Data Privacy/Security - Group Case Study #1

MMI 407 Project 2

Golkonda, Jyothi

2/17/2013

Summary of Case study #1

Maria, Amy and I met three times during last two weeks and we had good discussion on the various issues within the case. Maria bought in the clinical perspective with her back ground. Amy and I bought in the issues from the IT perspective. We've discussed about how the hospital staff must have reacted either to the grandmother or the wife, and how the CEO must have reacted to the wife. Also the wife finding her way to the hospital informatics department and the incidental disclosures as a result i.e. chances of Mrs. Smith coming across PHI accidentally in the informatics department. Must patients or their relatives be allowed into the informatics department? We discussed about the hospital being transparent on their metrics but at the same time any memorandum marked as internal must not be distributed to the public. We talked about the need for a BA since the informaticist is a contractor and not hospital employee. After all the discussion here's the summary of issues in this case study.

Issue 1: Hospital staff's response to the Grandmother

The Grandmother learned from a neighbor about the emergency surgery for her grandson as a result of an accident at the factory he worked. The hospital staff must be courteous and understand the concern of the grandmother, but they cannot give the details of the patient especially medical related information to someone on the phone if the patient did not authorize sharing of medical information. Under HIPAA all covered entities such as hospitals and health systems have the responsibility for protecting the privacy and confidentiality of their patients and patient information. If the patient has opted out of the hospital directory then the staff cannot reveal any information to the grandmother. They will have to redirect her to check with other

relatives in the family who may have knowledge of her grandson's condition. If the patient has not opted out of the hospital directory then the hospital staff may provide the patient's location in the facility, and a description of the patient's condition that does not communicate specific medical information.

Issue 2: Neighbor downloading and printing 510 medical records

There are several issues around the neighbor accessing and printing 510 medical records. The issues can vary depending on the answers to the following questions.

1. Is there any PHI in the 510 records the neighbor has printed?
2. Is the neighbor an employee or contractor of the covered entity?
3. If the neighbor is a contractor for the covered entity, then is there a business agreement?
4. If the neighbor is an employee or contractor was the neighbor trained on HIPAA personal information security and is the training current?
5. If the neighbor is not an employee or contractor then clearly a breach has occurred and the hospital, as a covered entity must take the necessary actions of contacting the patients impacted by the breach and make a public announcement regarding the breach and notify HHS, since more than 500 patients could be potentially impacted.

If the neighbor is either an employee or a contractor then several questions as above have to be answered to determine if it were a breach or not. If the neighbor is an employee and has accessed the 510 patient records when there was no reason to access, then it is a HIPAA security issue. If the neighbor has legitimate reasons to access the 510 patient records then the rules discussed in issue #1 apply to the neighbor on disclosure of patient information to the grandmother. If the

patient has opted out of the hospital directory then the neighbor was not supposed to disclose the patient's information to the grandmother and has clearly violated the privacy rule.

If an employee knowingly and wrongfully obtained, used or disclosed medical information, they may receive fine for HIPAA violation ranging from $100 to $50,000 per day and annual cap of $1.5 million for the same violation based on if the violation was due to "reasonable cause" or due to "willful neglect". In addition the employee may also receive more severe consequences like probation or prison sentence.

Issue 3: Hospital Staff's response to the Chicago Police

The Chicago police can only access any medical records if they come with a court order or court-ordered warrant. Even in case of a court order only the "minimum necessary" information must be provided. Appendix B covers the scenarios when law enforcement agencies can request PHI. The covered entities should have policies and procedures that require office staff to verify the recipient's fax number and use a cover sheet that does not include protected health information.

Since the patient was injured at the company where he was working, the employer of the patient may have access to the blood tests if the patient had workers compensation. The HIPAA privacy rule does not apply to entities that are worker's compensation insurers, workers compensation administrative agencies or employers.

Issue 4: Hospital staff's response to BCBS

HIPAA privacy rule allows a covered entity to use and disclose protected health information, with certain limits and protections, for treatment, payment, and health care operations activities.

However a covered entity must develop policies and procedures that reasonably limit its disclosures of, protected health information for payment and health care operations to the "minimum necessary"[1]. In the case of Blue Cross Blue Shield the hospital staff can provide the information requested based on the "minimum necessary" clause for the processing of payment.

Issue #5: Nurse and wife interaction

Mr. Smith's wife approached the nurse with questions on Mr. Smith's care and took the discussion further by asking questions on the hospital metrics regarding similar cases for that particular post-op bacterial infection. The Nurse provided Mrs. Smith with a 1 year old hospital internal memo. The nurse must not share any memos that are marked as internal with the patients or with patient's relatives. This is a business and ethical issue. If the internal memo has any PHI, then the nurse has violated HIPPA privacy rule also. The Nurse HIPAA training status must be evaluated to determine if the violation was "willful neglect". As discussed earlier the Nurse can face fines and may be jail in addition to being fired from job.

Issue # 6: Wife and Informaticist interaction

After discussion with the Nurse, Mrs. Smith went to the informatics department. This is a security issue. There is no reason for patients or their relatives or care takers, to visit the informatics department. The access to the informatics department must be restricted to avoid "incidental disclosures". The informatics department may be researching on better patient care and studying the various trends in patient care. There may be accidental disclosures of PHI in the

1. (HHS.gov)

informatics department due to discussion between the staff or information displays on screens with PHI.

Mrs. Smith had a lengthy discussion with the informaticist. There is a business issue hear. The job description of the informaticist does not include answering patients or patient's representatives. The informaticist must not have any discussion with Mrs. Smith but instead refer her to Mr. Smith's physician. The case study does not detail what was disclosed by the informaticist. But the "Business Associate Agreement" between the hospital and the informaticist prevents unauthorized use or disclosure of information. The informaticist may face termination of contract for disclosing information to Mrs. Smith even if PHI was not involved.

Issue # 7: Wife and CEO interaction

The CEO must meet with the wife of Mrs. Smith and explain to her all the efforts the hospital is taking to improve patient care and prevent hospital acquired infections. Explain that the 2 year study under research by the informatics department is one such effort. The CEO must explain the preventive measures that are being followed at the hospital and prove that Mr. Smith was also provided all such care by administering antibiotics before surgery and additional measures taken to disinfect everything the patient may be exposed to etc.

The CEO can provide the published hospital metrics for last year and this year to Mrs. Smith to show how the hospital has improved since last year. The CEO can promise Mrs. Smith that they will investigate Mr. Smith's case to see if the infection is due to the negligence of the hospital and wave any expense to treat the infection if it was hospital acquired. Medicare does not pay for hospital mistakes and infections. Similarly if Mr. Smith's infection is hospital mistake then he must not be charged for the treatment of the infection.

The CEO must not be worried about Mrs. Smith going to The Chicago Tribune as long as the internal memo does not have any PHI. If the hospital publishes their yearly metrics and is transparent with their status then the information that Mrs. Smith has will not be a surprise to the public. The year old information may not be relevant anymore if a more recent report was already published.

If the internal memo has PHI then it is a security issue and must be stopped from being published. Even if the memo is stopped from being published since the PHI was already exposed the hospital must contact the affected patients within 60 days of the discovery of the breach with a description of what happened and steps for individuals to protect themselves, a description of the hospital's efforts to investigate, mitigate and prevent further breaches, and contact information. If more than 10 patients are impacted the hospital must do a conspicuous Web site posting or notice in major print or broadcast media. If more than 500 patients are involved in the breach then the patients must be contacted and the hospital must provide notice to “prominent media outlets” and self-disclosure to HHS.

In the case of the 510 patients medical record printed by the neighbor, and if the neighbor was a non-employee and not a contractor and printed the records or if the neighbor was an employee who was not supposed to access that information, then the hospital must contact all the 510 patients with information on the breach and how to protect themselves and provide notice to “prominent media outlets” and must also provide immediate notice to HHS.

References:

Hospital and Law Enforcement Guide to Disclosure of Protected Health Information Fourth Edition (August 2010) Retrieved from http://www.wsha.org/files/62/HIPAA_Guide_2010.pdf

SUMMARY OF THE HIPAA PRIVACY RULE - section - Permitted Uses and Disclosures. Retrieved from HHS.gov
http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf
http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html

DISCLOSURES FOR WORKERS' COMPENSATION PURPOSES (2003, April). Retrieved from HHS.gov
http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/workerscompensation.pdf

Consequences of an Employee Violating HIPAA
http://www.ehow.com/info_8544751_consequences-employee-violating-hipaa.html

HIPAA Violations and Enforcement. Retrieved from AMA
https://www.ama-assn.org/ama/pub/physician-resources/solutions-managing-your-practice/coding-billing-insurance/hipaahealth-insurance-portability-accountability-act/hipaa-violations-enforcement.page

Breach Notification Rule. Retrieved from HHS.gov
http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html

Uses and Disclosures for Treatment, Payment, and Health Care Operations. Retrived from HHS.gov
http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/usesanddisclosuresfortpo.html

HIPAA: Health Insurance Portability and Accountability Act. Retrieved from AMA
http://www.ama-assn.org/ama/pub/physician-resources/solutions-managing-your-practice/coding-billing-insurance/hipaahealth-insurance-portability-accountability-act/frequently-asked-questions.page

Incidental Uses and Disclosures. Retrieved from HHS.gov
http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/incidentalusesanddisclosures.html

Business Associate Contracts. Retrieved from HHS.gov
http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html

Appendix A – Case Study #1

Yesterday, a call came into the ICU nursing station from what sounds like an elderly woman. She said she is the grandmother of one of the patients on the unit named John Smith who, she just learned from a neighbor, had emergency surgery 3 days earlier after an accident at the factory where he worked. She was obviously distressed and wanted to know how her 25-year old grandson was doing. A preliminary investigation found the neighbor had downloaded and printed out the medical records of 510 hospital patients 2 days earlier, including the records of John Smith. Last night, a Chicago Police Officer called the ICU asking them to fax over copies of the patient's blood tests and other lab results from when he was admitted through the ED, because Mr. Smith's supervisor suspects that drugs were a cause of Mr. Smith's accident. Early this morning, a representative from Blue Cross/Blue Shield called and wanted additional medical treatment information to begin processing Mr. Smith's insurance claim. Shortly thereafter, while a nurse was checking Mr. Smith's vital signs, his wife came in to visit. Mrs. Smith begins to ask questions about Mr. Smith's care, including what data the hospital has on how many other patients in this hospital have ever come down with this particular post-op bacterial infection. The nurse told her that "they did a study a year or so ago, but that this kind of post-op infection still happens all the time here, so we just treat them as best as we can" and gave her a copy of a 1-year old internal memo from the hospital's clinical informatics department that showed an increasing trend in post-op bacterial infections at the hospital. The wife finds her way to the hospital informatics department and speaks at length to the informaticist who wrote that old memo and who is an independent consultant hired for this 2-year research project. Mid-morning, the wife called the hospital CEO and demanded that he cancel any medical billing for her husband's admission because the hospital caused her husband's life-threatening infection and knew this was a hospital problem of long-standing, or else she will call The Chicago Tribune and report what the nurse told her, as well as supply the newspaper with a copy of that old hospital memo. The CEO wants to talk to you about this situation and what to do about it.

How should staff respond to the grandmother?
What should be given to the Police officer?
How should you respond to BCBS?
Did staff respond appropriately to the wife?
How should the CEO respond to the wife?
Is there a BA Agreement involved here?
Why should the CEO be concerned about the release of the 510 med recs?
Outline how the CEO should respond to the wife?
What are the consequences if the "neighbor" was a hospital employee?
Are there any Incidental Disclosures here?
Outline the HIPAA security issues arising from the visit to the hospital informatics dept?
Do you see any other business, legal, ethical, or social issues not already addressed here by these Qs? *Hint…there are several!*

Appendix B - Permitted Uses and Disclosures

Covered entities may disclose protected health information to law enforcement officials for law enforcement purposes under the following six circumstances, and subject to specified conditions:

1. as required by law (including court orders, court-ordered warrants, subpoenas) and administrative requests;
2. to identify or locate a suspect, fugitive, material witness, or missing person;
3. in response to a law enforcement official's request for information about a victim or suspected victim of a crime;
4. to alert law enforcement of a person's death, if the covered entity suspects that criminal activity caused the death;
5. when a covered entity believes that protected health information is evidence of a crime that occurred on its premises; and

by a covered health care provider in a medical emergency not occurring on its premises, when necessary to inform law enforcement about the commission and nature of a crime, the location of the crime or crime victims, and the perpetrator of the crime.

Retrieved from
http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf

Appendix C - HIPAA Violations and Enforcement

HIPAA Violation	Minimum Penalty	Maximum Penalty
Individual did not know (and by exercising reasonable diligence would not have known) that he/she violated HIPAA	$100 per violation, with an annual maximum of $25,000 for repeat violations (Note: maximum that can be imposed by State Attorneys General regardless of the type of violation)	$50,000 per violation, with an annual maximum of $1.5 million
HIPAA violation due to reasonable cause and not due to willful neglect	$1,000 per violation, with an annual maximum of $100,000 for repeat violations	$50,000 per violation, with an annual maximum of $1.5 million
HIPAA violation due to willful neglect but violation is corrected within the required time period	$10,000 per violation, with an annual maximum of $250,000 for repeat violations	$50,000 per violation, with an annual maximum of $1.5 million
HIPAA violation is due to willful neglect and is not corrected	$50,000 per violation, with an annual maximum of $1.5 million	$50,000 per violation, with an annual maximum of $1.5 million

Retrieved from AMA

https://www.ama-assn.org/ama/pub/physician-resources/solutions-managing-your-practice/coding-billing-insurance/hipaahealth-insurance-portability-accountability-act/hipaa-violations-enforcement.page