Second draft of investigation from PwC to Cascade and CMS
August 29: Cascade response to second draft to PwC
September 1: Final report (with Cascade responses) from PwC to CMS
December 22: Final report from CMS to Cascade

Audit Checklist and Documentation Request Form

The investigation team used a documentation request form similar to the one shown here.

Administrative Safeguards	
AS-1	Policies and procedures on creation, maintenance, and governance of risk assessments and system security plans
AS-2	Most current risk assessment for impacted applications and general support systems, including certification/approval page Please note: if there are multiple risk assessments/system security plans, please provide those for applications and general support systems that process or store personally identifiable information (PII)/protected health information (PHI).

AS-3	Most current system security plans for impacted applications and general support systems, including certification/approval page Please note: if there are multiple risk assessment/system security plans, please provide those for applications and general support systems that process or store PII/PHI.
AS-4	Policies and procedures on protection of PHI and electronic PHI (ePHI), including sanctions for violation of policy: • Including procedures on the protection and use of Blackberry devices, thumb drives, portable disk drives, etc. • Compliance with HIPAA security rule • Evidence to support distribution of procedures to pertinent personnel
AS-5	Listing of all PHI violations within the past year
AS-6	Policies and procedures governing monitoring of access and violations, including follow-up activities for suspicious activity; policies and procedures that include information on: • Records logging information system activity, including audit logs, access reports, and security incident tracking reports • Incident response activities-detecting, reporting, and responding to security incidents • Intrusion detection system
AS-7	IS department organization chart, including privacy/HIPAA official
AS-8	Job description for privacy/HIPAA official
AS-9	Security awareness, privacy, training content (initial and annual)
AS-10	Listing or organization chart of all incident response team members, including job descriptions for team members
AS-11	Listing of all current employees (including name, department, cost center, job title, and direct supervisor/manager)
AS-12	Listing of all employees hired within the past year (including name, department/cost center, job title, and direct supervisor/manager)
AS-13	Policies and procedures governing security awareness training (new hire and refresher)
AS-14	Policies and procedures governing virus identification software, including updating, detecting, and reporting malicious software or viruses

AS-15	Policies and procedures (baselines) governing passwords including: • Password standards, configurations • Creation, changing, and safeguarding • Passwords on remote devices (laptops, PDAs, etc.)
AS-16	Policies and procedures for data and resource classification
AS-17	Most recent internal audit/review of HIPAA compliance
AS-18	Network diagram
Technical Safeguards	
TS-1	Policies and procedures governing the use of generic, group, or system IDs
TS-2	Policies and procedures governing disabling vendor-supplied defaults
TS-3	Policies and procedures governing granting of dial-up/remote access
TS-4	Policies and procedures on the encryption/decryption of ePHI: • During transmission • ePHI on remote devices • ePHI on backup and archived data
TS-5	Evidence of the implementation of password policies on platforms which store, transmit, or process ePHI
TS-6	Transmission security procedure (formal requirements for transmission of ePHI, controls governing integrity of information transmitted on networks)
TS-7	Configuration standards for platforms which store, transmit, or process ePHI (including workstations)
TS-8	Policies and procedures governing the use of wireless networks in the environment
TS-9	Wireless access points baseline configurations (if applicable)

Physical Safeguards	
PS-1	Policies and procedures governing workstation security (for devices storing ePHI) including onsite, laptops, at home system use, etc.
PS-2	Inventory of laptops and desktops in your environment
Remote Access	
RA-1	Procedures/baseline for firewall protection on laptops
RA-2	Listing of users provided with laptops and remote access
RA-3	Rules of behavior, personnel security rules for laptop users
RA-4	Entity-wide patch management policy (including pushing updates to remote devices)
RA-5	Entity-wide configuration management policy (including remote devices)

Sample HIPAA Complaint Investigation Summary

A gap analysis chart captured the issues identified in the investigation and Cascade's response and corrective action plan. A sample item is shown here.

HIPAA Security Rule Area	HIPAA Security Rule Section	Control Area and Step	Gap Noted between Procedures and HIPAA Requirement or Addressable Area	Recommended Corrective Action if Requested

Administrative Safeguards	164.308(a)(1) (ii)(A) Risk analysis: "Conduct accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity." (Required)	Determine if relevant information systems have been identified. Determine if a risk assessment has been conducted and documented.		
Covered Entity Response		**Covered Entity Planned Corrective Action Plan (CAP) Steps**		**Target Date for Completion of CAP Steps**
Add response here		Add corrective action here		Set target date for compliance here

Note

1. Office of the Inspector General. "Nationwide Review of the Centers for Medicare and Medicaid Services Health Insurance Portability and Accountability Act of 1996 Oversight." October 2008. Available online at www.oig.hhs.gov/oas/reports/region4/40705064.asp.

Judi Hofman (jhofman@cascadehealthcare.org) is a privacy and information security officer at Cascade Healthcare Community in Bend, OR.

Article citation:
Hofman, Judi. "Surviving a CMS Security Investigation: Oregon Facility Shares an Early Look at the Process" *Journal of AHIMA* 80, no.2 (February 2009): 42-45.