Medical Record Theft, HIPAA Security and HITECH

According to the United States Postal Inspection Service (USPIS), identity theft is America’s fastest growing crime. The USPIS website states, “Last year alone, more than 9.9 million Americans were victims of identity theft, a crime that cost them roughly $5 billion” ("Identity Theft"). Another article in U.S. News and World Report mentions that, “Medical identity theft currently accounts for just 3 percent of identity theft crimes, or 249,000 of the estimated 8.3 million people who had their identities lifted in 2005, according to the Federal Trade Commission” (Andrews, 2008).

What happens to the stolen information? The stolen insurance information can be used to get services or goods. Finding and cleaning up the mess is not as easy as it is with financial ID theft. When a credit card gets stolen and used, the unusual activity is quickly monitored by the credit card fraud people and presented before the card-holder who can put a hold on his card or admit that the activity was truly his own. Not so with medical ID theft. Fraudulent activity may never be reported until great damage has been done to the user’s medical record and credit report. Expensive procedures may go unnoticed until the unpaid bills pile up and the issue is made known.

Recently, hackers broke into the Medicaid and the Children's Health Insurance Program in the state of Utah and stole 182,000 electronic medical records, compromising 25,000 social security numbers. Quoting from the Huffington Post, “Utah health officials said Friday that hackers who broke into state computers last weekend stole far more medical records than originally thought, and the data likely includes Social Security numbers of children who have received public assistance. The information was stolen from a new server at the Health Department, Weiss said. Although the state has multiple layers of security on every server, a technician installed a password that wasn't as secure as needed” ("Utah Medicaid," 2012).

What is being done about medical identity record theft? State and federal government regulations are requiring health-care organizations to report if there has been a data breach where electronic medical records were compromised or stolen. According to the Health Information Technology for Economic and Clinical Health (HITECH) Act, all health-care organizations are required to communicate with individuals if 500 or less medical records were compromised. If more than 500 medical records were compromised, the media and the “Secretary of Breaches” (a high-up individual in the Department of Health and Human Services) are also to be notified ("Breach Notification Rule,"). The HITECH Act is just a part of a group of regulations that are known together as the HIPAA Security Rule and HITECH Act. The purpose of the Health Insurance Portability and Accountability Act and HITECH is to create a minimum guideline for all health-care organizations to build a foundation from and to create accountability and lines of communication between health-care organizations, the individuals they serve, and the U.S. Government.

HIPAA and HITECH together are a list of around 60 (depending on the type of health-care organization) regulations that translate into 60 policies. One of the goals of the HIPAA Security Rule is for health-care organizations to create and maintain a formal information security program. The National Institute of Standards and Technology crafted a very helpful resource that helps information security officers and project managers make sense of the HIPAA Security Rule. SP 800-66 (An Introductory Resource Guide for Implementing the HIPAA Security Rule) is seen by many as the Bible of the HIPAA Security Rule, turning vague, one sentence regulations into pages of guiding material that informs the hospital’s information security department on how to implement all the different standards. To quote from SP 800-66,

> Under the Security Rule, covered entities (health-care organizations) are required to evaluate risks and vulnerabilities in their environments and to implement security controls to address those risks and vulnerabilities. The selection and specification of security controls can be accomplished as part of an organization-wide information security program that involves the management of organizational risk - that is, the risk to information, individuals, and the organization as a whole. The management of risk is a key element in the organization's information security program and provides an effective framework for selecting the appropriate security controls for an information system - the security controls necessary to protect individuals and the operations and assets of the organization (Scholls, Stine, Bowen, Johnson, Smith & Steinberg, 2008).

The HIPAA Security Rule is split into three separate groups of safeguards:

- Administrative Safeguards

- Physical Safeguards
- Technical Safeguards

A separate part of the security rule but required now by law is the HITECH Act which concerns itself with breaches to electronic protected health information (also known as ePHI). The first group of safeguards is known as Administrative Safeguards and consists of nine standards and twenty implementation specifications. Again, quoting from the National Institute of Standards and Technology (NIST), “An implementation specification is a more detailed description of the method or approach covered entities can use to meet a particular standard. Implementation specifications are either required or addressable. However, regardless of whether a standard includes implementation specifications, covered entities must comply with each standard.” (Scholls, Stine, Bowen, Johnson, Smith & Steinberg, 2008) The Administrative Standards focus on the human perspective of information security. Some of the major issues covered and tasks accomplished are

- Identifying key members in the hospital to consist of a governing committee that will read, verify, and acknowledge all of the policies that are required by HIPAA, and will be the engines that will cause change in the way the hospital handles ePHI.
- Conducting a risk assessment and create a risk management program that applies controls to high and medium level threats to information security.
- Creating a disciplinary policy that states what appropriate sanctions will be had against non-compliant employees.
- Choosing the official HIPAA Security Officer who is responsible to ensure that the hospital stays compliant to the HIPAA regulations.
- Ensuring that ePHI is limited only to authorized users. Roles and responsibilities are formulated and a chain of command is established. Terminated employees are handled in a way that protects the health-care organization from damage due to disgruntled ex-employees.
- Implementing a role-based access control system This is a huge project that may require third-party software and consultants. Most health-care organizations end up giving access

based on a discretionary system. For example, Nurse Joe is a new employee and is replacing Nurse Ann, so he should be given the same accesses she had. The problem with this type of access granting is that Nurse Ann had worked at the hospital for twenty years and has more access than a new employee should have. Therefore, Nurse Joe is granted more access than needed – and remember that there are a lot of burned out nurses getting replaced on an annual basis, so this situation is very common.

- Instantiating a security awareness and training program. All hospital employees will be required to take an annual training course (usually delivered online), and all new employees will have it as part of orientation. The training will educate users on how to recognize threats against the hospital's information systems (suspicious e-mails, how to browse the Internet safely, how to protect passwords). The awareness part of the program (fliers, posters, and reminders on the intranet – the hospital's internal network) will help remind users of the importance of being smart and safe while using the hospital's information systems.

A very important part of the administrative safeguards covers security incident procedures. It is required that a security incident response team be identified and trained to respond to security incidents that could lead to a data breach. Procedures must be written down that go into detail on how to respond to and report security incidents. A report detailing on what was done during the security incident must be written up that can be used in the case of a legal fallout due to a data breach. Also, an after-action review is required in order to reflect upon lessons learned. This review is also useful in that it allows the information systems to better themselves by beefing up security in the previously breached area.

A substantial portion of the administrative safeguards is known as the contingency plan. There are a total of four plans/procedures:

- Business Impact Analysis (BIA) – This plan goes in one of the key first steps in developing a contingency plan. The BIA goes over each different department as an individual business unit, and it determines the criticality of that business unit in comparison to the whole organization. Thomas Mawson, executive director of Disaster Recovery Institute International has this to say regarding Business Impact Analysis: "Doing such an analysis accomplishes three important things:

    1. A BIA establishes the value of each organizational unit or resource as it relates to the function of the total enterprise.

    2. It provides the basis for identifying the critical resources and functions required to develop recovery strategies.

    3. It establishes an order or priority to restoring the critical functions of the enterprise in the event of a disaster (Mawson, 2003).

- Disaster Recovery Plan (DR plan) – The disaster recovery plan (DR plan) goes over the actual work that will take place during a disaster. A good rule of thumb in choosing a disaster scenario is the worst-case scenario (e.g. the entire data center went up in smoke). With all the details planned out under the worst case scenario, the same DR plan can be used for less disastrous situations.
- Business Continuity Plan (BCP) – This plan goes over how business will continue to operate during a disaster. The difference between a DR plan and the BCP is the DR is a detailed plan on how to recover from a disaster, while the BCP is focused on how business is to continue during a disaster.
- Testing and Revision Procedures – HIPAA requires that all these plans be tested and revised to keep up with the changing environment. This is not done as often or as thoroughly as it should be, seeing how most hospitals have a limited budget to maintain and increase information systems, much less spend extra resources to plan for hypothetical disasters. Nevertheless, these continuity plans need to be tested, and there are a few different types of tests that can be employed:
    - Tabletop exercises (dry run) – A few hours with all of the members of the disaster recovery team and many holes and discrepancies within the plans can be found.
    - Full-scale exercises –A full-blown disaster is simulated off-site using rented equipment to test and validate the actual DR activities.

Evaluation is a very crucial part of the Administrative Safeguards. It involves the information security committee going through the security program on an annual basis to see what parts of the security program need to be changed based on new technology or new procedures. This can be accomplished internally or externally using a third party performing a risk analysis on the organization. The last portion of the administrative safeguards is the Business Associate (BA) Contracts and Other Arrangements. The BA's are required to be compliant to HIPAA. The covered entity (the one hiring the BA) is not responsible for ensuring that the BA is compliant to HIPAA. According to the HIPAA Security Rule, this must be explicitly laid out in the contract agreement.

The next section of the HIPAA Security Rule is the Physical Safeguards section. The majority of the section is usually already being handled by the on-site security staff and maintenance team. In this grouping of safeguards there are four standards and eight implementation specifications. NIST defines the physical safeguards, as the "physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion" ("Code of Federal," 2011). Thus the first standard regarding physical safeguards requires an analysis of the current physical safeguards (locks on high security areas, cameras, fire extinguishers) to see what areas need to be improved. These safeguards are not enough – there must also be written procedures on how people are granted access to secure locations. Most of these procedures and documents are already in another group of policies that are managed by the on-campus police/security department.

The second and third standards cover the location, use, and security of all the workstations – tablets, desktops, smartphones, laptops. If it has a hard drive that can contain ePHI, it is considered a workstation. All workstations must be accounted for, and their location must be documented. A blueprint of each of the hospital floors with each workstation is recommended, and tracking documents/software are also a necessity. The responsible party for these safeguards usually is the help desk organization. Workstation security can be determined with the help of the onsite security/police force. High volume traffic areas like the front desk and reception areas should have their workstations physically secured to the desk or table they are mounted upon with a lock and cable.

The last standard for the physical safeguards is the Device and Media Controls standard. The standard reads, "Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information, into and out of a facility, and the movement of these items within the facility" (Scholls, Stine, Bowen, Johnson, Smith & Steinberg, 2008). This involves documenting procedures that handle how ePHI is disposed. There must be an accountability of all hardware and electronic media and a level of determination on which media can be re-used and which media needs to be disposed of. Many employees will try to take hard-drives home with them after they have re-formatted them, thinking that all the data has been wiped off. A regular format will not clean a hard-drive fully, and improperly disposed of hard drives have led to many lawsuits when dumpster divers and other criminals have recovered data and sold the data or posted it online. Using devices like a shredder or an electromagnet to destroy the hard drive is the current best practice for the disposal of hard drives. Shredding is also a good way to dispose of optical disks.

The third and final group of safeguards is the Technical Safeguards. There are a total of five standards and seven implementation specifications. Being technical, the responsible party for these safeguards will be those individuals that handle the network and IT security side of things (the Chief Information Security Officer).

The first and major standard is regarding access control. The administrative safeguard on access control was focused on the human side of access control (e.g. is the employee eligible for the job?) The physical side of access control was the badge access system (i.e. does the employee have a badge to access a certain area of the hospital?) The technical side of access control focuses on the levels of software and hardware access the human will receive. The four implementation specifications are as follows:

1. Unique User Identification (Required) Does each user have a unique identifier that can be used in case of an audit (e.g. Who viewed patient A's health information on May 20, 2012?)
2. Emergency Access Procedure (Required) In case of an emergency, how is access to ePHI controlled, and who is it granted to?
3. Automatic Logoff (Addressable) If a workstation is idle for a certain period of time, is there a timed logoff option? (Many hackers have been able to get onto machines left unlocked already logged in to and done great damage to the hospital.)

4. Encryption and Decryption (Addressable) What procedures are there to encrypt ePHI from unauthorized viewers? Wireless connections have the potential for packet sniffers and eavesdroppers where the data has been viewed or copied by unauthorized users. Encryption will ensure that only the authorized user can view the information.

Also, if a user has changed positions, there must be a solid documenting process to ensure that the access granted is current and that the user does not have too much or too little access.

The second standard is called the Audit Controls standard: “Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information” (Scholls, Stine, Bowen, Johnson, Smith & Steinberg, 2008). All ePHI data needs to have audit trail connected to it. The potential for a hospital employee to break the law by viewing a very important person’s (VIP) medical records is very high, and many lawsuits have been served because of this. Nadya Suleman (aka “Octomom”) sued the hospital where she was admitted which resulted in fifteen of the employees being fired. Security training and HIPAA Security awareness could have spared this hospital a lot of bad press and fines ("Hospital: 15 Fired," 2009). Having audit trails on ePHI will keep the finger of blame pointed at the appropriate party, rather than at the hospital as a whole.

The third standard is the Integrity standard: “Implement policies and procedures to protect electronic protected health information from improper alteration or destruction” (Scholls, Stine, Bowen, Johnson, Smith & Steinberg, 2008). This standard is basically a reminder to encrypt data while in motion, to audit all ePHI, and to ensure that the employees are trained to handle ePHI in an appropriate manner in accordance with HIPAA security.

Person or Entity Authentication focuses on checking to ensure that the user who desires to access the information is the person he claims to be. This would be accomplished by entering in a password or some other type of authentication (biometric – fingerprint or iris scan).

Transmission Security is the final standard in the technical safeguards. This covers all the different ways ePHI can be transmitted: wired, wireless, VPN, e-mail, remote usage, and mobile computing (laptops). Basically, there needs to be some documentation on what security measures are in place for each venue of transmission. For example, the wireless security policy might have the following documented:

- Ensure that 128-bit or higher encryption is used for all wireless communication.
- Fully test and deploy software patches and updates on a regular basis.
- Deploy Intrusion Detection Systems (IDS) on the wireless network to report suspected activities.

The Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009, was signed into law on February 17, 2009, to promote the adoption and meaningful use of health information technology ("Hitech Act Enforcement, 2009"). The following are the main focus of HITECH on data breaches and communication:

- If more than ten individuals are affected and cannot be contacted directly, the covered entity or business associate is required to post a general notification of the breach on his Web site and notify local print media.
- If more than 500 individuals are affected by the breach, the covered entity or business associate must notify Health and Human Services, and the responsible party must report to well-known media outlets of the breach ("Health Information Technology," 2009).

Basically, individuals who are affected by a data breach need to be notified, and if necessary (500 or more individual files), so do media outlets and the department of Health and Human Services. A listing of all hospitals who have reported breaches of 500 or more ePHI files are listed here: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/postedbreaches.html.

Health identity theft is a fast-growing crime, and steps must be taken to defend against it. HIPAA and HITECH are the government’s way of ensuring that all hospitals meet a minimum level of security. This baseline should be maintained and improved upon in an ongoing basis. By adhering to HIPAA and HITECH, the hospital is not only remaining compliant, but also ensuring to its patients that it is constantly improving its security in a dangerous environment.

References:

(2009). Health information technology for economic and clinical health (hitech) act hitech explained. CONEXIS, 5, Retrieved June 28, 2012, from https://www.conexis.org/pdfs/CONEXIS Comment July Issue.pdf

Andrews, M. (2008, February 29). Medical identity theft turns patients into victims. *U.S. News and World Report*, Retrieved June 7, 2012 from http://health.usnews.com/health-news/family-health/articles/2008/02/29/medical-identity-theft-turns-patients-into-victims

“Breach Notification Rule” *U.S. Department of Health and Human Services*, Retrieved June 28, 2012 from http://www.hhs.gov/ocr/pr"ivacy/hipaa/administrative/breachnotificationrule/index.html

“Code of Federal Regulations: Title 45-Public Welfare”. (2011, October 01). Retrieved June 28, 2012 from http://www.gpo.gov/fdsys/pkg/CFR-2011-title45-vol1/xml/CFR-2011-title45-vol1-sec164-310.xml

“Hospital: 15 Fired for Looking at Octuplet Mom's File.” (2009, March 31). *CNN*, Retrieved June 28, 2012 from http://articles.cnn.com/2009-03-31/us/octuplets.mom.firings_1_nadya-suleman-octuplets-la-habra?_s=PM:US

“Hipaa Security Series: Security Standards.” (n.d.). Retrieved June 28, 2012 from http://www.hhs. gov/ocr/privacy/hipaa/administrative/securityrule/physsafeguards.pdf

“Hitech Act Enforcement Interim Final Rule.” (n.d.). Retrieved June 28, 2012 from http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/hitechenforcementifr.html

“Identity Theft is America’s Fastest-Growing Crime.” (n.d.). Retrieved June 7, 2012 from https://postalinspectors.uspis.gov/investigations/MailFraud/fraudschemes/mailtheft/IdentityTheft.aspx

Mawson, T. (2003). Crucial business impact analysis. *Security*, *40*(8), 44. Retrieved from http://jproxy.lib.ecu.edu/login?url=http://search.proquest.com.jproxy.lib.ecu.edu/docview/197739643?accountid=10639

Scholls, M., Stine, K., Hash, J., Bowen, P., Johnson, A., Smith, C. D., & Steinberg, D. I. U.S. Department of Commerce, Computer Security Division. (2008). An introductory resource guide for implementing the health insurance portability and accountability act (hippa) security rule (800-66 Revision 1). Retrieved May 29, 2012, from National Institute of Standards and Technology website: http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf

“Utah Medicaid Cyberattack Affected 25,000 Social Security Numbers” (2012, April 06). *The Huffington Post*, Retrieved June 7, 2012 from http://www.huffingtonpost.com/2012/04/07/utah-medicaid-cyberattack_n_1409214.html