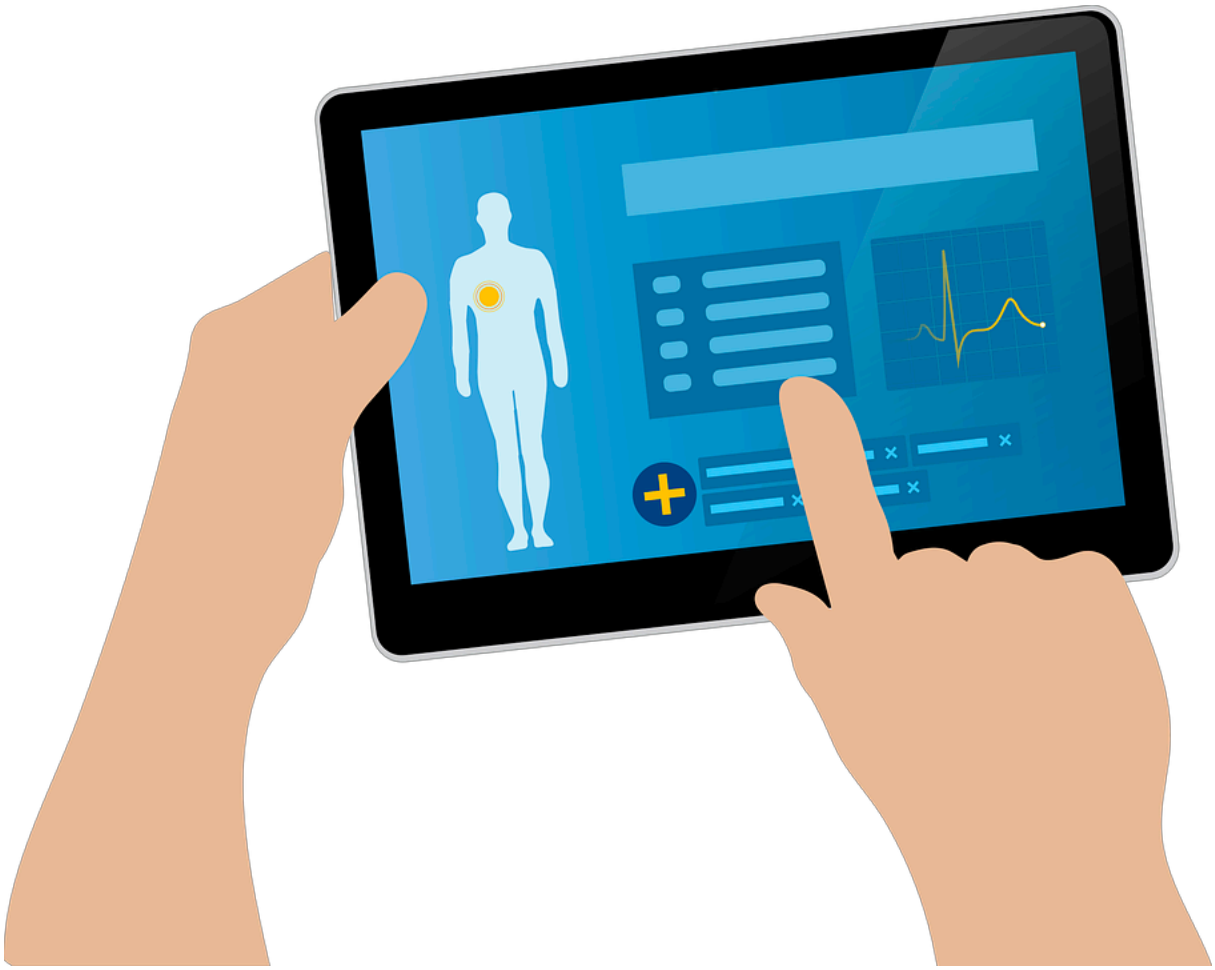
HEALTH|TECHNOLOGY

The Problems with Electronic Health Records

The short-comings of Electronic Health Records in physician-patient relations and data privacy concerns.

By Anika Jagow on April 13, 2019



https://pixabay.com/vectors/ehr-emr-electronic-medical-record-1476525/

Nervously shaking her leg, Susan fills out her first-time patient information on the space grey iPad in the waiting room. The screen prompts her to enter her personal information like name, birthday, medical history, insurance plan, and so forth. She, like so many others before her, quickly scrolls through the legal jargon and consent forms that ask her to read carefully before signing. Scribbling her signature, Susan taps done and hands the tablet back to the receptionist.

While Susan might not be a real person, this scenario plays out for thousands of patients in the United States everyday. Technology has changed the way in which we interact with doctors when we go for appointments, the way doctors interact with us in the examination room, and the way we interact with medical information. In this not so far fetched scenario, Susan has

acknowledged that her health records can be shared with other health-care providers without her being contacted and allowed her data to be anonymized for medical research.

BACKGROUND AND PROPOSED BENEFITS

Electronic Health Records (EHRs), collections of patient and population electronically-stored health information in a digital format, are the predominant way hospitals and local practices store patient information. In the past, health care providers kept information as paper records, which made it difficult for them to share records with other practices and patients to obtain old records. The old method was slow and inefficient; and patients would oftentimes have to wait for days and days to hear back about their results. EHRs promised to change all that.

Proposed major benefits of EHRs included improved patient treatment recommendations, communication between patients and physicians, and more data for medical research. In theory, they help with physician burnout since they allow physicians to spend more time on the patient, and quickly enter information on a computer once instead of having to scribble notes on a pad and transfer to a computer later. Additionally, patients have more immediate access to information a physician told them during an appointment, results from tests, and future appointments. An added bonus is that medical researchers now have access to way more data than they've ever had in the past. This means, they can more easily find correlations between patient symptoms and diagnoses and recommend personalized treatment options based on what worked well for other people with similar health issues. While these many benefits to EHRs do help to improve patient quality of care, there have been many unforeseen drawbacks like decreases in physician productivity, increases in data privacy concerns, and abuses in the medical data industry.

DRAWBACKS OF EHRS

https://cdn.pixabay.com/photo/2016/12/18/12/49/cyber-security-1915628_960_720.png
https://cdn.pixabay.com/photo/2017/11/21/10/19/icon-2967800_960_720.png

PHYSICIAN FEEDBACK

A survey conducted by The Physicians Foundation in 2018 asked nearly 9,000 physicians across the country what they disliked the most about the field: they responded with EHRs and lack of clinical autonomy. Looking into these responses, it seems that, in general, physicians feel like EHRs and technology are creating more boundaries between patients and doctors instead of following through with its promise of improving patient-doctor relations. So far, many of the EHR systems that have been created are clunky and unrefined, expensive to implement, and don't always increase productivity. A study released by University of California-Davis claims that physician productivity dropped by around 25-33% during the first few weeks of implementing EHRs. It's unknown how long it took for productivity to return back to normal levels.

DATA PRIVACY CONCERNS AND HIPAA

From a patient's standpoint, EHRs pose a threat to privacy. After hearing about huge data privacy leaks from big companies we've trusted in the past like Google and Facebook, we are becoming more concerned about what gets shared with the world over the internet and how our data is getting used. A survey conducted by the California HealthCare Foundation found that 69% of participants were "very concerned or somewhat concerned that an EMR system could lead to more sharing of your medical information without your knowledge" (Miller, 2009). This fear, at first glance, might seem unwarranted, but looking at current day regulations on EHRs, some serious reform is needed.

In 1996, the **Health Insurance Portability and Accountability Act of 1996** (HIPAA) was passed to ensure that we, as individuals, had rights over our own personal medical information. This law ensured that private medical records couldn't be shared without consent of the individual and should a data breach happen, they would be notified. HIPAA has been updated in recent years to address data security and mandate that hospitals implement EHR systems that at least follow a baseline standard for electronic data security. So then why is data security still a concern?

THE MEDICAL DATA INDUSTRY AND "DE-IDENTIFIED" DATA

https://cdn.pixabay.com/photo/2018/05/22/01/38/money-3420280_960_720.png

Current regulations allow medical records to be shared without patient consent as long as the data is anonymized. This way, data can be used for research and the advancement of the medical field. This type of data contains information that's been "**de-identified**" — meaning names of patients and doctors have been removed. As long as data has been de-identified, hospitals have the right to use it for their own purposes and/or sell it to third party sources. Data like this can be shared without a patient's consent, so it falls outside the purview of HIPAA, and is a major source of income for hospitals and third-party vendors since medical data is a hot commodity in the medical world right now.

While, in theory, this data is completely anonymized, recent studies have shown that it's not that difficult to re-identify de-identified data. By law, sellers are required to strip records of personal information like social security numbers, names, addresses, birthdays, and so forth. However, in order to increase the value of the data, companies create unique ids for a person that they use across the data sets they sell. For instance, John Doe's anonymized id number that will be used for all records concerning him is #123. By keeping this identifier consistent, it becomes easier to figure out that patient #123 is John Doe. This has been a known problem for a long time, and yet measures haven't been put in place to stop it. In a famous case in 1997, a Massachusetts Institute of Technology student, Latanya Sweeney, was able to find the current governor of Massachusetts' medical records. These records had been supposedly anonymized but without too much effort, she was able to find his information by looking at gender, age, and recent visits to his local hospital.

Even data that's supposedly going toward the betterment of society has the potential of being used for nefarious purposes. While yes, some de-identified data helps medical researchers make discoveries that benefit patients, other times it's used to help drug companies target patients and how they can get them to buy their product. The distinction between how the data is used is basically non-existent: third party sellers don't care what the data is used for, they just want the money.

WHY DOES THIS MATTER TO PATIENTS?

https://regmedia.co.uk/2018/03/02/shutterstock_data_thief.jpg?x=442&y=293&crop=1

Patients should be aware that information they tell their doctors, their medical records, pharmaceutical data, and more is getting sold in a multi-billionaire dollar industry without their knowledge. Additionally, this information, while technically stripped of their personal information, can be traced back to them without too much difficulty.

This poses a huge problem since with this data, people and employers can find out personal medical information that individuals would rather be kept private. We begin to lose the protections put in place by HIPAA and employers could start making hiring and promotion decisions based on this information they found off the books. Additionally, data thieves could use this data for extortion and medical identity theft: both of which could potentially harm our careers and future healthcare options.

ACCOUNTABILITY AND ACTION

http://iiblp.org/wp-content/uploads/2017/10/Hold-for-value-300x246.jpg

Many physicians, themselves, aren't aware of these grey-area data practices and don't realize that information they record during examinations is being sold to third party buyers. Similarly, most patients don't even realize that their "de-identified" data doesn't fall under HIPAA regulations, and other patients, like Susan from the example above, don't realize they're acknowledging that their data is being sold to third party vendors when they sign agreement forms.

Hospitals are well aware that they're profiting greatly from us without our knowledge and permission. Even our health insurance companies, oftentimes, receive a cut of the profit from de-identified medical data sales. We, as unknowing data providers, should either have the choice to share our data or, at the very least, receive part of the profit from the selling of our data. This data, after all, belongs to us so why shouldn't we get a say in how it's used and receive compensation for it?

EHRs, while have promised to improve the healthcare system, have ended up opening the healthcare system to a new wave of security and moral problems that it never had before. From decreased physician productivity to flagrant violations of patient privacy, the current EHR system needs an update, and fast. Physicians need to once again, feel in control and make

personal connections with their patients and patients need to feel like their medical information is safe and being used appropriately.

Sources

Carter, J. "Electronic medical records and quality improvement." Neurosurgery Clinics, 26(2), 245-251. n.p.: n.p., 8 . 6 Apr. 2019.

Evans, R. "Electronic health records: then, now, and in the future." Yearbook of medical informatics, 25(S 01), S48-S61. n.p.: n.p., 9 . 6 Apr. 2019.

Miller, A and C Tucker. "Privacy Protection and Technology Diffusion: The Case of Electronic Medical Records." Management Science, 55(7), 1077-1093. n.p.: n.p., 2 . 6 Apr. 2019. <http://www.jstor.org.ezproxy.neu.edu/stable/40539198>.

Palma, G. "Electronic Health Records: The Good, the Bad and the Ugly." George Palma, MD, Medical Director, of Simpler Consulting, discusses benefits and draw backs for electronic medical records. n.p.: n.p., 14 Oct. 2013. 6 Apr. 2019. <https://www.beckershospitalreview.com/healthcare-information-technology/electronic-health-records-the-good-the-bad-and-the-ugly.html>.

Sharma, R and R Sharma. "The Privacy Myth of De-Identified Medical Data." n.p.: n.p., 2 Oct. 2017. 6 Apr. 2019. <https://medium.com/healthwizz/the-privacy-myth-of-de-identified-medical-data-10b9678e4bea>.

Tanner, A. "How Data Brokers Make Money Off Your Medical Records." n.p.: n.p., 1 Feb. 2016. 6 Apr. 2019. <https://www.scientificamerican.com/article/how-data-brokers-make-money-off-your-medical-records/>.

"The Physicians Foundation." n.p.: n.p., n.d.. 6 Apr. 2019.

Torrey, T. n.p.: n.p., 5 Nov. 2018. 6 Apr. 2019. <https://www.verywellhealth.com/who-has-access-to-your-medical-records-2615502>.

Reflective Note:
I decided to write an opinion piece article that could be found in a magazine. It's supposed to give background information and then go into what I think should happen in the industry. Throughout the piece, I think a lot of the information given is very biased. I decided to cite my sources in MLA because that's common in the art and humanities field. I decided to break up the article into different sub categories and start out with a fabricated story about "Susan." The reader is supposed to be able to put themselves into Susan's shoes and maybe be reminded of a time they did the

same thing while waiting for a doctor's appointment. Additionally, I sometimes used phrases like "we interact" and "we access" in order to be more relatable and make it sound like this is something that affects us all and we can all relate to. I picked this more fun graphics because in a lot of web articles, they have colorful graphics instead of photos. I don't think photographs would be super helpful and the graphics helps grab the reader's attention.

I don't think this would fit into my professional portfolio since for my major, employers care more about personal side projects that are coding related.