Risks and Opportunities of the Electronic Health Data

One of the many crucial aspects of privacy extraction lies in the medical field where the use of electronic health data is rapidly increasing. Electronic health data is a breakthrough in information technology. It changes the way the health care providers do their jobs, it makes their procedures easier and more convenient by providing the patients with better services. However, to efficiently utilize these services, the providers need to collect and store the patients' personal information in many forms and by many ways. The use of the electronic health data is increasing because it "enhance[s] sharing of information among healthcare providers as well as enhance[s] communications between healthcare providers and patients/consumers" (Win 91). The most common way to manage patients' health data is through the electronic records. This creates a context for the debate about privacy when there are proofs that patients' privacy is being invaded more and more through the use of the electronic health data without them noticing. A question is raised: whether patients' privacy is worth sacrificing for the benefits coming from the uses of electronic records in healthcare?

To answer that question, it is necessary to know the specific benefits as well as the privacy concerns of the electronic records in healthcare and the trend in which these electronic records are adopted. There are two primary types of electronic records in healthcare: the electronic medical records (EMR) and the electronic health record (EHR). The EMRs are a digital version of the paper charts in the clinician's office that contain the medical and treatment history of the patients in one practice (United States). The EMRs are kept under the ownership of a single healthcare institution and can only be transferred to other institutions by printed out papers and delivered by mail. The EHRs are the same to the EMRs; they are used to perform all the tasks that the EMRs do with one advanced feature: upon the request of the patients, selected portions of their health information can be shared with other agencies (Thede). With these characteristics, the electronic records are being adopted widely by many healthcare providers for its benefits in diagnostic and treatment.

"Traditionally, the recording of patient health histories and patient care are performed through the use of paper medical records and charts" (Clarke et al. 65). All the procedures that take place during a patient visit to the clinic including check-in, diagnosing, and filling prescriptions are recorded and kept in paper forms. These records are then stored on shelves or in drawers and are not given to the patients when they change practitioners, making the patients build new medical records at the new facility. This causes many disadvantages in tracking, and maintenance. It is also a waste of time and complicates matters for the patients as they cannot remember their health information as they age. On the other hand, the EMRs and EHRs provide the providers and patients with many benefits. For the providers, the electronic records allow the providers to "track data over time; identify patients who are due for preventive visits and screenings; monitor how patients measure up to certain parameters, such as vaccinations and blood pressure readings; and improve overall quality of care in a practice" (United States). Electronic records improve the physicians' work as health information is typed into the computer and stored in computerized networks; this data can be accessed by many providers around the world via many devices such as laptop or tablets that are optimized for medical uses. For the patients, the electronic records allow them to keep track of their health data and carry the records with them to other health care providers. In additional to those benefits, the "adoption of EMR could [also] reduce America's $1.9 trillion annual health care bill by $81 billion through increased efficiency and safety" (Miller 2). The electronic records eliminate all the disadvantages of the paper records, it improves the health service critically by saving more time, providing better accesses to health care providers and patients, making the treatment procedure more efficient and reduce the government cost of health care. Therefore, the electronic records are important and critical for the future of United States' healthcare industry.

The benefits of the electronic records are undeniable and very attractive. However, this system also contains high risks of privacy invasion without notice of the victims. Once they are aware of the invasions, the consequences are usually unbearable. There was a real case where the electronic records could lead to serious medical identity theft. In 2008, Brandon Reagin's medical identity was stolen by a man named Arthur Watts. Watts then used this fraud medical identity to visit hospitals on several

occasions to treat kidney stones and an injured hand. This ran up nearly $20,000 in medical charges under the name of Reagin. After finding out what happened, Reagin not only needed to deal with the outstanding hospital bills, he also had problem with his medical records which Watts used for treatments that Reagin never received. If Reagin needs medical attention, those records could complicate his treatment and event cause harm (Andrews). As doctors and hospitals switch from paper-based records to electronic records, people will have more accesses to patients' sensitive medical information. The case of Reagin is an example of medical identity theft, one of the three main concerns of consumer privacy when it is linked to the use of electronic medical records. These concerns include: medical identity theft, privacy and integrity of health related data, and security breaches (Clarke et al.).

The first privacy concern is the risk of medical identity theft. "Medical identity theft is when someone uses another name or part of their medical history to obtain medical services or goods" (Clarke et al.). As in the example above, the impostor could use one's medical identity to obtain medical services. With the widespread adoption and implementation of EHRs, the patients' records are scattered among many different providers, and with the security breach the impostor could breach the system and steal other medical identities. The danger of this activity is that it could cause the victims to suffer unexpected cost of medical treatment. The health information of the thief will be mixed with the victims in the records; this will lead to fatal problems in their future treatments, giving the doctors incorrect health data (transfusion of the wrong blood type, for example). There is another undesirable outcome from the medical identity theft. The Health Insurance Portability and Accountability Act (HIPAA) states that a covered entity (the healthcare providers, for example), does not have to remove incorrect information. It can mark the information as incorrect and keep it as part of the health record (Clarke et al.). This makes the amendment for the records become difficult as the doctors will easily make mistakes if they do not read the records carefully and this also make it difficult for the right owner to comprehend and follow his records.

The second concern when using the electronic records is privacy and integrity of health related data. The integrity of health data is at risk for patients desire to keep their medical problem confidentially

to avoid embarrassment and prevent significant harms. For instance, employers may decide to discontinue employment or refuse to hire those who they fear may incur expense to them through health-related costs (Deapen 634). Or the health and insurance providers may track the applicants' medical history to accept or decline provision of coverage. With the development of electronic health data, it is easy for the employers and insurance providers to seek and eliminate unwanted excessive cost. As a result, "people are developing privacy-protective behavior to shield themselves from what they consider to be harmful and intrusive uses of their health information" (634). People will try to hide or withhold their medical information; they will be reluctant in providing fully information to the healthcare provider. However, by covering their health information, they accidentally face some unintended consequence such as poor quality care or incorrect diagnostic because the doctors are lack of complete and reliable information from the patients.

The third concern of privacy from using the electronic medical record is its technical safety. The use of EHRs required the doctors to upload the health records on a mutual network that several healthcare providers could access. There are approximately 150 people including nurses, clinicians, and billing clerks have access to at least part of a patient's medical record (Clarke et al.). More people with access to one patient's record will lead to higher chance for that record to be stolen. According to the Privacy Rights Clearinghouse, at least 34 million medical records have been stolen since January of 2005 (68). This raises a concern about the security of the EHRs in protecting the sensitive information.

Even though there are certain privacy concerns about the use of the electronic records, in recent years there has been an increase in the adoption rate of the electronic records. In 2013 according to the Accenture poll – which queried the health IT usage of 3,700 physicians in the U.S., Canada, England, France, Germany, Spain, Singapore and Australia, 93 percent of American doctors are now using the EMRs (Miliard). For the EHRs, in 2012, 44% of non-federal acute care hospitals had adopted at least a Basic EHR (United States). This represents a threefold increase in the EHR adoption rate since 2009. More physicians and healthcare providers in general tend to choose the electronic health record for its time and cost efficiency. Also, survey data shows that although Americans are concerned about the

privacy of medical records, the majority of Americans are aware of the benefits of the electronic records, they believe that the ability to share information can result in better care (Thede). The patients understand the risk of privacy intrusion but with the convenience and flexibility that the electronic records bring to them, they are willing to take risks to avoid waiting hours each time they visit their doctors or taking days to have the paper records mailed to them. The increase in the adoption rate of the electronic records and the survey data prove that their benefits outweigh the concerns about privacy.

Since the adoption of technology in improving healthcare service is essentially beneficial, and "the perceived boundaries of privacy seem to be retreating" (Kasper 91), people seems to undermine the privacy threats that are unseen and unknown and go for the benefits that are noticeable and come beforehand. The electronic records have certain concerns about safety, but as a matter of fact, neither the electronic record nor the paper records could guarantee 100% safety. This does not mean that efforts to protect healthcare data should be lessened. This means we need to acknowledge and consider possible security practices to protect the electronic health data that is on its way to integrate and improve more the people life.

Works Cited

Andrews, Michelle. "Medical Identity Theft Turns Patients into Victims." *Health.usnews.com.* U.S. News & World Report LP, 29 Feb. 2008. Web. 18 Nov. 2013.

Clarke, Irvine III, Theresa B. Flaherty, Stacy M. Hollis, and Mark Tomallo. "Consumer Privacy Issues Associated With The Use Of Electronic Health Records." *AHCMJ* 5.2 (2009): 63-73. *Proquest.* Web. 10 Nov. 2013.

Deapen, Dennis. "Cancer Surveillance and Information: Balancing Public Health with Privacy and Confidentiality Concerns (United States)." *Cancer Causes & Control* 17.5 (2006): 633-637. Web. 12 Nov. 2013.

Kasper, Debbie V.S. "The Evolution (Or Devolution) of Privacy." *Sociological Forum* 20.1 (2005): 69-92 *Jstor.* Web. 11 Nov. 2013.

Miliard, Mike. "EMR and HIE see big adoption numbers." *HealthcareITNews.* MedTech Media, 9 May. 2013. Web. 15 Now. 2013.

Miller, Amalia R,. and Catherine Tucker. "Privacy Protection and Technology Diffusion: The Case of Electronic Medical Records." Management Science, 55.7 (2007): 1077-93. Web. 10 Nov.2013.

Thede, Linda. "Electronic Medical Records Do Not Increase Identity Theft."*The Online Journal of Issues in Nursing* 15.2 (2010). *Opposing Viewpoints in Context.* Web. 12 Nov. 2013.

United States. HealthIT.gov. Adoption of Electronic Health Record Systems among U.S. Non-federal Acute Care Hospitals: 2008-2012. N.p.:n.p., March 2013. Web. 19 Nov. 2013.

---. *What is an Electronic Medical Record (EMR)?* N.p.: n.p., n.d. Web. 19 Nov.2013.

Win, Khin T., and John A. Fulcher. "Consent Mechanisms for Electronic Health Record Systems: A simple Yet Unresolved Issue." *Journal of Medical System* 31 (2007): 91-96. *Jstor.* Web. 17 Nov. 2013.