

## The Next Evolution of HIPAA Security

### **Introduction**

It is difficult to remember a time without the HIPAA Rules, yet, only four years have passed since implementation of the HIPAA Security Rule. Much to the surprise of Security Officers, the Security Rule was found to be more difficult to interpret and implement than the industry-changing Privacy Rule. Not surprising then are a number of health industry reports indicating many covered entities are not yet, years later, compliant with *all* of the specifications of the Security Rule.

Because the Security Rule is intentionally written to be scaleable and flexible, it leaves covered entities with a great amount of uncertainty as to whether they are truly complying with all the standards. The complexity of diverse clinical applications, a lack of industry standards, constantly changing technologies and limited information technology (IT) budgets have lead some organizations to essentially ignore the HIPAA Security Rule. Incomplete implementation has flourished because there has been very little governmental oversight or enforcement action. With so many competing priorities, where is the logic in putting precious time and resources into complying with a regulation that isn't being enforced?

Nevertheless, enforcement was inevitable. The federal government has officially begun conducting HIPAA Security audits and sanctioning organizations that fail to comply. The positive side of the recent investigations, if there is one, is that they provide some insight into how the government is interpreting the Security Rule and more specifically, what Security Officers, Privacy Officers and Compliance Officers need to do to be best prepared.

# HIPAA Security Timeline

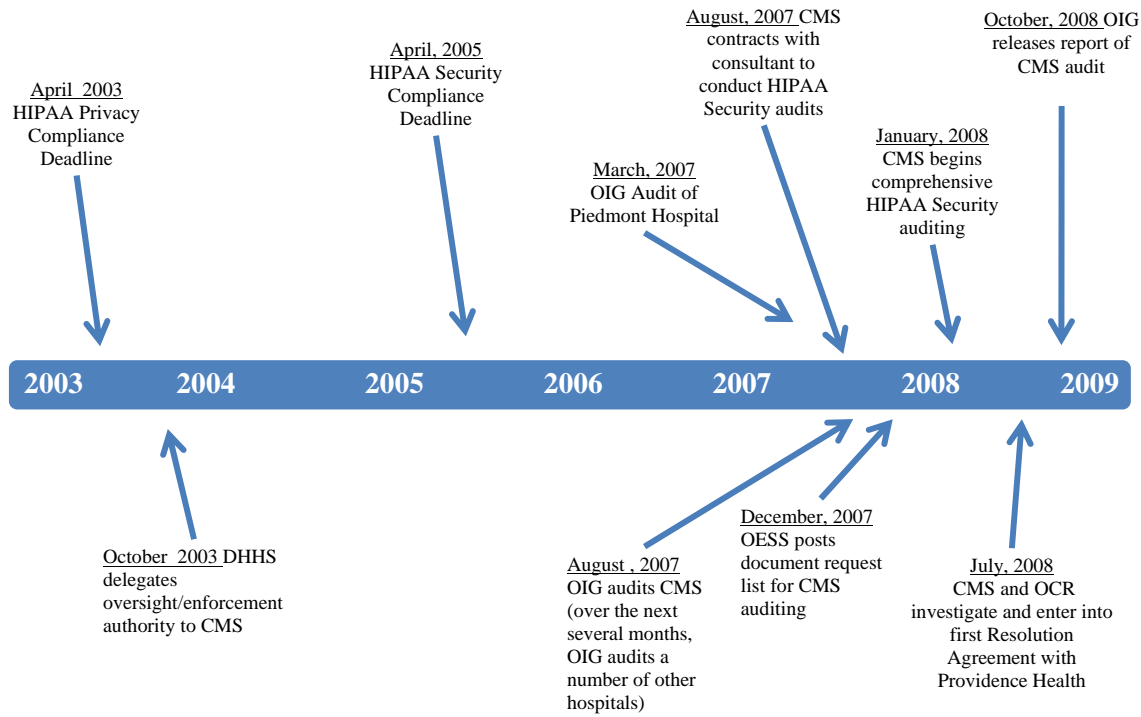


Exhibit A.

## Federal Auditing

In October 2003, the Department of Health and Human Services (DHHS) delegated authority to the Centers for Medicare and Medicaid (CMS) to enforce compliance with the HIPAA Security Rule. This is in contrast to oversight of the HIPAA Privacy Rule which was delegated to the Office for Civil Rights (OCR). Since the compliance deadline for covered entities in 2005, virtually nothing has been heard about HIPAA Security auditing or enforcement.

Because of this perceived lack of enforcement action, the Office of Inspector General (OIG) stepped in and audited CMS in August 2007. The purpose of their audit was to “evaluate the effectiveness of CMS’s oversight and enforcement of covered entities’ implementation of the HIPAA Security Rule.” In late October 2008, (14 months after the audit was completed) the OIG released their report in which they found CMS had “not provided effective oversight or encouraged enforcement of the HIPAA Security Rule.” In its report, the OIG further states that “as of August 24, 2007, [2 years after the implementation date for covered entities] CMS had not conducted any compliance

reviews of covered entities to determine whether the HIPAA Security Rule was being properly implemented.”

CMS’ response to the reprimand from the OIG is that their enforcement approach was complaint-driven, and founded on a philosophy that emphasizes voluntary compliance, much like the enforcement strategy of the OCR which has been in place for a much longer period of time. Based upon their investigation of a few hundred complaints, CMS stated the problems are widely distributed across the diverse HIPAA Security standards and that the vast majority of violations are not ill-intended or deliberate. Still, the OIG recommended, and CMS concurred, that CMS needs to focus on conducting audits of covered entities for compliance with all of the Security Standards, and not just focus on simple complaint specific investigations. CMS agreed to implement a formal audit process to conduct *comprehensive* HIPAA Security reviews of covered entities that have had a complaint filed against them.

In the 14 months between the OIG’s audit of CMS and the release of the results of that audit, and perhaps to develop their own understanding of how covered entities were interpreting the flexible standards, the OIG conducted their own on-site HIPAA Security audit of a covered entity. In March of 2007 the OIG audited Piedmont Hospital of Atlanta and found “significant vulnerabilities” that left electronic Protected Health Information (ePHI) unprotected. After the Piedmont audit, the OIG proceeded to conduct audits of other hospitals around the country and found results consistent with the first, i.e., weaknesses in the implementation of the administrative, technical and physical safeguard provisions of the Security Rule. The OIG has not published findings specific to the Piedmont audit, or of each of the other independent audits they conducted, but only summarized results indicating less than adequate compliance by the covered entities and inadequate enforcement by CMS.

Late in 2007, the DHHS Office of E-Health Standards and Services (OEHS) posted on CMS’ website a sample document request list for an on-site compliance audit. This was the first real insight covered entities had into federal interpretation and enforcement of the HIPAA Security Rule. CMS now states on their website that they have been conducting, through an independent consulting firm, compliance reviews of covered entities since January 2008.

Of the audits CMS has conducted for over a year, the only specific audit results released have been the mid-2008 audit of Seattle-based Providence Health & Services (Providence), conducted in cooperation with the OCR. The final audit report states that on a number of occasions in 2005 and 2006, media and laptops containing PHI were removed from company property, left unattended, not encrypted and/or either lost or stolen. Failure on Providence’s part to implement policies and procedures to protect PHI were the focus of the audit. The audit resulted in the first Resolution Agreement between the federal government and a covered entity. The Agreement and Providence’s Corrective Action Plan (CAP) are available on the OCR’s website.

After careful review, three additional observations can be made of the Providence audit. First, because Providence voluntarily worked in full cooperation with the governing federal agencies, no civil monetary penalty was imposed. Next, the Providence audit was conducted jointly by the OCR, responsible for oversight of the Privacy Rule, and CMS, responsible for oversight of the Security Rule. Finally, the audit was complaint-driven. In compliance with State of Washington notification laws, Providence notified the patients whose PHI was mishandled, who in turn complained to the Department of Health and Human Services who turned the matter over to CMS to perform an on-site investigation.

### **Complaint Driven Investigations**

Since all HIPAA Security investigations to date seem to be complaint driven, more insight can be gained from understanding of the types of complaints CMS is receiving. CMS posts on its website, albeit difficult to find, HIPAA Enforcement Statistics which are a summary of the types of complaints they have received, beginning in July 2007. CMS manages, on average, over 330 complaints per month which includes a cumulative total of both open and closed complaints. Each security complaint received is categorized into the type or types of violations alleged; a single complaint can result in a number of different violations of the security provisions.

Consistently throughout 2008, the 3 greatest numbers of complaints CMS received monthly regarding specific Security Standards were:

- Information Access Management (Administrative Standard 164.308(a)(4)(i));
- Access Control (Technical Standard 164.312(a)(1)); and
- Security Awareness and Training (Administrative Standard 164.308(a)(5)(i)).

Of the complaints and violations CMS is receiving and investigating more than half are related to Access Management and Control. The third greatest number of violations can be attributed to training.

Based upon the findings of the compliance audits they began conducting in January 2008, CMS has begun posting specific compliance scenarios, “HIPAA Complaint Examples”, on their website as additional guidance. These real-life scenarios provide valuable insight into enforcement. The scenarios currently listed highlight a problem with shared passwords, and an incident in which patient information was errantly viewable (on a provider’s website intended to assist patients’ in self-scheduling.) Both incidents were closed after CAPs were implemented.

### **Industry Best Practices**

Given the audit findings, statistics on complaints and examples of violations, a number of conclusions can be drawn from the government’s seemingly uncoordinated auditing:

- Increased governmental scrutiny of compliance with the HIPAA Security law is definitely going to become a reality, even if the target for on-site audits is still based upon complaints received by CMS.
- The OCR and CMS will likely continue to collaborate to conduct on-site investigations for potential non-compliance of patient confidentiality issues simply because the privacy and security rules are so inter-twined.
- Most importantly, the most significant problem faced by covered entities subject to the HIPAA Security Rule is the passive loss of data due to their own inaction. The regulations are, of course, in part, designed to address what all covered are potentially in danger of: an intentional attack on our information systems from those without authorized access. But, these types of planned and/or malicious threats are not where the most vulnerability lies. *Failure of covered entities to fully and completely implement the regulations, resulting in non-compliant activity by authorized users, is the greatest compliance risk.*

A thorough analysis of the information summarized above, along with the original Security Rule documents, enables conscientious Security Officers to formulate a sound action plan in preparation for a HIPAA Security audit. Covered entities should carefully consider and implement the following:

- **Conduct a complete, and up-to-date risk assessment.** If the objective vetting of practice versus regulations has fallen by the wayside because of competing priorities and lack of regulatory oversight, covered entities should conduct an up-dated risk analysis as soon as possible and implement the necessary risk management strategies.
  - In evaluating your risk, consider how you have addressed Information Access Management and Access Control. Non-compliance with these two closely related but distinct sets of standards results in the majority of complaints and violations handled by CMS.
  - Carefully evaluate what is perhaps the problem heard most about in the news and what seems to also trigger many of the initial complaints and subsequent investigations—remote access to PHI and portable media containing PHI.
- **Documentation is essential to compliance.**
  - Focus precious resources on ensuring you have written policies and procedures in place, especially for your highest risk areas. The violations summarized by CMS to-date evidence problems with information access, access controls and adequate training. Be sure these standards and implementation specifications have clear policies and procedures.
  - Remember that your rationale for the addressable but not required implementation specifications must be documented.
  - Use the CMS document request list provided by the OESS as a guide to preparing all the necessary documentation. If, in reviewing this list, all your documentation is not in order, create an action plan with deadlines to get it completed.

- **Comprehensive training of your entire workforce cannot be emphasized enough.** If HIPAA Security training has not been conducted in the last couple years, or has not been provided since the compliance deadline in 2005, get something scheduled. Excellent policies and procedures are wasted without an effective training program.
  - Train based on your greatest risk areas identified in the Risk Assessment.
  - While providing HIPAA Security training at new employee orientation is necessary, on-going, regular training for the rest of your workforce is an absolute must.
  - Be sure your workforce (including employees, vendors and officers) knows your policy for remote access to ePHI and on ePHI saved on or transmitted through portable media. It would even be recommended that you require all those with remote access or who use portable media of any type, to sign an attestation stating they:
    - ✓ have received the education,
    - ✓ agree to abide by the policies of the organization,
    - ✓ understand the risk to ePHI inherent in electronic use and
    - ✓ know the degree of discipline they face for violations of the policy.
  
- **A sufficient disciplinary policy is a necessity.** You need to both have a strong disciplinary policy in place and to abide by it. Training without enforcement is of little value. There should be serious consequences for violation of HIPAA security policies since such a violation may be putting the confidentiality of your entire patient population at risk. Taking strong disciplinary action against an employee who violates your policies and procedures and/or the Security Rule provides, perhaps, one of your best defenses should you be investigated.
  
- **Realize that if the OCR is collaborating with CMS to conduct HIPAA audits your Privacy Officer and your Security Officer should be collaborating in preparation for an audit.**

To further assist with the recommendations above, the federal government offers many written resources and guidance to help sort through the complex compliance requirements. The challenge can be in locating these various types of information because they are scattered on a number of different government websites.

Many private sector organizations, recognizing the burden of complying with the various HIPAA regulations placed on health care entities, also offer resources. Just to mention one, the Workgroup for Electronic Data Interchange (WEDI) is an association whose purpose is to improve health care quality through electronic information exchange. To facilitate industry-wide collaboration for the implementation of HIPAA and other IT standards, WEDI formed the Strategic National Implementation Process (SNIP). WEDI SNIP further supports regional affiliates in many states that offer a multitude of resources at little or no cost. For instance, in the State of Wisconsin the consortium is the HIPAA

Collaborative of Wisconsin. (Yes, it's referred to as HIPAA COW!) Since 2001, HIPAA COW has offered on their website a multitude of sample policies and procedures, white papers, forms and other resources. They also sponsor interactive conferences three times per year.

## **Conclusion**

What we are witnessing is the next evolution of HIPAA Security, not just the latest regulatory trend. The recent American Recovery and Reinvestment Act (ARRA), the Economic Stimulus Bill, is going to have an enormous impact on HIPAA Security and Privacy practices. Included in the ARRA are tens of billions of dollars to expand the use of health information technology as well as significant changes to the HIPAA laws. The changes greatly affect business associates of all covered entities, the rules regarding electronic health records (EHRs), accounting of disclosures as established in the HIPAA Privacy Rule, and drastic changes in enforcement. Part II of this article will outline and examine the sweeping changes ARRA is going to have on health care entities. You would do well to prepare yourself now for the inevitability of a HIPAA Security audit.