An Analysis of Electronic Health Records in America from a Utilitarian Framework

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science

University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree

Bachelor of Science, School of Engineering

Austin Campbell

Spring 2024

On my honor as a University student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Advisor

William J Davis, Department of Engineering and Society

"What, then, is the government? An intermediary body established between the subjects and the sovereign for their mutual communication, a body charged with the execution of the laws and the maintenance of freedom, both civil and political."

"As soon as any man says of the affairs of the State "What does it matter to me?" the State may be given up for lost."
— Jean-Jacques Rousseau, The Social Contract

Introduction

Swiss-born French philosopher Jean-Jacques Rousseau states in his idea of the social contract that individuals give away partial rights to their government in order for their government to protect and serve their interests as a collective society (D'Agostino et al, 2024). But what happens when the government supposed to uphold their end of the bargain fails to do so, and instead the systems that are put in place are detrimental to the medical privacy of the people they are supposed to be protecting? The US healthcare system today would be Rousseau's worst nightmare come to life, as everyday citizens find themselves disadvantaged by a medical record system not built to support their own needs, interests, and privacy, but that to bolster the pockets of those at the top.

Conflicting interests between the healthcare system and the public have long existed, but at what point is enough when faith in the system seems questionable at best as a poll of independent voters in 2019 showed that 90% of them believe that the current healthcare system should be improved or replaced (Quinnipiac University Poll). From 2005-2019 there were close to 250 million people affected by healthcare data breaches, with over 60% of these cases just in the last five years of that stretch alone (Seh et al, 2020). As the electronic records system keeps expanding, it is important to mitigate these data breaches that harm millions of people every year. Currently, the medical community is split between the ethicality and security of the digitization and sharing of medical records. Professor William Price II of the University of

Michigan Law School and Professor I. Glenn Cohen of Harvard Law School attempts to weigh these ethical and legal limitations that come with medical privacy in the age of "Big Data" and potentially fix problems with the regulation of such systems (2019, p.37). According to Cohen and Price, digitization of medical files has led to "increased accountability, quality, efficiency, and innovation" but inevitably at the risk of more generated patient data and thereby more privacy risks (2019, p.37). The question arises at what moral grounds should the system stand upon?

To answer this question of weighing the risks and rewards of such a system, I will explore the benefits and pitfalls of the expansion of electronic health records (EHR) through numerous papers and literature reviews and then apply a utilitarian point of view to the problem. Utilitarianism is a form of consequentialism that can be put simply as the moral choice that maximizes the overall total 'good' for the most people (Driver, 2022). Additionally, I seek to understand the current loopholes that the legislature has failed to address in order for the betterment of security concerns regarding EHR and online medical databases as a whole. In this paper I argue that the continued use of EHR will advance the healthcare system in terms of accountability, speed of care, and accessibility, but the legislature in place requires change in order to secure the cost of patient privacy and shore up technical and privacy limitations that come from the expansion of the EHR system. This conclusion comes from examining from a utilitarian lens ethical and literature reviews of the use of EHR within the medical community as well as loopholes that have been exposed in the legislature protecting the people.

Background

Traditional health records have begun the move from the standard locker and manila folder in the basements of hospitals and insurance companies to a switch to immense collections

of personal data all stored and shared on digital clouds since the beginning of the 1960's when the technology was first in its infant stages (Gariepy-Saper and Decarie, 2021, p.74). The importance of such a system was first brought to national attention in 2004 with the State of the Union Address as President Bush stated that the creation of EHR would help "avoid dangerous medical mistakes, reduce costs, and improve care" for the people of the United States (Washington Post, 2004). Again, in a 2009 bill EHR were mandated for use in hospitals that treated government-insured patients, which is a tremendous thing as the ease of EHR delocalization is that it permits for quick access from entity to entity that require use of the EHR (Atherton, 2011, p.188).

Tracy Gunter, MD and Nicolas Terry, LLM sought to explore the initial expansion of EHR architectures in 2005 by addressing potential models and the associated risks of developing such a system. Their conclusion was that the benefits of the creation of EHR databases were undeniable and expansive as it allowed for instantaneous delivery to any medical site that was required, but the development of this system also came with inherent risks to the people that it sought to help in the form of developmental costs, privacy concerns, and litigation risks (Gunter and Terry, 2005). This is a common problem for everyone now in the age of technological advancement as everything in our lives is being quantified and stored somewhere in a large bank of personal information that are "massive targets for attackers" (Curran, 2023, p.7). This mass data collection for population research of course has its benefits and drawbacks, and the ethicality of such a system can be brought into question, but the main target of this paper is specifically in the privacy of EHR and the legislation in place to protect the people from risks in the system that could be exploited (Aitken et al, 2018). For EHR collections to be most effective, it will have to come at the cost of putting patients at the risk of exposure to security breaches and

other unethical ways to obtain an individual's EHR, but these risks should be measured and weighed against the benefits of the system (Gariepy-Saper and Decarie, 2021, p.82).

The question resides on what metrics this justification between the privacy risks associated with EHR for millions of American citizens and the benefits that those exact EHR present to the future of medicine. Kitty McClanahan, PhD, is an assistant to the director in the School of Information Sciences at the University of Tennessee and wrote extensively on the topic of privacy in her research paper titled "Balancing Good Intentions: Protecting the Privacy of Electronic Health Information" that explored how to weigh privacy concerns with the overall betterment of the health system. McClanahan describes how the benefits of EHR could save thousands of patient lives in the emergency wings of hospitals each year as less medical errors are made because of the ease of access for the flow of information (2008, p.76). Meanwhile the risks of EHR systems are in terms of large-scale privacy breaches and improper disclosures to non involved entities and not the factor of human lives (McClanahan, 2008, p.72). The difficulties of perfecting the EHR system in America reside in how there is not a clear best solution to standardizing the protection of privacy for everyday citizens as private vendors predominately control the market selling directly to doctors and patients (Dinh-Le et al, 2019). This also complicates matters as Google and Microsoft sell personal health record (PHR) details to partners and back to patients with no standard level of security (Jones et al, 2010, p.246). There needs to be a standard for the level of security that EHR systems have in place as well as increased legislation on the sharing of the information as small and isolated EHR systems would not need the ability for as much ease of access as a EHR reliant on society would.

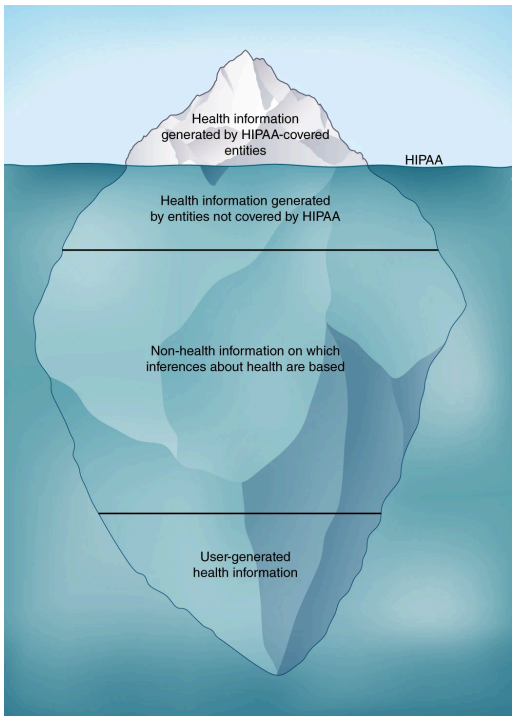
The most important documentation in the field of medical privacy is the Health Insurance Portability and Accountability Act (HIPAA) as it "established national standards, forms, and

protocols" for the distribution of EHR (McClanahan, 2008, p.72). Under HIPAA health care providers, insurance companies, and their business associates are prohibited from using or disseminating protected health information (PHI) except in a list of specific conditions (Cohen and Price, 2019, p.39). HIPAA has many problems built into it such as an inconsistent level of scrutiny for privacy and being too overprotective in some areas as well as underprotective with others (Eisenberg and Price, 2017, p.35). One example of this is how HIPAA's most important strategy for protecting patient privacy from breaches is removing specific identifiers from PHIs like names and emails, however deidentified data may become identifiable through other datasets through 'data triangulation" (Philibert et al, 2014). This problem exists purely because of significant recent advances in data science as companies sharing and selling data that they view as deidentified and following HIPAA guidelines are no longer truly doing so as effectively de-identifying PHIs is almost impossible with present technology. The significant problem lies in the fact that when Congress enacted HIPAA in 1996 it was focused just on EHR data and the entities it could predict would use it, but as big-data has grown the data from entities covered under HIPAA are just a small part of a global conglomerate of data collection (Cohen and Price, 2019, p.39). HIPAA does not protect the privacy of generated data with entities that were not around in the beginning of its conception such as people and products that are not the patient, smartphone apps, online searches, or even shopping history at a local pharmacy (Riley, 2018). HIPAA has not had any significant updates in the last 20 years and when it was enacted was originally for paper based information and before digital health tools (Theodos and Sittig, 2020, p.7). An expansion of HIPAA and clearer regulations regarding the numerous new methods of data collection and generation are needed as the privacy of everyday citizens are being exploited

by technological innovations that were not foreseen as possible risks in the past. A visualization of the medical data covered and not covered is presented in Figure 1.

Figure 1

Data Covered by HIPAA



Note. The data that is and isn't included in HIPAA symbolizing the information above the water being the data covered by HIPAA and below the water is not (Cohen and Price, 2019, p.39).

With certain companies claiming to be able to provide health information on more than 300 million Americans, it is more important than ever to shore up some of these lapses in the protection that HIPAA covers as most patients remain in the dark about how their data is managed, used, and transferred (Krumholz, 2023). The health data of today has been expanded from just traditional health information to now extrapolating hypothetical data points from individuals by cross referencing across many different datasets and potential indicators for the betterment of the companies amassing these data points for commercialization and personal use. The way the system needs to be adjusted must be done by taking a holistic look at the current

state of the system and the easy flow of information between associated parties who the patient could never be aware of that has their data. This can only be done by looking at the legislation in place and the current state of electronic privacy transmission of PHI as well as taking a moral approach and weighing the benefits to society and the inherent risks that such a system imposes on the individual patients.

Methodology

The methodology of this paper was formed from an adaptation of previous research methodology conducted during a literature review of the ethicality of EHR's and research performed by Gariepy-Saper and Decarie in their 2021 study. Their rationale for the methodology stemmed from finding a list of sources that contained two distinct categories of topics, confidentiality and electronic health records, including words that were synonymous for both (Gariepy-Saper and Decarie, 2021, p.75). Additionally they narrowed their search range only from papers published from 2005-2020 as 2005 was when EHR began to receive national attention, and limiting the sources to the last five years they deemed would ignore the time complexity of the issue (Gariepy-Saper and Decarie, 2021, pp.75-6). From their rationale I adapted my own which was to search primarily for scientific and peer reviewed papers that had one of three distinct features published in a similar year range of 2005-2024.

The first distinct focus was on papers with an emphasis on the current state of electronic health records systems with an adoption of electronic data storage and collection. This was to better grasp the present situation of the current system as well as to determine what current benefits and potential pitfalls such a system poses for users of all demographics. The second focus were papers that questioned the ethicality of such a system as the one that is currently implemented, in order to gain a more holistic perspective on how different entities in the field

viewed the topic as well as their own arguments and rationales for their perspectives. The last focus was on papers that addressed the current legislation regarding these systems in order to understand what currently is in place and how companies can jump through loopholes in order to address the problem areas with the ways things are currently being handled.

To implement this process I applied the search criteria to seemingly more general papers to get a better working knowledge of the current state of things. After getting a decent grasp on how EHR were being utilized and the controversy surrounding them I looked for more specific papers, both research and arguments on ethicality, that addressed one (or more) of the three key highlighted areas. Specifically, I dove into the sources of these papers in order to find more specific arguments and information that these research papers were drawing from that could improve my own knowledge and therefore argument. After researching the papers and being satisfied with my understanding I formed a preliminary argument from a utilitarian framework and understanding of the current state of the system with a focus in mind of the combination of the three highlighted fields that I chose to give myself more comprehensive knowledge of the problem.

The first paper I looked into was a literature review conducted by Katherine Gariepy-Saper and Nicholas Decarie that won the 2020 JSCHLA Student Paper Prize awarded for the best unpublished paper on health sciences. The review was helpful mainly for the first key topic of outlining the history and current state of the EHR system as well as providing a successful methodology to build my own off of when finding papers and articles with specific criteria. They identified four key themes in their review surrounding the EHR system: the benefits of such a system, the patient privacy concerns, the technological advancement to shore up EHR privacy, and the implications over ownership with record to EHR (Gariepy-Saper and

Decarie, 2021, pp.77-80). Additionally, the paper outlined the pitfalls of EHR systems and the conclusion of acknowledging the inherent risks but also praising the benefits (Gariepy-Saper and Decarie, 2021, p.82).

The second paper I looked into was that of Cohen and Price, of Harvard Law and Michigan Law, respectively. The paper outlined the legal and ethical challenges that big data brings in terms of privacy and had a general focus on my second key search criteria which was outlining the ethicality of the current EHR system (Cohen and Price, 2019, p.37). More specifically it highlighted how big data was being used in healthcare but also how to think about health privacy in both consequentialist and deontological ways. Consequentialism is the view that the morality of actions depends only on the consequences of the actions (Sinnott-Armstrong, 2023). Utilitarianism, the framework I chose, is a subset of this. The consequentialist concerns regarding EHR revolved around the negative outcomes and affecting the person whose privacy has been breached (Cohen and Price, 2019, p.38). Deontology on the other hand is an ethical approach in which the morality of actions arise from universal rules and principles and is considered the foil to consequentialism (Alexander and Michael, 2021). The deontological concerns revolved around the fact that privacy concerns exist whether or not a person's data breach resulted in it being used against them, or if they were aware their privacy had been violated and the issues arise with the lack of overall protection (Cohen and Price, 2019, p.38). This paper was helpful in exploring different ways that the ethicality of such a system can be thought of, and provides two examples of ethical frameworks. As stated previously, I chose to use a utilitarian framework on this issue which takes into account all of the repercussions of EHR records and weighs them with the benefits such as speed, accountability, and ease of use (Driver, 2022).

Kitty McClanahan of the University of Tennessee explored the last theme of my search criteria in her paper on balancing the good intentions of EHR and how to more robustly protect EHR. She both covered the current state of the EHR legislation but more specifically outlined the importances of HIPAA in her exploration of the relevant sections of HIPAA as well as the current implications. She provided recommendations to improve HIPAA and was a great source to pull from as her paper, written in 2008, outlined what problems existed all the way back then in order to contrast with how certain problems could still be perpetuated today in other forms.

All three of these key papers covered my three key search criteria but more importantly allowed me to expand my sources and pull from the information that they found in order to gain a more holistic understanding of the situation. The framework and approach that I employed rely mainly on finding specialized information on the three main fields of: electronic health records as a whole, arguments of the ethicality of the system in place, and what the current legislation is. These three areas were chosen because of the importance they would provide in order to build a foundation upon any opinions and recommendations I would have. By finding specific papers that focused on expanding my own knowledge on one of these three areas I was able to build my knowledge and also see how other individuals perceived things from their side. Diving deeper into these paper's sources and the background for their motives provided some context from which the authors were coming from as well as seeing where they were getting their information.

Analysis

The widespread use and expansion of the EHR system in America has benefited the public a tremendous amount in terms of the advancements it has had for the healthcare system such as improvements in accessibility and efficiency (Atherton, 2011, p.188). When considering a utilitarian perspective, it is apparent that even with drawbacks such as privacy abuses, general

data collection, and privacy breaches they still contribute more for public betterment than not (Gariepy-Saper and Decarie, 2021, p.82). Currently, the benefits of the EHR system offset the negative consequences to contribute to benefits for healthcare workers and Americans in general, however it might not always be that way. It is apparent that there needs to be significant overhaul in terms of legislation and specifically on ensuring HIPAA can stand up to the type of scrutiny that the future of technology and data collection will provide (Theodos and Sittig, 2020, p.2). Such changes are needed in order to better secure the information in the EHR system, improve patient consent and privacy, and restrict specifically who can access or collect EHR information. Currently, technology is expanding at a rate that the legislature can not keep up with after the fact and securing EHR information is a necessity (Theodos and Sittig, 2020, p.7).

This change in the privacy legislature needs to be a preemptive one rather than reactionary, even if it is partially counterproductive to the efficiency of the EHR system it is vital to protect individuals in the long run (Theodos and Sittig, 2020, p.7). A key example of this is the paper on data triangulation of HIPAA's 18 key identifiers and how the individual medical records could still be predicted back to specific individuals (Philibert et al, 2014). As the abilities of data analytics grows the need to mitigate potential breaches and expand HIPAA and legislation to better safeguard the system is an absolute necessity. In the same way you would need better locks to secure bigger safes, the information present in EHR systems is ripe with information that needs to be protected in terms of IT security but also legislative backing (McClanahan, 2008, p.78). Additionally, while mostly everyone is having their data collected in some form or another there needs to be more awareness from the American public about who can use and access EHR information legally as well as additional consent requests before sharing with new entities. This red tape may reduce the efficiency of EHR systems but is a positive step

toward a more conscientious and protected public for the long run. As well, more consent and restrictions regarding the sharing of information between companies that are tangentially related are needed and that can be solved by simple expansions of HIPAA to clearly define what is and what is not acceptable under conditions (Cohen and Price, 2019, p.39). Overall, the ethicality of the EHR system remains firm from a utilitarian perspective as it does contribute more to the overall benefit of society, but legislation needs to change to further protect EHR systems, PHI's, and most importantly Americans (Gariepy-Saper and Decarie, 2021, p.82).

There are always going to be risks with how we store our most private information, technology can be breached, safes can be broken into, even sharing with one singular person can be spread. Growing connectivity and accessibility can't and shouldn't be stopped even if the growth of technology will always be followed by the presence of unforeseen risks. What should be done is most effectively overhauling the system that we have to protect the most amount of people's privacy, even if it seems overprotective it is better to err on that side than that of risk. At the end of the day the use of technology with EHR systems has been able to tremendously advance our healthcare system but will always come with risks to our data and personal privacy (Cohen and Price, 2019, p.37). The job of the legislature is to mitigate those risks even if a bit over restrictive in order to best protect the people.

Conclusion

Based off of the evidence presented specifically with regard to the literature review conducted by Gariepy-Saper and Decarie, the analysis by McClanahan of HIPAA, and the ethical study by Cohen and Price it is apparent that the need for EHR systems exists, is ethical from a utilitarian perspective, but HIPAA and legislation need to more effectively protect the

information. Legislation needs to be expanded in order to fully encompass the growing needs of privacy such as information security and protecting the dissemination of information. The implications of this are that of the importance of securing our EHR system and changing the legislature to more reflect the growth of data protection and analytics. Practical applications come from an analysis of HIPAA and the shortcomings in terms of privacy and changing legislation to better protect individuals PHI. Limitations of this work arise mainly from the subjectivity of justifying a system based on utilitarianism and maximizing the greatest good for the most people. Additionally, the study from McClanahan simply highlighted the deficiencies in HIPAA during the mid 2000's in order to apply them today, and a more comprehensive understanding of the nuances of HIPAA and EHR systems would be needed in order to change legislation. I would like to make an acknowledgement to all the researchers and their studies that I based this paper off of, specifically Gariepy-Saper and Decarie who I based my research methodology on.

References

Aitken, M., Porteous, C., Creamer, E., & Cunningham-Burley, S. (2018). *Who benefits and how? Public expectations of public benefits from data-intensive health research*. Big Data & Society, 5(2). https://doi.org/10.1177/2053951718816724

Alexander, L & Moore, Ml. (Winter 2021). *Deontological Ethics*. The Stanford Encyclopedia of Philosophy, Edward N. Zalta (ed.) Retrieved from https://plato.stanford.edu/archives/win2021/entries/ethics-deontological/

Atherton, J. (2011, March). *History of medicine: Development of the electronic health record*. Virtual Mentor, 13(3), 186-189. https://doi.org/10.1001/virtualmentor.2011.13.3.mhst1-1103

Curran, D. (2023). *Surveillance capitalism and systemic digital risk: The imperative to collect and connect and the risks of interconnectedness*. Big Data & Society, 10(1). https://doi.org/10.1177/20539517231177621

D'Agostino, F., Gaus, G., & Thrasher, J. (2024). *Contemporary Approaches to the Social Contract*. In E. N. Zalta & U. Nodelman (Eds.), The Stanford Encyclopedia of Philosophy (Spring 2024 Edition). Retrieved from https://plato.stanford.edu/archives/spr2024/entries/contractarianism-contemporary/

Deontology. Oxford Reference. Retrieved 24 Apr. 2024, from https://www.oxfordreference.com/view/10.1093/oi/authority.20110803095711126.

Dinh-Le, C., Chuang, R., Chokshi, S., & Mann, D. (2019, September). *Wearable health technology and electronic health record integration: scoping review and future directions*. Journal of Medical Internet Research, 7(9), e12861.

Driver, J. (Winter 2022). *The History of Utilitarianism*. The Stanford Encyclopedia of Philosophy, Edward N. Zalta & Uri Nodelman (eds.) Retrieved from https://plato.stanford.edu/archives/win2022/entries/utilitarianism-history/

Eisenberg, R. S., & Price, W. N. II. (2017). *Promoting healthcare innovation on the demand side*. Journal of Law and the Biosciences, 4, 3–49.

Gariépy-Saper, K., & Decarie, N. (2021). *Privacy of electronic health records: a review of the literature*. The journal of the Canadian Health Libraries Association, 42(1), 74–84. https://doi.org/10.29173/jchla29496

Gunter, T. D., & Terry, N. P. (2005, January). *The emergence of national electronic health record architectures in the United States and Australia: Models, costs, and questions*. Journal of Medical Internet Research, 7(1).

Jones, D. A., Shipman, J. P., Plaut, D. A., & Selden, C. R. (2010, July). *Characteristics of personal health records: Findings of the Medical Library Association/National Library of Medicine Joint Electronic Personal Health Record Task Force*. Journal of Medical Library Association, 98(3), 243-249.

Krumholz, H. M. (2023). *In the US, patient data privacy is an illusion*. BMJ, 381, p1225. https://doi.org/10.1136/bmj.p1225

McClanahan, K. (2008, February). *Balancing good intentions: Protecting the privacy of electronic health information*. Bulletin of Science, Technology & Society, 28(1), 69-79.

Philibert, R. A., et al. (2014). *Methylation array data can simultaneously identify individuals and convey protected health information: an unrecognized ethical concern*. Clinical Epigenetics, 6, 28.

Price, W. N., & Cohen, I. G. (2019). *Privacy in the age of medical big data*. Nature Medicine, 25, 37–43. https://doi.org/10.1038/s41591-018-0272-7

Quinnipiac University Poll - California. (2019). *In general, would you prefer to improve the current healthcare system in the United States, or would you prefer to replace the current health care system in the United States with something new*? Accessed October 26, 2023, from https://ptn.infobase.com/articles/UG9sbFF1ZXN0aW9uOjc0MTYwNQ==?aid=98131

Riley, M. F. (2018). *Big data, HIPAA, and the common rule: time for a big change*? In Big Data, Health Law, and Bioethics (Eds. I. G. Cohen, H. Fernandez Lynch, E. Vayena, & U. Gasser). Cambridge University Press: New York.

Rousseau, J. (1968). *The Social Contract*. Baltimore, MD.: Penguin Books. Retrieved from www. academia.edu

Seh, A. H., Zarour, M., Alenezi, M., Sarkar, A. K., Agrawal, A., Kumar, R., & Khan, R. A. (2020). *Healthcare Data Breaches: Insights and Implications*. Healthcare (Basel, Switzerland), 8(2), 133. https://doi.org/10.3390/healthcare8020133

Sinnott-Armstrong, Walter. (Winter 2023). *Consequentialism*. The Stanford Encyclopedia of Philosophy, Edward N. Zalta & Uri Nodelman (eds.) Retrieved from https://plato.stanford.edu/archives/win2023/entries/consequentialism/

Theodos, K., & Sittig, S. (2020). *Health Information Privacy Laws in the Digital Age: HIPAA Doesn't Apply*. Perspectives in health information management, 18(Winter), 1l.

Washington Post (2004). *President Bush's 2004 State of the Union Address*. Washington Post . (2004, January 20). https://www.washingtonpost.com/wp-srv/politics/transcripts/bushtext_012004.html