Novelty Journals

ISSN 2394-9694

International Journal of Novel Research in Humanity and Social Sciences
Vol. 3, Issue 4, pp: (149-150), Month: July – August 2016, Available at: www.noveltyjournals.com

Health Care Organizations Must Protect Patient Information or Pay

Carroll M. Sapp

BSRT, RRT, RCP

When congress passed the Health Insurance Portability and Accountability Act of 1996 (HIPAA) it transformed the way businesses think and act when it comes to being compliant with the privacy of information shared with individuals throughout their networks. HIPAA's privacy and security rule "is designed to ensure that health information is protected from unauthorized access and disclosure, and designates the administrative, technical, and physical controls that covered entities must put in place (U.S. Congress, 1996; The HIPAA Security Rule, 2013)" (Koontz, 2015). These new rules bring new adjustments, which organizations must make, including mandatory training of personnel on HIPAA rules and regulations and creating a breach notification response plan, in which employees should be educated and fluent.

According to the HIPAA privacy rule, an entity is categorized as a health care provider, a health care clearinghouse, or a health plan that shares information electronically. The HIPAA rule maintains that "an organization or individual that is one or more of these types of entities is referred to as a "covered entity" in the Administrative Simplification regulations, and must comply with the requirements of those regulations" (CMS, 2015). One example of a "covered entity "can be seen in discharge planning, when a hospital of acute care, shares patient information electronically with an outpatient sub acute care rehab.

Upon HIPAA's introduction, the government recognized that many organizations "had difficulty interpreting the Privacy Rule's requirement that a covered entity make reasonable efforts to limit the disclosure of PHI to the "minimum necessary" to accomplish the purpose of the disclosure" (Claiborne, Hesse, & Roble, 2009). The vagueness of the rule caused many misinterpretations of the rule. Thus, clarity was later provided by the government, which further defined what "minimum necessary" entailed. The HIPAA rule now mandates "that covered entities limit the use, disclosure, or request of PHI to the limited data set, to the extent practicable, or, if needed by the entity, to the minimum necessary to accomplish the intended purpose" (Claiborne, Hesse, & Roble, 2009).

In 2009, an act called the Health Information Technology and Economic and Clinical Health (HITECH), was introduced to broaden privacy regulation and hold HIPAA violators to stiffer punishment's for non-compliance. HITECH penalties are arranged in order of a hierarchy of offense. For a lower level violation, the minimum penalty imposed is one hundred dollars. A second level of violation would bring a minimum penalty of one thousand dollars. Violations at the third level of offense will produce a minimum penalty of ten thousand dollars. Lastly, for a level four violation, which is considered to be the most obtrusive of offenses, the minimum penalty or fine is fifty thousand dollars. The rules under HITECH "make a covered entity liable for civil penalties, due to a business associate or business associate's subcontractor's violation, regardless of whether there was a compliant contract in place or whether the covered entity knew of the violation or acted appropriately in response to the violation" (Degaspari, 2011).

One recent article, announced the settlement of a HIPAA breach occurrence. A company named Cancer Care Group, P.C., was fined seven hundred and fifty thousand dollars related to an incident in which one of their employees had a lap top computer stolen from them (HHS, 2015). Not only did the thieves get a laptop top computer, but also, "unencrypted backup media, which contained the names, addresses, dates of birth, Social Security numbers, insurance information and clinical information of approximately 55,000 current and former Cancer Care patients" (HHS, 2015). The gross mishandling of patient medical information, surrounding this case has resulted in an organization's bottom line being hit

hard, and has gotten other health care companies scrambling to strengthen their own privacy policies, in an effort to avoid being found non-compliant with HIPAA and ensure that their patients' information is protected.

There are many pathways for a patient's information to be inadvertently released without the patient's knowing or consent. One such way is through a cyber attack in which a health care providers database is illegally hacked into, resulting in patient information being stolen and then sold for criminal intent. Theft of patient information can be monetarily lucrative for criminals, and they will seek out all avenues available to obtain it. Either by a malicious cyber attack, or as in the case of the Cancer Care Group, in which a laptop computer was stolen from an employee. For these reasons, it is essential that an organization "make arrangements with their laptop suppliers to ensure that laptops are encrypted before they are allocated to staff members" (Delaney, 2010). Another way a patient's information could be released without his or her consent could be through the information being electronically sent to a wrong destination, or inadvertently lost. For example, the laboratory results of a patient could be sent via e-mail to the wrong recipient. Thereby, making the patient and their information vulnerable.

Companies and associates of like must comply with HIPAA rules and regulations. A patient's privacy must be observed, preserved, and protected. Failure of an organization, being able to meet any of these privacy demands will be met with stiff penalties, as a result of the HITECH act. There are many different ways patients medical information can be exposed, or released without their consent. One such challenge is theft. Companies should implement policy and procedure of the highest standard, in order to meet these challenges.

REFERENCES

[1] Claiborne, A. B., Esq, Hesse, J. R., Esq, & Roble, D. T., Esq. (2009). Legal impediments to implementing value-based purchasing in healthcare. *American Journal of Law and Medicine*, *35*(4), 442-504. Retrieved from http://search.proquest.com/docview/749650010?accountid=89121

[2] Covered Entity Charts. (n.d.). Retrieved November 12, 2015, from https://www.cms.gov/Regulations-and-Guidance/HIPAA-Administrative-Simplification/HIPAAGenInfo/Downloads/CoveredEntitycharts.pdf

[3] Degaspari, J. (2011). Preparing for HITECH and HIPAA compliance. *Healthcare Informatics*, *28*(2), 56-56,58,60,62. Retrieved from http://search.proquest.com/docview/851708500?accountid=89121

[4] Delaney, M. (2010). Patient information and data protection. *Irish Medical Times*, *44*(26), 22. Retrieved from http://search.proquest.com/docview/606648768?accountid=89121

[5] HHS. (2015, September 2). $750,000 HIPAA settlement emphasizes the importance of risk analysis and device and media control policies. Retrieved November 14, 2015, from http://www.thefreelibrary.com/$750,000 HIPAA settlement emphasizes the importance of device control...-a0433436498

[6] Koontz, L. (2015). Health information privacy in a changing landscape. *Generations*, *39*(1), 97-104. Retrieved from http://search.proquest.com/docview/1683507002?accountid=89121