https://doi.org/10.48009/2_iis_2009_237-241

PRIVACY UNDER HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) OF 1996: THE IMPACT OF RFID

William Roach, Washburn University, william.roach@washburn.edu
Gene Wunder, Washburn University, gene.wunder@washburn.edu

ABSTRACT

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) includes the Privacy Rule. The Privacy Rule creates a national standard for the protection of Protected Health Information (PHI). Radio Frequency Identification (RFID) chips have expanded the size and scope of files that contain PHI. Because the size and scope of the databases containing PHI is so much larger, policing the Privacy Rule needs to be automated.

Keywords: HIPAA, Privacy Rule, RFID, HL7

INTRODUCTION

HIPAA privacy rules apply to all healthcare providers (who transmit healthcare information in electronic form), health plans, healthcare (information) clearinghouses, and business associates. Healthcare providers had been developing security protocols for a long time before the passage of HIPAA. N The Health Level 7 (HL7) was founded in 1987 to develop standards for the transmission of administrative, clinical and financial information (IWay Software, 2009).

Applying the Privacy Provisions of HIPAA

The process of determining whether a given entity is subject to the privacy provisions of HIPAA is complex enough to require a flowchart. (HHS, 2006) The Privacy Rule protects all "individually identifiable health information" held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. The Privacy Rule calls this information "protected health information *(PHI)*." (OCR , 2007) .

Protected Health Information

Examples of Protected Health Information (PHI)	
■ Name ■ Address ■ DOB ■ SS# ■ Email ■ Employer ■ Fax/Phone # ■ Internet address/Web URL	■ Med Record # ■ Account # ■ Photos ■ Certificate/license # ■ Finger or voice prints ■ Any "other" identifying number, characteristic or code

The privacy regulation lists about two dozen categories of information identifiers which must be removed from any information that is disclosed. If it is possible to use several information identifiers from several categories to deduce information about an individual, then disclosure of those categorical statistics is prohibited. The privacy rule permits use of "individually identifiable health information" for 12 national priority purposes.

12 National Priority Purposes	
■ Required by Law ■ Public Health ■ Victims of Abuse, Neglect or Domestic Violence ■ Health Oversight Activities ■ Judicial and Administrative Proceedings	■ Law Enforcement Activities ■ Organ, Eye or Tissue Donation ■ Decedents ■ Research ■ Serious Threat to Health or Safety ■ Essential Government Functions ■ Workers Compensation

The covered entities must

- Secure patient records
- Establish sanctions for employees that violate HIPAA regulations
- Take reasonable steps to limit use/disclosure of PHI
- Adopt policy and privacy procedures
- Train employees about HIPAA
- Designate a Privacy Officer
- Obtain signed authorization from a patient for use of PHI

Covered Entities are obliged to provide notice to patients of the privacy practices at the patient's first visit.

> "A covered entity must maintain reasonable and appropriate administrative, technical, and physical safeguards to prevent intentional or unintentional use or disclosure of protected health information in violation of the Privacy Rule and to limit its incidental use and disclosure pursuant to otherwise permitted or required use or disclosure." (HIPAA Glossary , 2008)

At this point, the use of RFID technology starts to have implications for the HIPAA Privacy Rule. As a result of using RFID technology, the covered entity will have:

- More protected information in machine-readable form
- Higher quality data

The more sophisticated information system that goes with RFID may create a higher standard of conduct for the protection of patient privacy. A breach of privacy with a large, sophisticated information system is likely to involve many records and many patients. However, the volume of data and the complexity of the data structure make it less likely that PHI will be compromised unless the breach involves the use of the software that goes with the data.

The HIPAA Privacy Rule provides for both fines and prison sentences. Not complying with a specific rule can result in a $100 fine per incident subject to an annual maximum of $25,000. The fine may be waived if the violation was not intentional. An intentional disclosure can result in a $50,000 fine and / or a one year prison sentence. If the offense was committed under false pretenses, the fine goes up to $100,000 and the prison sentence up to five years. If the offense was committed for financial advantage, the fine escalates to $250,000 and the prison sentence to ten years.

HIPAA Privacy Rule
Non-Compliance Criminal Sanctions

HIPAA imposes the following criminal sanctions for each act of non-compliance with the Standards for Privacy of Individually Identifiable Health Information, "The Privacy Rule." (*HME Today*, 2002)

Violation Type	Monetary Penalty	Imprisonment
Knowing	$50,000	Up to 1 year
False Pretenses	$100,000	Up to 5 years
Commercial advantage, personal gain, or malicious harm	$250,000	Up to 10 years

Judgments on medical center fraud might give some sense of potential liability verdicts in this area.

BEST PRACTICES (OCR, 2007)

The HIPAA Privacy Rule requires a covered entity to make "reasonable efforts" to protect patient privacy and to follow "best practices." In the context of the HIPAA Privacy Rule and RFID, what might those best practices be?

HIPAA focuses on best practices of IT security; key requirements in the Security Rule include:

- Account management: granting or removing user access to systems with PHI
- Administrative procedures: polices to cover activities of IT staff and users
- Backup and disaster recovery: protecting data in event of a disaster
- Media reuse and destruction: handling and destroying media with PHI
- Emergency access: accessing PHI in the event of a medical emergency
- Physical security: controlling physical access to computers and networks
- Use of email: specifying how PHI must be handled in email
- System security: implementing best practices in desktop, server, and network security
- Workforce training: training of users in good computing practices (Gatzert, 2005)

The HIPAA privacy requirements are not unusual. Publicly owned corporations must meet similar requirements under the provisions of Sarbanes Oxley (45 CFR 2002) ISO 17799 / BS 7799, HL7 (healthcare data), SWIFT (financial and banking data) also offer guidance in this area. The Gramm-Leach-Bliley Act of 1999 covers employee training requirements for financial firms (including health care providers) who hand confidential information. Canada imposes similar obligations under the Personal Information and Electronic Documents Act (PIPEDA) (INFOSYSSEC, 2000).

Privacy and Security Standards

Standard	*Date*	*Covers*
HL7 Health Level 7	*1987*	*WEB Protocol for healthcare data*
HIPAA	*2002*	*Personal Health Information (PHI)*
ISO 17799	*2005*	*Generic*
Sarbanes -Oxley	*2002*	*Generic*
COBOT 4.1	*2009*	*Generic*
PCI DSS	*2008*	*Payment Card Industry*
SWIFT	*2005*	*Bank and Financial Transfers*

In short, there are many places for healthcare providers to go for guidance for compliance with the HIPAA Privacy Rule. RFID does not change the nature of the obligations imposed by the Privacy Rule, but RFID does raise the stakes. RFID will result in the collection of much more and much higher quality information. While the obligations have not changed, the liability exposure will be greater.

HIPAA COMPLIANCE SOFTWARE

The size of healthcare information systems requires that Privacy Rule compliance be automated. There needs to be a comprehensive information security program which includes:

- Administrative Procedures
    - Policies
    - Procedures
    - Education of workforce
- Physical Safeguards
- Technical controls
- Information Security Officer (Borton, 2001)

Healthcare providers need not reinvent the wheel. Policies appropriate for a particular kind of entity are available from a wide variety of sources. Automated training with employee certification is also available. Physical safeguards and technical controls are similar to those for other large databases like ERP systems.

The required administrative procedures include:

- Certification
- Chain of trust partner agreement
- Contingency plan
- Record processing controls
- Access controls
- Auditing
- Personnel security
- Configuration management
- Security incident procedures
- Termination process
- Training

Certification refers to documenting that employees have appropriate knowledge of privacy and security practices required under HIPAA. "Chain of trust" is a term used in the information security field to refer to contractual agreements which document the security practices employed by both parties and the conditions under which it is appropriate to assume that data transmissions have occurred and been received. Contingency plans relate to "acts of God" rather than security incidents. Record processing controls include control totals, hash totals, conservation of records, etc. Access controls should be very specific to the information involved; particular individuals should have access to the information they need to do their jobs and only for the time frame in which they are doing that job. Records should be kept of who accesses what data and those records should be audited regularly. Background checks should be performed on personnel who will have access to PHI. Configuration management is the process for controlling what equipment and software is installed. Security incidents should be reported, and the responses to those incidents documented. Personnel who violate privacy and security rules should be terminated.

Physical safeguards for PHI include:

- Media controls
- Physical access controls
- Workstation use policy guidelines
- Secure workstation location position
- Security awareness training

Media controls are policies that govern the receipt and removal of media that contain PHI. On a personal level, when one submits the hard drive on a discarded computer for shredding, one is following a media control policy. Physical access controls limit physical access to computers and files containing PHI and also provide for recovery of data. Workstations that can access PHI must be monitored and their use governed by appropriate rules. A secure workstation location is one in which it is not possible for unauthorized viewers to see the information on the computer screen.

Technical controls include:

- Access controls
- Audit controls
- Authorization controls
- Data "authentication" (integrity)
- Entity authentication
- Event reporting alarms

Access controls means limiting physical access to computers and workstations which contain/ display PHI. Audit controls require that entities conduct audits to verify that the various control procedures are working. PHI are only released with appropriate authorization. Data authentication procedures assure that PHI have not been altered or deleted in an unauthorized manner. The identity of entities accessing PHI must be verified with appropriate techniques. Adverse events in healthcare must be reported to appropriate authorities.

CONCLUSIONS

1. RFID raises the stakes for HIPAA Privacy Rule compliance; medical data bases include more PHI and higher quality PHI. The complexity of the data base context makes casual disclosure less likely.
2. The HIPAA Privacy Rule is not unlike many of the privacy rules that various corporations are held to. There are many models for healthcare providers to imitate.
3. Many vendors provide appropriate systems and training. Some systems are very specific to the kind of healthcare provider.
4. If a breach of privacy occurs, it will be very important for the healthcare provider to have a track record of vigorous efforts to protect PHI. Such a record makes it more likely that the breach will be seen as unintentional.

REFERENCES

1. Borton, Kate (2003) "Healthcare and the New Federal Security Protections" Microsoft PowerPoint Presentation retrieved from http://www.blackhat.com/presentations/win-usa-01/Borten/bh-win-01-borten.ppt at 10:30 a.m. on 21 October 2008
2. Davenport, Chris (November 2007) "The Quest to Achieve Best Practices in Healthcare Information Security" *Healthcare and Life Science Solutions Case Study IBM*
3. Gatzert, Bene and Phil Chuang (Fall, 2005) " HIPAA Security" *INews: IT Policy* Retrieved from http://inews.berkeley.edu/bcc/Fall2005/hipaasecurity.html at 2:30 p.m. on 9 October 2008
4. "HIPAA Glossary" Retrieved from http://www.hippa.com/cgi-bin/viewglossary.cgi?ALETTER=A at 12:50 p.m. on 18 October 2008
5. IWay Software, "IWay Intellgent Adapter for HL7" (2009) Retrieved on 28 March 2009 from http://www.iwaysoftware.com/products/adapters/hl7.html
6. INFOSYSSEC, "Security Standards, Laws, and Guidelines" (2000) Retrieved at 4:30 p.m. on 28 March 2009 from http://www.infosyssec.com/infosyssec/secstan1.htm
7. Office for Civil Rights (HHS) (2007) *Frequently Asked Questions on the HIPAA Privacy Rule* Retrieved at 3:06 p.m. on 16 September 2008 4:00 p.m. from http://privacyruleandresearch.nih.gov/faq.asp
8. Warren, Dennis (December 2002) "HIPAA's Darkside" *HME Today* Retrieved on 16 September 2008 3:30 p.m. from http://www.hmetoday.com/issues/articles/2002-12_12.asp United States Department of Health and Human Services *OCR Privacy Brief: Summary of the HIPAA Privacy Rule* (2003) Retrieved from www.hhs.gov/ocr/privacysummary.pdf *at 10:00 a.m. on 2 September 2008*
9. Stoney Brook University, School of Nursing (2003) *Training Manual For New Employees & Students Of The Health Sciences Center* retrieved on 16 September 2008 4:00 p.m. from http://www.nursing.stonybrook.edu/nursingwprod.nsf/HIPAATraining?OpenForm
10. United States Department of Health and Human Services *Covered Entity Charts* (2006) Retrieved from http://www.cms.hhs.gov/HIPAAGenInfo/Downloads/CoveredEntitycharts.pdf a t 11:00 a.m. on 2 September 2008
11. United States Department of Labor, Wirtz Labor Law Library "Sarbanes-Oxley Act of 2002: On Line Resources" Retrieved from http://www.dol.gov/oasam/library/law/lawtips/sarbanes_oxley.htm at 1:00 p.m. on 18 October 2008
12. 45 C.F.R. § 160.103 (2002)
13. 45 C.F.R. § 164.530 (c). (2002)