

Term Paper

Alexandria Bergeron

August 16, 2020

HCA-450-OL01

Health Information Technology

Health information technology is the input of patients health care records into an electronic information's system in which can be accessed virtually. The purpose of this is to "improve the quality of health care, prevent medical errors, reduce health care costs, increase administrative efficiencies, decrease paperwork, and expand access to affordable health care" (OCR). While there are many benefits associated with having electronic records it also imposes ethical conflicts as well. That the main objective is to ensure that patients are receiving the best health care while still maintaining privacy and security through these electronic health information systems.

The electronic medical records (EHRs)

Electronic medical records (EHRs) are a patient's health data record all converted into a virtual chart that can be accessed virtually. EHRs are "real-time, patient-centered records that make information available instantly and securely to authorized users" (HealthIT.gov). However, some health care organizations have been indisposed to implement EHRs for different reasonings such as privacy, confidentiality and security.

First being patient privacy because as HIM professionals it is critical to keep all patient information secured. When looking at patient privacy it is considered to be a social value that means the "right to be let alone" (Harman, p. 78). That the patients information is to be protected and only used by the individuals that have been given access to it. Even if the patient is to go to another doctor, for example, before the new physician can gain access to the patients information the patient has to sign over the permission to do so. The patient is in control of whom is allowed to have access to what information.

When looking at confidentiality this is the information that the patient is sharing with the physician. When this interaction takes place it is automatically presumed that the information is going to be kept between them and not discussed elsewhere. This is why before employees are allowed to interact with patients and their information they must take a HIPPA class. That is because this is the first point in which employees are properly informed on what it means to keep patient information confidential and to only be used when it involves the patient in question.

In order for the healthcare system to operate effectively patients have to be able to confide in their physician's with confidential information. The managers and doctors need to make sure they establish themselves as a respectable figure that will not tolerate unethical use of patient information. This is important in order to effectively aid the patient to get the best desired outcome. If the patient doesn't feel comfortable enough to share all of the information they will only share parts. When this happens it can lead to unnecessary testing and misdiagnosis. Without having obtained all of the information from the patient, the health care provider can only do so much.

Lastly is security, because it is because they have to be able to ensure patients that their information is being kept safe within their technology system. This means that they have a system that keeps their system locked from outside hackers and if they see a threat they find a solution. It also means that they have control over who will be able to access their private information. They can protect this information by only allowing individuals who have been authorized to access their health information the permission to do so.

One strategy to help reassure the implementation of a new health information system is to ensure that all HIM professionals are always aware of any changes that are happening within the laws that they have to abide by. "The goal is to practice HIM in ways that meet the AHIMA Code

of Ethics" (Harman, 2015, p. 328). That they are always staying current with the laws because that is the best way to ensure that they are not conflicting with the ethical concerns that can arise from the misuse of technology. Also by staying accredited ensures that the HIM professional has taken the appropriate actions needed to help lower the chances of ethical issues arising. Another important law that helps with this is HIPAA since its main focus is the privacy and confidentiality of patients.

The Health Insurance Portability and Accountability Act (HIPAA)

The Health Insurance Portability and Accountability Act of 1996 also known as HIPAA was implemented in order to set regulations that needed to be followed in order to protect the privacy and security of patients health care information. These electronic information systems hold more than just the patients' health records but also their private information in order to "pay claims, answer eligibility questions, provide health information and conduct a host of other administrative and clinically based functions." (U.S. Department of Health & Human Services). Healthcare professionals are constantly receiving and reviewing their patients personal and confidential information which is why it is important that all HIM professionals take the time to understand the importance of valuing and preserving the privacy of their patients. Before HIM professionals are allowed to interact with patients and their private information they have to take a HIPAA class in order to learn these "regulations protecting the privacy and security of certain health information" (Office for Civil Rights, 2013).

The reason that HIPAA is so important is because patients privacy begins once the patient comes in contact with the HIM professional. The professional needs to be knowledgeable on how and when to affectively use patients information. The patient needs to

feel that they are protected and that their personal health information is not going to be misused. Otherwise, it can effect the patient professional relationship which hinders the healthcare that is being received. Because now the patient isn't going to confide into the provider like they should in fear of their privacy being breached. So in return this causes the patient's medical records to not be fully accurate because all information is not be disclosed.

The Health Information Technology for Economic and Clinical Health (HITECH) Act

The health information technology for economic and clinical health act is to encourage health care professionals to use electronic systems while still ensuring that patients privacy and security is still protected. It also is has a financial incentive if providers switch to this information technology system but it also increases the penalties if violations occur in HIPPA.

The medical staff can increase the quality of medical services by using HITECH because patients are able to be seen faster. Information is transported and read quicker through technological devices versus on paper. They also have to enter information by coding which is a quicker way for professionals to get a quick understanding of what the patient is being seen for.

The digital health technologies

With digital advancements in health care technologies there are ethical considerations and conflicts that affect the consumers, patients and caregiver. Almost all doctor offices, urgent cares, and hospitals are updated with virtually everything being done through some form of electronics. However, there are still offices that have yet to catch up to this newer form of technology information systems. Whether it is because they do not have the funding's to do so or they are an older practice that is not on board to making the switch. So while other doctors and nurses are carrying around tablets or laptops where they are capable of pulling up all of the patients records, these clinics are not doing so making it a much longer process of getting

patients in and out. There are also instances where the consumer is not adequately using their information systems to their full potential even though they have everything that they need.

Patients also have the ability to check themselves into these places via a tablet in the front lobby making it more convenient for both the patient and facility. However, the only problem that arises with this that not all facilities are using the same information systems. So this makes it challenging to access patient information through these different systems. Data technology is so advanced that patients can even access their own electronic health records through data portals provided by their physician or hospital they were seen at. They also have the ability to "enter the information themselves in the device, or the device collects information on command or passively" which is why data quality is so important (Harman, p. 548). However, this is risky because it becomes a greater target for hackers because it is easier for them to gain access to this personal information.

These risks also arise when patient information is not being properly inputted into these data systems. It is up to the HIM professionals to try and ensure that all information that are in these electronic records are accurate. Otherwise, this is when mistakes begin to be made because without all of the accurate information patients are not getting the adequate treatment that they need. An ethical concern is that in emergency situations or if the HIM professional is not properly performing their job, the screen in which the patient information is being displayed can be easily accessed by others whom are not supposed to see this information. Patient privacy is also a concern because their information is more easily accessible to be breached by outsiders. This is why it is always a good idea to have "a third-party auditor" to ensure that information is being stored properly and that employees are abiding by the HIPPA law (Tank,2018).

Digital health technology is important in our day of age even though it does pose risks. More patients are able to be seen which is needed for emergency situations when the health problem isn't great enough to take up space in an emergency room but yet the patient still needs to be seen in a timely manner. With this comes HIM professionals always rushing around in which can lead to them accidentally leaving patient records open to be accessed from individuals who do not have permission to do so. One way this could be avoided is if the computers automatically time out on their own if no activity occurs within a minute or two. It is a lot easier for the HIM professional to just log back in than it is to go through all of the hassle of someone getting a hold of what was on the computer.

Another precaution that can be taken is black out screen protectors. By doing this it makes the screen appear as if it is complete off even when it is not. This eliminates temptation of being accessed because it would be assumed that the electronic device is not on. They also can enforce all providers to merge to one primary information systems. By doing this would allow for providers to have easy access to patients information regardless of where they were seen at because it will all be in one system. They also would be able to focus heavily on security by only using one information system because they would have more people informing of where errors are occurring. This would allow them to better form a protection wall on these systems.

The laws and penalties

In healthcare there is a clear difference between fraud and abuse. When looking at fraud we are looking at the intentional act of dishonesty. Being that an employee incorrectly informed the workplace of the skill sets that they have and are still trying to perform these tasks without the proper knowledge. Another common example would be billing patients or not billing patients for procedures that they did or did not actually receive. Abuse on the other hand are "practices

that are inconsistent with accepted sound fiscal, business, or medical practices, and result in an unnecessary cost or in reimbursement for services that are not medically necessary or that fail to meet professionally recognized standards for health care." (The Johns Hopkins University, 2019). This is why HIPPA and HCFAC was put into place in order to help prevent fraud and abuse from occurring. That as a HIM professional they are obligated to perform their job and abide by their oaths to do what is right for the patient and the facility in which they work for.

The False Claims Act "prohibits the presentation of such false or fraudulent claims to the government" (Harman, pg. 121). Meaning that it doesn't allow for HIM professionals to knowingly report claims that did not happen. If they are caught doing so it will result in criminal, civil, or administrative liability. This is why as a HIM professional it is important to remain aware at all times of the information that is being given and properly interpreting it. If it becomes prevalent that fraud is taking place it is within their responsibility to not continue the documentation because they are aware of what is going on and it needs to be addressed. This is why the American Hospital Association established the Coding Clinic to simplify and unify the way data is being imported. All of this is done for the protection of patient privacy. To ensure them that they are receiving the best quality of care while there private information is being protected.

The ethical principles of the (HIM) professionals

There are four ethical principles used by HIM professionals: autonomy, non-maleficence, beneficence and justice. Autonomy is ensuring that the patient is coherent in order to make sound decisions on their own healthcare. Meaning that they are aware and acknowledge the side effects and outcomes that are possible. It also means that the patient came to a conclusion without

having been influenced to make a decision that they otherwise wouldn't have. Non-maleficence is the result of performing a procedure is going to have no harmful effects on the patient nor the ones performing the procedure. That the provider is not going to intentionally perform an operation or prescribe certain prescriptions knowing that the outcome is not for the greater good of the patient. Beneficence is when the healthcare being delivered is for the best outcome of the patient. It also requires that "health care providers develop and maintain skills and knowledge, continually update training, consider individual circumstances of all patients, and strive for net benefit" (Stanford University). Justice "seeks to ensure that the benefits and burdens of a policy are distributed evenly, or at least fairly, throughout the community" (Harman, pg. 250).

Saint Leo core values of integrity and excellence

When looking at health information technology, Saint Leo University's core values of integrity and excellence can be seen as a vital role that plays within this system. When looking at excellence, it is the "conscientious commitment" that is being made to the mission, vision and goals that have been set forth (Saint Leo University). That as a HIM professional it is important to learn all the necessary information and skills in order to perform the job at the highest standards. When looking at integrity, HIM professionals "pledge to be honest, just and consistent in word and deed" (Saint Leo University). That professionals have to ensure that they are staying committed to their patients and ensuring that they are receiving the quality care that they deserve. That they are not going to risk hurting their patients by exposing their privacy and always keeping their confidentiality.

References

- Harman, L. B. (2017). *Ethical Health Informatics*. [VitalSource Bookshelf]. Retrieved from <https://bookshelf.vitalsource.com/#/books/9781284114799/>
- HealthIT.gov. (2019, September 10). What is an Electronic Health Record (HER). Retrieved from <https://www.healthit.gov/faq/what-electronic-health-record-ehr>
- John Hopkins University. (2019). Health care fraud and abuse. Retrieved from https://www.hopkinsmedicine.org/johns_hopkins_healthcare/providers_physicians/health_care_fraud_and_abuse/
- OCR. (2019, April 19). Health Information Technology. Retrieved from <https://www.hhs.gov/hipaa/for-professionals/special-topics/health-information-technology/index.html>
- Office of Civil Rights. (2013, July 26). Summary of the HIPPA Security Rule. Retrieved from <https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html>
- Saint Leo University. (2020). History, Values and Catholic Roots. Retrieved from <https://www.saintleo.edu/history-values-catholic-roots>
- Stanford University. Medical ethics 101. (n.d.). Retrieved from <https://web.stanford.edu/class/siw198q/websites/reprotech/New%20Ways%20of%20Making%20Babies/EthicVoc.htm>
- Tank, Aytekin. (2018, April 30). Best Practices for keeping Patient Data Confidential. Retrieved from <https://healthitsecurity.com/news/best-practices-for-keeping-patient-data-confidential>

U.S. Department of Health & Human Services. (2013, July, 26). *Summary of the HIPPA Security Rule*. Health Information Privacy. Retrieved from <https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html>