Kary Mason
MED INF 407, Winter 2011
January 8, 2011

Case Study: PHI Breach Strikes Local Hospital

Over the past several years, many changes have and continue to be in the forefront of health care. A leading concern is driven by the implementation of technology in the form of Electronic Medical Records (EMR's), Electronic Health Records (EHR's), and Personal Health Records (PHR's). Coupled with increasing knowledge that can be obtained through use of the internet in the form of general information as well as publically reported health care data, bring the heightened concern for confidentiality and patient privacy issues. These concerns are being addressed through legislation such as Health Insurance Portability and Accountability Act (HIPAA), American Recovery and Reinvestment Act of 2009 (ARRA) and Health Information Technology for Economic and Clinical Health Act (HITECH) with the objective to minimize litigation and establish guidelines for enforcing penalties resulting from violations by health care providers.[3] Litigation refers to cases resulting from breaches of confidentiality and integrity of Personal health information (PHI) resulting from misuse or disclosures. [3] The rule was also established to allow flow of information while protecting the public and "promoting high quality healthcare." [3] The following case study of a local hospital will demonstrate a sampling of violations of this legislation.

An ED physician from a St. Louis hospital (covered entity) contacted a local hospital (covered entity) in an effort to obtain medical information (PIH) about a former employee. The former hospital employee named Bob Evans (patient) had been at the local hospital last year and was involved in a car accident so the ED physician requested medical information be faxed right away. Jane Jones, an employee at the local hospital and former neighbor of Mr. Evans, used her access to the EMR to obtain PIH information out of curiosity. During the action of reviewing Mr. Evans EMR, she learned of his positive HIV status (PIH). During a neighborhood block party, Ms. Jones shared Mr. Evans HIV status (PIH). Discovery during preliminary investigation found not only did Ms. Jones review Mr. Evans

record; she downloaded and printed his record along with 510 other patients. It was also discovered Blue Cross/Blue Shield (covered entity) called requesting additional medical treatment information (PHI) to review a denial of Mr. Evans' insurance claim from his last admit at the local hospital. Bob Evans Jr. (son) visited the local hospital with the intent of pickup and delivery of other old medical records/x-rays/test results that had been requested by the St. Louis ED physician.

While Mr. Evans Jr. was picking up records, he mentioned his father's participation "in some kind of a clinical trial" requesting records from the trial. In an effort to assist Mr. Evans Jr., he was lead to the clinical informatics department and introduced to the informaticist aggregating data from the study. The informaticist was an independent consultant ("business associate"), hired specifically for the research project, proceeded to share preliminary results of the clinical trial with Mr. Evans Jr. The following day, after Mr. Evans' Jr. learned of the public's knowledge of Mr. Evans ("patient") HIV status he arrived at the local hospital requesting a meeting with the CEO.

Review of the details in this case demonstrates several violations that could result in penalty in the form of litigation and/or fines to the local hospital ("covered entity") as well as disciplinary action to the employees. Violations in this case can be summarized as follows:

- PIH information accessed by employee without "need to know"
- PIH information shared inappropriately
- Release of information violations to family and payer
- Release of information violation by "business associate" (consultant)

While there are obvious violations, some questions remain unanswered that may ultimately affect the outcome of this case. Additional information that may affect this case includes the role of the employee(s) involved and compliance with current policy and procedures. In addition, it is not clear if a contract exists between the "business associate" and the "covered entity".

HIPAA legislation was introduced in 1996 to provide protection of health information by establishing *Standards for Privacy of Individually Identifiable Health Information* also known as the

"Privacy Rule". The rule established standards for the use and disclosure of individuals' personal health information ("protected health information") by organizations ("covered entities") covered by the Privacy Rule. [3] "Covered Entities" are divided into three categories: healthcare providers (i.e., physicians, clinics, pharmacies, hospitals, etc.), health plans, and healthcare clearinghouses.(1) HIPAA also mandates security measures be implemented to protect against anticipated losses and disclosures as well policy and procedure requirement for covered entities.[3]

With an understanding of the objectives, the first violation was PIH information being accessed by an employee without "need to know" and further, she shared PIH (HIV status) with neighbors. The request for PHI from the St. Louis hospital ("covered entity") for the purpose of providing treatment for the patient is permitted and in fact is routine in healthcare but requires management within the law. Although the employee role is unclear in this case, Mrs. Jones may in fact be the appropriate person to send information to the requested "covered entity", however, perusal and disclosure of her findings within the record was a violation based on the provisions of use and disclosure of PHI documented in 45 CFR Subtitle A § 164.502 and § 164.514:[1]

> "(a) Standard. A covered entity may not use or disclose protected health information, except as permitted or required by this subpart or by subpart C of part 160 of this subchapter.
> (1) Permitted uses and disclosures. A covered entity is permitted to use or disclose protected health information as follows: (i) To the individual; (ii) For treatment, payment, or health care operations, as permitted by and in compliance with"
> "(b) Standard: Minimum necessary--(1) Minimum necessary applies. When using or disclosing Protected health information or when requesting protected health information from another covered entity, a covered entity must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request."[1]

Ms. Jones (employee) point of access in obtaining PIH was the EMR. As mentioned earlier, the employee's role is unclear, however, it is known the PIH information was accessed through use of the EHR. Section 45 CFR Subtitle C § 164.306 of HIPAA states addresses requirements for policies and procedures to maintain adequate security and ensure appropriate access to EHR data.[1] The rule allows for flexibility for the "covered entity" determining the best solution, however, role-based security tools would be a means of system security for EHR's.

Similar to the release of information to another covered entity, release of information to family and payers ("covered entity") need to be in keeping with the regulations set forth in 45 CFR Subtitle A § 164.502. Release of PHI to BCBS for payment falls under that of covered entities, however, appropriate measures are required to ensure PIH is being released to an appropriate covered entity, which should be established through policy and procedure. The son, however, would require medical power of attorney to authorize access to the patient's medical records and should only be released in keeping with hospital policy written in conjunction with HIPAA regulations.

It was the HITECH Act of 2009 that lead to modification of HIPAA in defining business associates responsibilities to healthcare organization in ensuring privacy and security as well address concerns for privacy and security for health information technology (HIT) including EHR's. "Under the HITECH Act, business associates are now directly "on the compliance hook" since they are required to comply with the safeguards contained in the Security Rule (SR)." [6] The HITECH act also established the regulations holding BA's subject to civil and criminal penalties for violations. [6]

The release of information violation by the consultant ("business partner") is based on 45 CFR Subtitle A § 164.502 and § 164.514. [1] This section of the regulations protects privacy and security of PHI and is inclusive of electronic PHI (ePHI). CFR's Subtitle A § 164.502 and § 164.514 defines appropriate use and disclosures of PHI that applies to the business partner. In addition, § 164.504 addresses the fact a business associate should have a contract that includes the requirements of use and disclosure as defined in § 164.502. If the consultant commits a "material breach of violations of the business associate's obligation" [1] the covered entity is noncompliant. [1] Introducing the son to the consultant ("business associate") allowing access to information of the clinical trial was inappropriate lead to the violation of the business associate agreement that should have been in place.

In summary, there have been several violations of HIPAA by the local hospital. The exposure of the hospital caused by this employee has opened the door for litigation from the patient and likely fines from the State's Attorney General and the Office of Civil Rights (OCR) at HHS. The violations

committed maybe the result of many factors including personal/professional judgment and lack of education on policy and procedure specific to HIPAA. In addition to the employee violations, the hospital could be held liable for violations from the business associate. It would be my recommendation that a complete and thorough investigation lead by the risk management department be completed. During the investigation, recommendation is to place the employees involved on suspension. In addition, implementation of the following action plans is recommended

Violation	Responsible Department	Recommendation
PIH information accessed by employee without "need to know" Release of information violation by business partner (consultant)	Information Technology	Implement role-based security in EHR Implement second level security access for sensitive PHI such as: HIV/AIDS test results, Mental Health, Alcohol and Drug Abuse, STD, Legal cases, Genetics
Release of information violations to family and payer	Medical Records	Risk Management investigation including running audits as established in HIPAA regulations to determine other breeches Review, revise and reinforce policies, procedures and practices of use and disclosure of PHI with focus on release of medical records Review, revise and reinforce policies, procedures and practices for obtaining ROI Implement policy addressing entry to secured areas such as IT departments, research areas, etc
PIH information shared inappropriately	Human Resources	Review and ensure proper investigation is completed with disciplinary action appropriate for violations
Use and Disclosure of PIH	Education Department	Review, revise and reinforce policies, procedures and practices of use and disclosure of PHI through education for all employees

References

1. http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/adminsimpregtext.pdf
2. American Recovery and Reinvestment Act of 2009, Public Law 111-5, February 2009 HR 1, 111th Cong, 1st Sess, Title XIII
3. Summary of the HIPAA Privacy Rule, United States Department of Health and Human Services
4. 45 CFR § 164.502
5. 45 CFR § 164.514
6. http://www.hipaasurvivalguide.com/hipaa-survival-guide-21.php