NORTHWESTERN UNIVERSITY

Case Study #1 – Kevin Scharnhorst

Kevin Scharnhorst

An independently written summary and analysis of issues identified in evaluating an assigned case study covering HIPAA and privacy and security concerns.

MMI 407 – Legal, Ethical & Social Issues in Medical Informatics

Fall 2010

Northwestern University

The objective of this project was to combine individuals with a diverse range of professional backgrounds and talents into a cohesive group to analyze and identify potential HIPAA and privacy and security related issues from a fictitious case study. The group was made up of four individuals with an equal split of half having technical and the other clinical backgrounds. The case study itself involved pretend actors including; a hospital patient named John Smith, his Grandmother, the Grandmother's neighbor, the Chicago Police Department, Blue Cross/Blue Shield (BCBS), Mr. Smith's wife, Mr. Smith's employer, the hospital's CEO and the Chicago Tribune. Through a course of events, Mr. Smith finds himself in the hospital having undergone surgery from a sustained accident at work. It was the group's responsibility to evaluate the situation and consider the privacy of information related to Mr. Smith's care. There were a total of seven issues identified, of which will be covered. (Appendix)

Issue #1 – Concerned Grandmother

The Grandmother had learned through her neighbor that her Grandson had been admitted for emergency surgery two days ago following an accident that happened at the factory where her Grandson worked. Concerned, she called into the ICU to find out how he was doing.

The genuine heartfelt concern for her Grandson is a social concern. It is natural for the ICU staff to want to cater to the share information with her about her loved one. The hospital, however, is a covered entity under the HIPAA Privacy Rule and because of this is accountable to protect any personal health information (PHI) regarding the care of Mr. Smith. This includes all informational formats such as electronic records, paper or verbal communications. HIPAA is concerned primarily with the use and disclosure of PHI. Assuming Mr. Smith was coherent and did not opt to be listed in the hospital's directory, the ICU would be okay to confirm his room number with the Grandmother, but not any medical information without prior consent from her Grandson. In the event that he did opt out, it would be recommended to suggest that she reach out to other family members to seek to find out her

Grandson's condition. If Mr. Smith were available it would be permissible to ask if he would like to speak to her.

Issue #2 – Potential Security Breach

A great deal is left for speculation on the issue of the Grandmother's neighbor. We know that through preliminary investigation that the Neighbor had downloaded and printed out the medical records of 510 hospital patients 3 days previous to the ICU inquiry. Research should seek to explain the Neighbor's role to the hospital, such as being an employee or consultant. If it were determined that they were a consultant, a Business Associate Agreement should exist as well as an understanding of the scope of that agreement. In either case, the Neighbor would be an agent to the hospital and the hospital responsible for their actions so it is important to establish the legitimate need for access and use of the information. The volume of records that were accessed and printed would also need to be justified. It could have been for a legitimate purpose such as research, medical coding, etc. In all cases where this person had authorized access to the medical records it would be prudent to ensure that this individual was current on HIPAA training and to ensure that the information was being used appropriately. The data set that was printed should be checked to see if it was limited or deidentied to HIPAA's required 18 points under the "Safe Harbor" provision. If the data were limited, a Data Use Agreement could cover the information for use pertaining to research, health care operations or public health purposes. If it were, the HIPAA privacy rules would not apply. The Neighbor's knowledge and training on HIPAA would also be of paramount importance. If they knowingly and wrongfully obtained, used or disclosed the medical information, they could be facing monetary fines and even prison according to consequences defined prior to the HITECH Act. The advent of the HITECH Act, brought fines and prison time that graduate in severity on a four tiered scale based on the person's determined level of knowledge or ignorance. If the person were not employed by the hospital, then follow up action

would be needed by the hospital to notify all 510 affected patients within 60 days of learning about the breach. (Health Information Privacy, 2010*)*

The implications on this issue could be grave and it would be wise to involve the hospital's Chief Privacy and Security officers further on the matter to be investigated formally and assess the risks better.

Issue #3 – Chicago Police Department

Law enforcement was involved on the employer's suspicion of Mr. Smith using drugs that caused the accident. Suspicion is not enough for the medical records to be provided to the Police Officer that called to request them. Under the Law Enforcement Exemption under HIPAA, the request must be accompanied with a legal request, such as a subpoena. Another potential issue is that the records were requested to be faxed. The security rule under HIPAA requires that covered entities such as the hospital have appropriate administrative, technical and physical safeguards in place to protect the transmission or exchange of PHI. Provided a subpoena existed, share only the minimum necessary data and ensure that the other end of the fax transmission at the police station is secured before transmitting. If not secured, then arrange for other means to exchange the records. The Police Officer could also seek to obtain patient permission to share the records. There are a number of justified reasons to share medical records with Law Enforcement under HIPAA (*SUMMARY OF THE HIPAA PRIVACY RULE, 2010)*. It would be appropriate in any case to advise the Chief Privacy and Security Officers of the request.

Issue #4 – Blue Cross / Blue Shield (BCBS)

BCBS called to get additional treatment information to start processing Mr. Smith's medical claim. BCBS is a covered entity under the HIPAA privacy rule and as such the hospital is not prohibited in any way to share the medical treatment information with them. However it would be appropriate to

share the "minimum necessary" such as date of service, length of stay, etc. and then leave the details to be submitted through billing when the medical claim is submitted from the hospital to BCBS. The information being requested by BCBS falls under payment under HIPAA's provision for sharing information related to the coordination of treatment, payment or healthcare operations (TPO). It is the provider's responsibility to make reasonable efforts to limit the amount of protected health information that is shared with the requestor. This would protect the hospital in the event that Mr. Smith was found to no longer be eligible through BCBS and this was found out through when verifying his coordination of benefits (COB). In sharing the information, it would also be necessary for the provider to ensure that appropriate security safeguards exist that are administrative, technical and physical in nature to protect the information exchange. (AMA, 2010)

Issue #5 – Wife, Nurse and Informaticist

Mr. Smith's wife approaches the Nurse with some very specific questions about post-op infections that have occurred at the hospital. The Nurse shares more she should have and gave her a copy of internal hospital memo on rising pos-op infections over the past year. Mr. Smith is not a covered entity and further the case study does not indicate if the Nurse checked to ensure that Mrs. Smith was even a designated representative. She should have referred the Wife to an attending physician and never given out the internal memo.

Leading from the memo, the Wife finds her way in the clinical informatics department and talks with the Informaticist who wrote the memo. The Informaticist is an independent consultant hired for this 2 year research project. The Informaticist's should not have spoken to the Wife, but did at length. The incident should have been reported to the Chief Privacy and Security Officer so the incident could begin being investigated further at that point. There should also be a current Business Associate Agreement in place with the Informaticist. It should be checked to determine what all is covered.

HIPAA training is required annually by the hospital. The last completed date should be checked for both the Nurse and the Informaticist to ensure they are current. Action should be taken accordingly based on their knowledge of HIPAA. The Nurse or Informaticist could be fired and additionally face civil or criminal charges based on their knowledge of wrongfully sharing the information and jeopardizing the hospital's liability in the issue.

Issue #6 and #7 – The CEO Debrief With the Wife

The Wife concludes after gathering all the information with a call to the Hospital's CEO demanding that he cancel any medical billing for her husband's admission because the hospital caused her husband's life-threatening infection. She follows the demand with a threat that she would go to the Chicago Tribune with a copy of the memo if he didn't.

At this point, both the CEO and wife are probably emotionally charged. It would be the proper action for the CEO to remove the emotion by empathizing with the Wife. He should respectfully commit to gather all the facts from all those involved at the hospital and arrange a follow up meeting with the Wife to collect her side. He should not react to the threat, but document it as such and possible extortion.

When the meeting occurs with Mrs. Smith, the Chief Security and Privacy officers should also be involved as they would be conducting the investigation.

After talking with Mrs. Smith all recommended corrective action should be followed through on and hopefully the situation will have deescalated to everyone's satisfaction.

References

HIPAA Health Insurance Portability Accountability Act. (2010). Retrieved October 09, 2010 from American Medical Association, 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.shtml.

Health Information Privacy. (2010). Retrieved October 07, 2010 from U.S. Department of Health & Human Services, Breach Notification Rule: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html.

SUMMARY OF THE HIPAA PRIVACY RULE. (2010). Retrieved October 07, 2010 from United States Department of Health & Human Services, HHS: http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf.

Appendix

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 two 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 3 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?

Are there any other business, legal, ethical, or social issues?