Information Trustworthy under HIPAA in Healthcare industry

By Eddy Tan

Overview

- What is HIPAA

April 13, 2003 was a landmark date for healthcare organizations through the United States. This is the day that the Healthcare Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule went into effect, carrying with it security implications in the form of privacy safeguards. HIPAA seeks changes or reforms in the following areas: portability of health insurance, prevent healthcare fraud and abuse, administrative simplification, tax related provisions, group health plan requirement and revenue offset.

- Purpose of HIPAA

The federal government introduced HIPAA with expectations to lower the health care administrative cost, improve the efficiency and effectiveness of health care delivery system and to protect and safeguard patient health information

- Application of HIPAA

HIPAA regulation applies to every health plan, health care clearinghouse, health care provider and their business associates that transmit any administrative health information in electronic form. Every transaction within the corporate entity is subject to HIPAA requirements just as they are between such entities. Any record transmitted electronically, even in paper format, is subject to the privacy rules.

Review

- **Key Concepts**

Security standards: General rules

Covered entities must do the following section 164.306(a):
:

1) Ensure the confidentiality, integrity, and availability of all electronic protected health information that 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 the Privacy Rule.
4) Ensure security compliance with this subpart by its workforce (Federal Register, vol. 68, no. 34, 8376).

Administrative safeguards

According to the definition of administrative safeguards in section 164.304, a covered entity must establish the "administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of the 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" (Federal Register, vol. 68, no. 34, 8376).

This rule also establishes the requirement for a written contract between the entity and any business associate who creates, receives, maintains or transmits PHI on the covered entity's behalf.

Physical safeguards

According to the definition of physical safeguards in section164.304, the covered entity must establish the "physical measure, policies, and procedures to protect their electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion" (Federal Register, vol. 68, no. 34, 8376).

Based on this section of the rule, an entity should incorporate facility planning into both its initial risk analysis as well as its on-going risk management activities.

Technical safeguards

According to the definition of technical safeguards in section 164.304, the covered entity must implement both the “technology and the policies and procedures for its use that protect electronic protected health information and control access to it” (Federal Register, vol. 68, no. 34, 8376).

This section of the rule outlines the technical standards for: access control, including unique user identification, emergency procedures for access to electronic PHI, automatic logoff, and encryption of electronic PHI; audit controls; information or data integrity including authentication mechanisms to ensure against the alteration or destruction of data in an unauthorized manner; person or entity authentication; and transmission security including integrity controls over and encryption of the electronic PHI in transit.

Organizational Requirements

This section of the rule delineates the contractual requirements (i.e., terms and conditions) for a business associate that is involved with the creation, receipt, maintenance or transmission of electronic PHI on behalf of the entity. Under the requirements of this section, an entity must take corrective action if they are aware of a pattern of activity or practice that would constitute a material breach or violation of their business associate’s contractual obligation. If corrective action is not feasible, then the contract must be terminated by the entity. The contract between the entity and the business associate must have a termination clause that supports this action.

Policies, Procedures and Documentation Requirement

The rule requires that an entity implement policies and procedures (P&Ps) outlining how they will comply with the standards, implementation specifications, and other requirements of the Security Rule. From a review of the entire rule, documentation will include: risk analysis results, audit logs, access reports, security incident reports and outcomes, policies and procedures related to security, contracts with business associates, facility maintenance records, device and media accountability and tracking records, media disposition and tracking records. Some of this information will contain electronic PHI and be subject to additional privacy and confidentiality regulations.

Both P&Ps and any other required records from an action, activity, or assessment must be maintained in written (including electronic) format for 6 years from the date of creation or the date of implementation, whichever is later. The information must be readily available to the workforce responsible for implementation of the procedures. The information must be reviewed and updated on a periodic basis, whether yearly or whenever the entity incurs changes in its operational processes, infrastructure, or environmental needs.

- ***Managerial Issues***

Why business should care about risk? In the health care industry, the risks are eminent including patient confidentiality, integrity of information. It is paramount to safeguard that information and bring the threat to manageable level before business spends plenty of money for vulnerabilities.

The overall objective of a HIPAA risk analysis is to document the risks that threaten to negatively impact the confidentiality, integrity, or availability of electronic protected health information and determine the appropriate safeguards to bring the level of risk to an acceptable and manageable level. It doesn’t make sense to blindly spend money and resources on security controls and safeguards without first knowing exactly what we’re protecting, what we’re protecting it from, what its weaknesses are, and the potential magnitude of loss (single loss expectancy (SLE)) due to an exposure. For example, it is not ‘appropriate’ to spend $50,000.00 per year on safeguards to protect the privacy of something when the annualized loss expectancy or impact to business would not exceed $10,000.00. The choices of safeguards should be based on actual risks to actual assets that have some value to the organization. The confidentiality, integrity, and availability of an asset is what we’re protecting; threats are what we’re protecting the asset from, the weaknesses are termed ‘vulnerabilities’, and the potential magnitude of loss or impact describes the ‘value’ or importance of confidentiality, integrity, and availability of the asset to the organization.

Risk is therefore a function of the value or criticality of an asset, the likelihood of and potential harm from threats to the asset, and the vulnerabilities of the systems that incorporate the asset to the threats.

Example and Cases

For the case study I picked the example GAIC Health. The Agency provides comprehensive family-centered, social, educational, and behavioral health programs for children and their families. They are involved in residential and day treatment programs, run two schools, and provide community based services. The Agency has non-profit status with funding sources that include the local county’s behavioral health system, state Medicaid, federal, and private funding sources.

The workforce includes permanent employees, vendors, business associates (Such as the legal counsel and IT vendors), volunteers, and interns. There are about 250 permanent employees and the retention rate is fairly high. All members of the workforce that have direct contact with the juvenile clients and all permanent employees undergo a stringent background check as part of the employment process and a lengthy probation period upon acceptance. Workforce IT skills are gradually improving commensurate with the growing dependence within the Agency on electronic information management.

Security-related activities were already distributed through out the agency there was no defined security support organization to address the emphasis that HIPAA placed on both the privacy and security of health-related information. The Information Management/Technology Department is the obvious focus for the Agency’s security organization.

Information Management

The Agency is transitioning from paper to a completely electronic environment for all their records. These include the medical, the mental health, and the educational charts for each juvenile client under Agency care.

When dealing with behavioral health issues, an increased level of privacy is required under both state and federal statues. Access to the medical and the mental health records for a client must be clearly separated and controlled strictly on a “need-to-know” basis. A medical doctor, for example, may be only authorized to see the medical history but not the mental health chart. Presently, the Agency concurrently manages both types of records in paper and electronic formats. This requires accurate tracking of who has authorized access to what type of record, who has accessed a record, when and for what purpose, and any unauthorized access to PHI.

The Agency has invested heavily in the development of an electronic medical records system. This is based on Microsoft SQL Server and is considered the Agency’s most mission critical system. Housed at the headquarters, it is slowly becoming the central ‘electronic’ chart room for the Agency, containing all medical, mental, and educational records for all Agency clients. The Agency still relies on the original vendor design for system administration and audit capabilities. The use of this system generates both privacy and security concerns under HIPAA.

Information Technology

The Agency is an excellent example of steady, sustained growth. Management has planned wisely and has invested in solid technology to support their workforce. In 1995, they had a total of 10 computer systems at a single site. By 1999, this had grown to 7 servers and 140 systems across 7 sites. As of October, 2002, the agency had 21 servers and 315 systems (of which 150 are laptops) across 4 main sites and numerous secondary ones to include four group homes, several middle and high schools where the Agency provides services, and the home offices of key staff members who telecommute.

The administrative offices are at the heart of the network. The gateway router to the Internet is located here as is the Cisco 3015 Virtual Private Network (VPN) concentrator and the main Agency firewall. Dedicated point-to-point T1 lines connect the three main facilities (the residential campus, the community based services and day school, and the community based school) to the administrative office suite. The systems supporting the Agency's mission critical applications are located at headquarters.

The initial situation assessment revealed many security gaps, both technically and functionally. The Agency was on the verge of becoming overly dependent on their tools without really understanding where the holes in the technology might be and where they might be compromised. The need to comply with HIPAA privacy regulations had been a wake-up call. Management was now aware that even privacy had security implications and, like most healthcare organizations, was concerned and edgy over what the implications were.

The major findings related to security are summarized below:

- *Audits and Alerts*. IM/T had not concisely defined what constitutes a "significant event" based on what they encounter in their review of system and network logs. The staff manually reviewed the logs from the Agency's over 20 servers on a weekly basis. Without auditing tools, this process is very error prone given the complexity of their operation. Workstations were also not routinely monitored or audited. Automated monitoring and alerting was essentially non-existent. The Agency basically did not have a proactive, automated capability to catch an incident in real-time.

- *Contingency and disaster recovery planning.* The Agency had developed a contingency and disaster recovery plan for the last JCAHO inspection over two years ago, but the document had not been updated commensurate with changes in their information systems and network. The plan also did not address any needed coordination between the IM/T, facilities, and other departments regarding availability to information, systems, communications, power, air conditioning, and key personnel in the case of an emergency.

- *Enterprise wide backup strategy.* The Agency performed daily, weekly, and monthly backups for their critical application servers, although the process was not centrally managed. They had a tape rotation schedule that provided for offsite storage and update of the backup tapes. Their backup strategy did not extend to user workstations where critical information may be resident, especially if service is abruptly suspended. They had not regularly tested whether their backups can be restored so there was low confidence in the overall process.

- *Facility and physical considerations for critical information systems.* The Agency had deployed many of their critical systems (e.g., records management, fund development, and human resources) with limited attention to availability, business continuity, or security concerns. Major application servers are located at headquarters. Configurations included RAID-5 disk systems, power protection, and hot swappable power supplies. They did not include fail-over modes or redundant systems at other Agency locations for availability, backup, or performance considerations, even as the Agency is moving towards operating their information systems on a 24 by 7 basis. The server room at headquarters lacked the sophistication needed for a growing organization. Cable management was missing. Servers were not rack mounted or even on shelves. The phone switch and patch panels were exposed to the non-IT vendors and vice versa. Due to lack of proper cooling capacity, the door was often left open and the room occasionally left unattended so that casual access by employees was possible.

- *Electronic Medical Record Security Management Capabilities.* The EMR system lacked robust security auditing or management capabilities. When the system was demonstrated to me, it was readily apparent that the capability of the system to set security settings for a user far exceeded its ability to audit these settings. An administrator could easily create highly customized group or user profiles from modifying a standard one. Yet there was no functionality that allowed them to collectively view the permissions they had set without retracing their original steps, a very cumbersome and error prone process. As a beta customer of the EMR vendor, the Agency needs to leverage their position and work directly with the system developers to understand and remedy the auditing issues for HIPAA security as well as improved system management and administration.

- *Infrastructure Management.* The Agency had various “ad-hoc” procedures and processes for managing their infrastructure and systems. They had not formalized them into an overall strategy for system and network configuration management that includes security as a key component. Procedures to evaluate and test infrastructure changes to the Agency’s electronic information security baseline were non-existent.

- *Media Control.* The Agency lacked any centralized control over the movement of their electronic system assets. They used hand receipts, charged back to an employee's department, to track the movement of hardware, software, and media. The Agency does follow rigorous procedures for the disposal of media, ensuring that hard disks are permanently cleansed of all information before they are released from the Agency.

- *Organization.* The Agency has committed to overall HIPAA compliance as documented in their Strategic and Operational Plans. They had developed an organizational structure for privacy. They had not appointed a Chief Security Officer (CSO), defined the CSO duties, and established one or more security support teams.

- *Policies and Procedures.* The Agency had implemented numerous security procedures, such as strong passwords, use of password-protected screensavers, and automated logouts after a specified time. However, their documentation did not match what they had implemented. Additionally, workforce members within various departments had created local procedures that potentially conflicted with an Agency policy. Formal documentation of policies and procedures for handling either electronic or paper-based health information did not exist within the Agency nor did an overall formal management review and approval process for policies, guidance, or procedures.

- *Security Training and Awareness.* The Agency workforce receives basic privacy and security training as part of the new employee orientation and during the actual probation period when "on-the-job" training is conducted. The Agency has not developed any formal guidelines or requirements for on-going security awareness. The extent to which the Agency requires security training and awareness of contractors and vendors was not clear. Workforce skills relative to information technology were not routinely evaluated to ensure that individuals understood and could comply with the technical aspects of electronic information security.

Recommendations after Reviewing the Rules

Based on the review of the rules, the following recommendations are put forward for the agency:

1) The establishment of a formal *security management process* is essential to the compliance with section 164.308. For this, a security management program should be established, documented by a formal plan. The program would “involve the creation, administration, and oversight of policies to address the full range of security issues and to ensure the prevention, detection, containment, and correction of security violations. This [program] would include implementation features consisting of a risk analysis, risk management, and sanction and security policies” (Federal Register, vol. 68, no. 34, 8346).

2) The *risk analysis and risk management processes* required by section 164.308 are critical to defining the measures against which the Agency’s implementation of HIPAA security would be assessed. Additionally, other sections of the rule reemphasize the criticality of a strong, well-documented risk analysis. Therefore, the development of demonstrable risk analysis and management processes was flagged as a priority for the Agency.

3) Because of their use of electronic PHI, *establishing “reasonable and appropriate” privacy safeguards* also meant that the Agency needed to implement the appropriate security safeguards. Otherwise, they could face simultaneous violations of both rules. For example, disclosure of electronic PHI to an unauthorized party, such as two users sharing

their account username and password to the EMR, would be in direct violation of both the HIPAA Security and Privacy Rules. The Agency needed to develop a security requirements database to demonstrate their determination of what is “reasonable and appropriate”.

4) The Security Rule is *documentation* intensive. According to the Government, “the standards do not allow organizations to make their own rules, only their own technology choices” (Federal Register, vol. 68, no. 34, 8343). The Agency must demonstrate how they comply with all the requirements of this rule, including justification for their implementation decisions and how effective their decisions are. The documentation requirements for security parallel those for privacy. The Agency privacy and security teams need to work together to develop a document management process that supports both rules.

5) The Agency needs to develop sanctions for *non-compliance with privacy,* coordinating with those under development by HHS. I have seen several references in the media that the final Security Rule will very likely be used as guidance in cases where privacy violations involving electronic PHI have occurred. I also anticipate that review of any Agency privacy incident or violation will include an in-depth review and assessment of the Agency’s security risk analysis, implementation documents, including their analysis of “reasonable and appropriate”, and other artifacts such as audits, incident reports, and corrective actions. The Agency needs to establish a *quality framework for security* based on objective metrics and indicators. They need to collect the data and demonstrate how this data measures the quality of the security management program.

6) The Agency has outsourced several critical IT services, including the VPN design, implementation, and management, hardware maintenance, and telephone switch support. These vendors are either

directly involved in the transmission of PHI or indirectly in its handling. Existing contracts or service level agreements (SLA) may be sufficient but need to be reviewed against the requirements of section 164.308 and §164.314 to ensure that the proper *contractual terms and conditions for business associates* are contained in those documents.

Emerging Technologies

Emerging technologies can make integration among information systems feasible and financially viable. As the trend for integrated care systems continues to evolve, these technologies might contribute significantly to this effort by offering a multitude of options for acquiring, maintaining and connecting systems. A brief discussion of some of these technologies as follows:

Application Service Providers (ASP)

The use of ASPs reduce the initial expense and time associated with implementing new systems by allowing organizations to "rent" the systems, which are housed and maintained by an ASP. Organizations connect to the ASP through their Internet service provider. Consequently, organizations can access the software and obtain the benefits without having to set up and maintain a computer operation at their own location.

ASPs also provide the possibility of connecting providers, payers, and government entities quickly, resulting in lower administrative costs.

XML (Extensible Markup Language)

XML is a computer programming language that allows data to be exchanged among many different systems with relative ease by being a translator that sits between the user and the systems. This technology facilitates data interchange, a core issue with current health care information systems, as integrated health care networks are frequently made up of many different organizations that use their own information systems. With XML it is not necessary for the parties to use the same hardware platform, operating systems, business applications, or database management system.

Supply Chain Management

This technology uses the Internet to reinvent procurement systems and reduce cost through virtual medical superstores. If a hospital is using a sophisticated inventory system or enterprise resource planning (ERP) program that can predict material needs based on historical patterns, an electronic procurement system can automatically reorder supplies without requiring staff time to transmit the paperwork, which reduces administrative costs.

Wireless Networking

This technology allows greater amounts of data to be transmitted faster and without the need to have direct connection with a physical workstation (PC) at a desk. Since many clinicians who work in health care organizations perform many duties away from their workstations or work areas, this new technology dramatically changes how information systems can be used.

Convergence

Convergence creates a network that can handle all of an organization’s data, video and voice applications. Users can communicate with remote parties as if they were in the same room. This blending of technologies promises more available bandwidth, simplified network installation and maintenance, faster image transmission and retrieval, better image quality, and unites data, video and voice in one communication network. The key to voice, video and data convergence is significant levels of bandwidth. This means that convergence must be built on a robust networking infrastructure, which is an expensive proposition.

Telemedicine

Telemedicine is the delivery of health care services across distances, as patient data and clinical information are sent between providers allowing the patient to remain in one place. Telemedicine applications typically use telecommunications technology for clinical diagnosis, direct care delivery, patient education and the movement of medical information electronically. This technology can have a dramatic effect on the way health care services are delivered because all providers along the continuum of care can use it. As the use of high-speed telecommunications technology becomes more readily available, this may become a critical tool for rural areas. These emerging technologies, like all the change factors listed above, promote hospital goals of reduced costs, better outcomes, integrated care systems, and operational efficiencies. They also pose significant challenges to hospitals.

Conclusions and Findings

Security involves a myriad of processes overlaid on an entity's existing organizational and technical infrastructure. The impact of this entire process was to integrate security practices into the Agency in an orderly and consistent manner. The major challenge was to define and then establish the business processes related to security. These processes required activities that were not necessarily directly security related, such as improvements related to network and systems management activities.

The benefit of automation and connectivity in an information-intensive industry such as health care is tempered by the risk that confidentiality of personal health care information can be more easily breached. The privacy rule proposed by the federal government attempts to address this concern.

There is general agreement on the goals and long-term benefits of the HIPAA regulations, particularly regarding standardization of formats, code sets, and identifiers for health care transactions, which are expected to simplify administration and reduce costs over time. Compliance with the regulations may ultimately provide the synergy needed for the health care industry to achieve the level of automation other information-intensive industries have achieved. However, short-term costs of implementation of standard formats are a concern for providers and, although some controversy and uncertainty surrounds the privacy rule, all parties agree that implementation of privacy provisions will be costly. The impact of HIPAA implementation is expected to vary by state and organization.

References

1. Healthcare Information and Management Systems Society, *Guide to Effective Healthcare Information and Management Systems and the Role of the Chief Information Officer*, 3rd Edition, 1998.

2. Carter, Joyce,Gray,Patrick. *Healthcare Information Technology*. http://cci.bus.utexas.edu/research/healthcare.htm,May, 1999.

3. Hawkes, Frederick. *Understanding HIPAA Security Implication of a wireless LAN Subsystem*. June, 2004.

4. Filkins, Barbara. *The impacts of Privacy and Security under HIPAA*. July 10, 2003.

5. Kinnealeta, Tony. *HIPAA: Paradise Lost*. Protiviti, April, 2006

6. Ralph, Chris. *Risk Analysis for HIPAA Compliancy*. January, 2005

7. Burrows, Dave. *GIAC Security Essentials Certification*. December, 2004

8. Journal of Healthcare Information Management. *Emerging Technologies as a Basis for Healthcare Innovation.* Volume 14, Number 2, Summer 2000.