

HIPAA In Health Care:
Information Security in a Health Care Environment

Daniel G. James

Table of Contents

Abstract.....3

Introduction

 What is HIPAA?.....4

 How Does It Protect Patient Data In The Health Care Industry?.....5

 What Are The Penalties For Non-Compliance?.....7

 How Will It Affect The Health Care Industry?.....7

Security Considerations

 Network Security Concerns In A HIPAA Regulated Environment.....8

 E-Mail Security Concerns In A HIPAA Regulated Environment.....10

 Personnel Security Concerns In A HIPAA Regulated Environment.....12

Conclusion13

Works Cited.....15

Abstract

Since the enactment of the Health Insurance Portability and Accountability Act in 1996, it has been the goal of health care facilities across the nation to comply with these new regulations. There are many reasons for the HIPAA regulations, but the most important is to ensure the privacy of patient data in health care and insurance facilities. If a health care facility fails to comply with these regulations, it could possibly result in millions of dollars in fines and restitutions. It is also possible for the person or persons responsible to serve time in prison. It is very important for anyone working with sensitive data to follow the most strict security policy available. Finding new ways and technology to protect the sensitive data has been a daunting task for health care facilities. The government did not assign any products or processes to comply with HIPAA. It is the responsibility of each organization to discover new products and processes to protect their data! There are several aspects to take into consideration when analyzing a potential data security problem. The first aspect to consider is network security. If hackers can penetrate the network, patient data is definitely at risk. The second aspect is Email security. This can be easily covered if the proper policies and education of employees are implemented. The third aspect is personnel. The workers at a health care facility can definitely be a security breach. In order to prevent this, they should be trained on the new regulations and company policies.

What is HIPAA?

Since the enactment of the Health Insurance Portability and Accountability Act (HIPAA) in 1996, it has been the goal of health care facilities across the nation to comply with these new regulations. Until now, most, if not all, of this impact have come from the portability provision, which has significantly changed the way insurers treat preexisting conditions for new enrollees. Prior to the enactment of HIPAA, changing health plans could be a financially devastating event for individuals with ongoing medical conditions. Since the enactment of HIPAA, individuals are now free to change employers, and health plans without risk of coverage limitations because of preexisting conditions (Balezantis & Halterman, 2002).

Although portability was a major breakthrough in providing access to health care coverage, there is actually much more to HIPAA. According to Balezantis & Halterman (2002), the legislation was a compilation of many separate issues that had been on the legislative agenda for several years. The final version of HIPAA as it was enacted, accomplished the following: 1.) Authorized the pilot program for medical savings accounts (MSAs), 2.) Created a Medicare fraud control program, 3.) Established parity for mental health benefits, 4.) Revised the tax deductibility of corporate owned life insurance (COLI), 5.) Created favorable tax provisions for long-term care insurance, 6.) Established favorable tax treatment for accelerated death benefits, 7.) Allowed for greater access to and portability of health care coverage, 8.) Provided for administrative simplification in health care data interchange (Balezantis & Halterman, 2002).

How Does It Protect Patient Data In The HealthCare Industry?

Although many of HIPAA's rules became effective in 1996 and 1997, several have yet to take effect (Whiting, 2002). One of the more emotionally charged rules contained within the legislation is the so-called privacy rule. The privacy rule was set forth through the administrative simplification provision of the act, which encompasses the following: 1.) Electronic health care transactions (final rule issued), 2.) Medical privacy (final rule issued), 3.) Security requirements (final rule issued), 4.) Unique identifier for employers (final rule issued), 5.) Unique identifier for providers (final rule issued), 6.) Unique identifier for health plans (final rule issued), 7.) Enforcement procedures (final rule issued) (Balezentis & Halterman, 2002).

The privacy rule is intended to protect the confidentiality of an individual's health information (Whiting, 2002). It requires organizations that collect or access health information in order to provide care, or process information about that care to implement and enforce specific safeguards and consent procedures. Not only is the information protected, but individuals must be given access to their information in order to validate its accuracy. Hospitals and medical practices will be required to provide information to patients about their privacy rights, adopt clear privacy procedures, train employees so they understand the procedures, designate a privacy official, and secure patient records so they cannot be accessed by those who do not need the information (Balezentis & Halterman, 2002).

The privacy rule gives flexibility to providers, as the rules are scalable to the size of the organization. In a large hospital, the privacy officer may be a full-time dedicated position; perhaps even with a staff that reports to the privacy officer, while the small

physician practice may simply designate the office manager or receptionist to handle the privacy officer responsibilities (Gue, 2002). Additionally, the policies and procedures of small practices may be more limited under the rule than those of a large hospital. This will be based upon the actual volume of health information transactions (Balezentis & Halterman, 2002).

In general, health care providers who see patients will be required to obtain consent before sharing information for treatment, payment and health care operations (Gue, 2002). Additionally, separate patient authorization must be obtained for non-routine disclosures and most non-health care purposes. Patients will have the right to restrict the use of these disclosures (Balezentis & Halterman, 2002).

As the privacy rule is meant to help patients and not limit their access to quality health care, there are circumstances in which consent does not have to be obtained, such as emergency situations. In the case of an emergency, the provider does not have to obtain consent until the situation allows for reasonable communication with the patient. This is meant to give providers discretion so that care is not delayed (Lageman & Melick, 2001). Within the U.S. Department of Health and Human Services (HHS) guidance, there are several confusing issues that have been clarified in order to ease the perceived burden placed on providers. One section makes it clear that hospitals do not have to take such steps as building soundproof rooms so that conversations about protected health information (PHI) are not overheard. Rather, the guidance states that reasonable safeguards need to be provided, such as curtains, screens and similar barriers (Balezentis & Halterman, 2002).

What Are The Penalties For Non-Compliance?

An important aspect of the privacy rule is that significant penalties have been established for misuse of personal health information. Not only are there civil penalties, but Congress also has established steep criminal penalties for those who knowingly violate patient privacy. The penalties range from one year in prison and \$50,000 for obtaining or disclosing protected health information to up to ten years in prison and \$250,000 for obtaining or disclosing such information with the intent to sell it or use it for personal or commercial advantage or malicious harm. As patient privacy has become a serious issue in this age of electronic information processing, the government has made it clear that violators will be prosecuted to the full extent of the law (Balezentis & Halterman, 2002 Gue, 2002, Ask the Expert).

How Will It Affect the HealthCare Industry?

HIPAA may have an overall negative financial impact on health care providers across the board because of the significant amount of capital expenditures that could be required to ensure compliance. Exacerbating this issue are existing negative pressures facing hospitals and other health care systems nationwide. Thus, at one of the most inopportune times, health care providers will have to review, evaluate, and implement various capital projects-an undertaking that will dip further into their already-limited pools of resources. Compliance with the HIPAA regulations may necessitate a complete overhaul of many organizations' technological, process, and security systems (Lageman & Melick, 2001). This will require evaluations of all current systems and the development of plans for compliance (Hagland, 1998). An additional burden will be the periodic monitoring demanded of health care organizations to maintain compliance with the regulations. The severity of the financial and operational impact will be directly

related to the level of disparity between that organization's current information technology (IT), security, and communications systems and those required by HIPAA (Lageman & Melick, 2001).

Network Security Concerns In A HIPAA Regulated Environment

Whenever a health care system posts a Web site, it takes advantage of a new marketing tool that gives consumers a window on the organization. But a Web page also builds a door into the organization's internal network, a door that can be opened by clever outsiders (Cupito, 1997). If your Web site runs from one computer, unconnected to others in your network, then your internal network is probably safe from outside snooping -- unless some hacker fiddles with your website as a prank, says Sandra Fuller, director of professional practice at the American Health information Management Association (AHIMA), an association of more than 37,000 medical record and information management professionals in Chicago (Cupito, 1997, Yasin, 2001).

"Somebody could pretend to be your Web site and put out false information about you ... They like doing that with the Department of Defense," says Cupito, 1997. "There are people who sit in their basements and do these things. I'd like to string them up by their toes." (Cupito, 1997). However, rarely are health organization's Web sites run from isolated computers. Many are hosted by machines connected to internal networks, and thus can put the internal network at risk of attack (Cupito, 1997, Yasin 2001).

Internet attacks are most likely to be of three varieties, notes Dale Miller, director of consulting services at Irongate Inc., a security-consulting firm in San Rafael, Calif.: 1.) Unauthorized access to the internal networks, 2.) Unauthorized disclosure of confidential

patient information, 3.) The introduction of computer viruses into the organization's network (Cupito, 1997). Security programs include firewalls, authentication techniques that prove the identity of the person requesting access, uniform methods to authorize and control access, aggressive software management, and regular monitoring to check for vulnerability (Groth, 1997).

Firewalls are built from hardware, software, and network equipment to permit some access from the outside world and deny other traffic. They range from the simple to the complex, and act as automated security guards or censors, scanning traffic from and to the Internet, and permitting only that which meets specified criteria (Groth, 2001). No matter how complex a firewall is installed, says Fuller, "The most important thing about developing it is knowing you're never done. People, in their spare time, find ways to get through them. You want to be certain you're keeping the firewall up to date. You want it to be able to identify an intrusion as quickly as possible." (Craig, 2001)

Besides the cost of installing the technology, network administrators also must spend time monitoring traffic through the firewall, and checking access logs to guard against attack or leaks. But setting up hardware and software to protect information does little good if employees use their own Internet accounts at work from network computers. Doing this sidesteps firewall protections and can put the organization at risk (Groth, 2001, Craig, 2001).

File transfer protocol, or FTP, can be dangerous as well. Employees, for example, could use FTP to download software that violates copyright provisions or infects the organization's network with viruses, Miller notes (Craig, 2001). Virus-scrubbing software

should be installed and updated regularly, since viruses can slip by firewalls undetected (Groth, 2001).

E-Mail Security Concerns In A HIPAA Regulated Environment

Consumers, who are becoming Internet-savvy, will expect to glean more health information using that technology, says Gail Gulinson, vice president for health network marketing, IBM Global Health Care Industry. They may be satisfied to learn generic health information from a hospital's Web site, she says, but they will also want to communicate directly with their health provider about specifics (Craig, 2001). "Our research is showing that people will ask questions across the Internet of a physician they'd never ask in person," she says. People's comfort level with e-mail, however, is one of its most dangerous aspects, experts note. While many people think e-mail is like a letter mailed in an envelope, it is more like a postcard, says Harry Rhodes, professional practice manager at AHIMA (Cupito, 1997).

Internet e-mail can be read and stored at many places en route to its destination. Once it arrives, there's no telling what happens to it. Many people's e-mail accounts are provided by their employers, who may read it and save it on backup systems, which is a possible security breach (Craig, 2001). "Once it gets to the patient's PC, it's easy to forward, to send out as a broadcast, to delete," Rhodes says. To provide a measure of protection for themselves, some doctors are asking patients to sign agreements that note unencrypted e-mail is not private and asking them to take some responsibility for keeping it to themselves. Rhodes suggests that sensitive e-mail, such as results of an HIV test, be kept to a simple, "Your test results are in. Please call us." (Cupito, 1997).

Encryption systems, which scramble the message so that only the holder of a secret key can decode them, can also help solve this problem. "But not all e-mail systems make it easy to encrypt the information at this point," says Miller of Irongate. And before a health organization makes a policy stating all patient-identifiable e-mail be encrypted, as suggested by the NRC committee and other experts, it should consider whether unencrypted e-mail may be more secure than sending such information by fax, which may lie around for all to see, Miller says (Cupito, 1997, Groth, 2001).

Ultimately, before people do a lot on the Internet, they'll have to have strong authentication programs. These systems verify a user is in fact who he says he is. While most authentication systems rely on passwords, these alone may offer little guarantee of security. People sometimes write passwords near their computers, tell them to others, or use short passwords that are easily guessed. To increase security, passwords should be changed frequently (Groth, 2001). They should be made up of at least seven letters and numbers, because hackers can use programs that guess virtually all possible English words. Strong authentication combines something someone knows, such as a password, plus something he has, such as a card with a magnetic strip. Stronger still are systems that use biological characteristics, such as fingerprints or retinal scans, to verify a person's identity. Of course, to use such a system, another device would have to be used at the workstation or home PC, which adds to the inconvenience, the maintenance and the cost, he says (Cupito, 1997,).

Health security experts agree technology can play only a part in protecting an organization's sensitive information from unauthorized use or attack. The other part must be a clear security policy that's understood and followed by all employees (Cupito, 1997). The NRC committee, which visited six health care sites, noted that a few with connections to the Internet detected some inconsequential snooping at their points of entry, but did not consider intrusion by outsiders a significant problem. The Internet is not the culprit. It's easier to go bribe somebody than to break into a server. Experts estimate that only about \$250 will do the trick (Cupito, 1997, Hagland, 1998).

As noted in a white paper by 3Com Corp.'s, 1998 Chuck Semeria, "Setting up an Internet firewall without a comprehensive security policy is like placing a steel door on a tent." People may be stopped at the door, he says, but can easily sneak in around the sides. "We think you should develop a policy before you throw the switch. What we suspect is happening is the opposite: People are buying systems and run into problems and then writing the policy," says AHIMA's Rhodes. "That's not a wise way of going about it." (Cupito, 1997, Hagland, 1998, Groth, 2001).

Security policies should delineate who is permitted access to which information and should spell out sanctions for violating the policies, the NRC committee noted. "You have to have a really clear statement that you take the privacy of patient and your business information really seriously, not just the first week they're hired, but on regular basis," adds AHIMA's Fuller. Employees should be asked to read and sign written agreements, noting that, "Not only do I know we have a policy, I have heard, understand and agree to live by it." Policies should also stipulate who may post information in the

company's name on the Internet and specify penalties for violating this policy, Fuller says. Employees who subscribe to Internet mailing lists to discuss business may unwittingly divulge proprietary information, unless they're trained about what is confidential and what is not, Miller says. "The organization needs to communicate with employees whether or not it's OK to post things like internal procedures." (Cupito, 1997).

Conclusion

While HIPAA may not seem to be an immediate threat to the financial stability of many health care systems, the eventual impact of these regulations will be significant. Unlike preparations for Y2K, HIPAA will require ongoing, detailed analysis of existing systems and development of future plans for compliance. Even after systems become compliant, organizations will need to monitor their systems to remain in compliance (Lageman & Melick, 2001).

There is no doubt that HIPAA will benefit the health care industry. By streamlining the information dissemination process, the industry should see significant administrative cost savings. Predictions of up to \$30 billion have been recorded. In addition, improving the accuracy of information should enable health plans to enhance their ability to monitor quality of care. However, despite these optimistic predictions, significant cost savings will be seen only once all the standards have been implemented. Each component must be in place for the system to work efficiently. Unfortunately, the most difficult part of the process will not likely be the technological changes. Those changes requiring procedural, cultural, and behavioral modifications will be the most challenging to health care providers (Lageman & Melick, 2001, Gue, 2002). Health care

organizations that begin preparing for HIPAA regulations now will be in a better financial and organizational position to comply with the rules as they are finalized. Those that wait until the final rules are announced will have significant time constraints for compliance (Lageman & Melick, 2001, Gue, 2002).

Works Cited

- Ask the Expert*. (2002, April 29). CIO. Retrieved November 17, 2002 from the World Wide Web: <http://www2.cio.com/ask/expert/2002/question/question861.html>
- Balezentis, M. , & Halterman, S. . (2002). HIPAA's privacy rule: What is it, and how does it affect you?. *Benefits Quarterly*, 18 (1), 53-59.
- Cupito, M. C. . (1997, September). Creating Web windows may leave doors to data unsecured. *Health Management Technology*, v18, 24.
- Groth, D. . (2001). Network+ Study Guide (3rd ed.). California: Sybex.
- Gue, D. . (2002, October). Determining what is HIPAA Affordable: A professional costing approach to HIPAA implementation. *Health Management Technology*, v23, 16.
- Hagland, M. . (1998, May). The gap: HIPAA and secure IT. *Health Management Technology*, v19, 24.
- Lageman, R. C., & Melick, J. R. (2001). HIPAA: Wake-up call for health care providers. *Journal of Health Care Finance*, 27 (4), 1-6.
- Whiting, R. (2002, June). Health-Care Providers Race To Meet Privacy Deadline. *InformationWeek*, 68.
- Yasin, R. (2001, February). Tools Stunt DoS Attacks. *InternetWeek*.