Privacy and Security of Electronic Health Records

Brian P. Hogan

IST618 – Information Policy

Syracuse University

2020

Author Note

This paper prepared for Information Policy taught by Professor Ian MacInnes, Ph.D.

Background

Privacy and security surrounding Electronic Health Records (EHR) provide an array of challenges ensuring the safety of patient records while record updating and sharing is performed on all categories of these highly sensitive records. Complex security algorithms are continually challenged with the growth of machine learning algorithms putting pressure on governments and the private sector to ensure client confidentiality. This requires providing a system that is increasingly cost effective, secure, and resilient to data mining efforts to help provide higher standards of care and confidentiality to all patients. There are clear advantages and disadvantages in gathering and managing health information but there are fundamental ethical dilemmas faced by both government and private sectors. The following assesses this landscape and reviews policy adjustments to help broaden ERH's transparency amongst individuals, and government institutions responsible for EHR accountability and best practices.

Advantages and Disadvantages of Electronic Health Record Information

The American Reinvestment and Recovery Act of 2009 (ARRA) was a stimulus package in response to the American recession providing an array of federal statutes to save jobs and devoted more than $19 billion to improve the healthcare records infrastructure. According to USFHealth, a key component was creation of a "meaningful use" healthcare digital record while maintaining privacy and security of patient information (USFHealth, 2020). Quality medical data "improves epidemic surveillance, decreases the length of patient stay, achieves work efficiency by reducing nonvalue added activities…and helps to make for timely decisions at reduced cost" (Adane, Gizachew, and Kendie, 2019, pg. 67). An ultimate advantage is achieving interoperability amongst health care institutions facilitating "medical staff's understanding of the disease, diagnosis, and decision-making process" (Adane, et al., 2019, pg. 70). Large scale medical research is another advantage of EHR structured data (Cowie, et al., 2017). Natural language processing (NLP) can be applied to free text note fields containing rich information and when associated with medical codes can lead to valuable insights across larger patient populations.

Disadvantages of EHRs are varied focusing around protected health information. While great efforts have been invested in securing medical information there is no single solution or automatic classifier available to administer this complex process across EHR subtypes. When large, or very large, EHR corpuses are accumulated adversarial machine learning has been found effective de-anonymizing data and re-identifying owners when combined with other publicly available information resulting in unforeseen privacy violations. According to Friedrich, Kohn, Wiedemann, and Beimann's research, anonymizing methods need word classifier enhancements with more stringent "aggressive vectorization," such as coding of a 25-year old person as "25" and "yo" (2019). Without such detailed parsing advanced machine learning, such as Python's deep learning *Keras* framework, can match "25yo," plus other patient chart characteristics, with public records such as birth data, to deanonymize records. With the research community performing a form a privacy self-regulation speaks to the need for government to consider embracing a clearer set of rules to help regulate such findings.

According to Swire, market imperfections regarding privacy protection vary and the "size and type of compliance costs is the degree of precision in the regulation" (1997, pg. 6). As medical privacy research is able to assess discrete actions health-care organizations can embrace regulation and structure rules resulting in increased compliance benefits for data owners. It is not necessarily a government failure when private companies are deploying effective anonymizing methods but government policy needs to allow for technology improvements. Swire reviews the benefits of market self-regulation as industry members want to promote the "reputation of the industry as a whole" (Swire, 1997, pg. 8). Even though industry leaders may have the best intentions technology advancements can put an entirely different spin on desired outcomes limiting the effectiveness of self-regulation without stringent technical standards oversight.

In summary, EHR interoperability is paramount for helping healthcare achieve cost reductions across delivery platforms but governments reliance on the private sector to self-regulate privacy concerns is questionable. Privacy concerns require EHR systems that can improve care diagnosis and delivery without compromising patient trust by establishing reliable and scalable medical information management systems.

Concerns and Ethics Surrounding Electronic Health Records

Privacy concerns on EHRs include accessing records on public computers and a user not properly logging off, printed patient records lost or dropped in a public spaces, inappropriate faxing or mailing of records, and possibly divorcees who gain access to a spouse records, such as blood test results, for use in litigate purposes. Other EHR privacy concerns focus around the potential for discrimination. According to Garcia-Murillo and MacInnes, "a primary reason people are concerned with their privacy is that we are afraid of being discriminated against" (2014, pg. 17). Use of medical record information in legal affairs, or perhaps even as a form of insurance discrimination, is of great concern for all citizens. With insurance coverage and rates being under continual review sharing of certain medical information, such as substance abuse, may lead to unfair scrutiny or "rate" judgment on a person's healthcare. On the other hand perhaps society should encourage sharing data on mistakes (Garcia-Murillo and MacInnes, 2014). Whatever the case healthcare information draws a very sensitive line that when crossed both personal and negative consequences flourish.

In my ways the growth of EHR fosters a "collect it all" mentality and Schneier, a digital privacy expert, cautions that without technologists as part of the policy planning process both the government and private sector may not have the proper tools to facilitate and ensure privacy (Schneier, 2017). Given the research around EHR data re-identification and gaps associated with assimilated knowledge perhaps machine and deep learning may require a new regulatory agency to help manage advanced programmatic findings. Machine and deep learning technology are complex technologies, require significant training and scientists with aptitudes across several disciplines such as statistics and data warehouses. Production environments are also subject to automation resulting in an incremental loss of human oversight. Considering such facets perhaps the healthcare world is in a EHR world-size autobot nascent state. According to Schneier, perhaps a balance of disconnected systems is required (2019, pg. 8) unless health data can be encrypted without limiting interoperability. In agreeing with Schneier, concern should be placed on government's management of health privacy information because while research is a notable endeavor vast storage of citizen biometric specifications, and their continued health changes, doesn't seem something a United States founding father would support harvesting.

Enabling values, such as health and education, are critical to support health equity initiatives (Schultz, 2006, pg. 8). EHR platforms advance societal transformation and promote justice by deepening an individual's social contract as described by John Rawls (ibid, pg. 9). While EHR research findings should expand an equality of opportunity by growing the health population of *best off from worst off* it is not without its ethical dilemmas (ibid, pg. 10). An *a priori* existence of an EHR system obligates new community individuals to embrace a technological mechanism they are not able to object to (Garcia-Murillo, M., 2020).

Electronic Health Records Policy Recommendations

According to Dinev, Hart and Mullen, American society is surveillance oriented and such perceptions have strengthened since Edward Snowden's 2008 revelations (2008). Policy surrounding EHR would benefit with specific data encryption methods and algorithmic techniques found most effective maintaining patient confidentiality. According to Hannah, the company Google envisions being able to save your life with a person's known or unknown information, such as machine learning projections of cancerous cell growth patterns derived from thousands of patients of varying age and race (2020). Implications are clear that any public and private patient EHR information harvested from whatever source will no longer be lost in physical basement files stored in abandoned hospitals. Old data and new data, such as fitness wristwatch or heart monitors, are connected on the internet of things (IoT) and the data is now a hot commodity, like corn or soybeans, awaiting stock exchange market pricing.

Privacy policies need to tailor how health care information can be transacted with customer feedback loops notifying them when, where and how their biometric information is consumed. Currently privacy "fails to convey a sense of urgency needed to address the serious health privacy consequences of comprehensive and longitudinal records" (Rothstein and Tovino, 2019, pg. 775). Privacy needs to re-establish this urgency to help mitigate drawbacks centering on this costly administrative oversight. Ensuring compliance is expensive but can be offset by providing a transparent privacy ownership platform governed by a central managing structure.

Conclusion

A patient's ability to access their electronic health records provides an opportunity to review their care from each visit fostering health ownership and greater engagement with care providers. This speaks to the importance of EHR portals helping patients become an active participant in their healthcare and expanding health equity across diverse patient populations. Moving forward, health-care technology need to continuously improve technology platforms enabling EHRs interoperability. Achieving interoperability, protecting health information, and providing secure data structures will help providers and researchers discover novel insights with machine learning technologies advancing health equity.

Word Count: 1491

References

Adane, K., Gizachew, M., Kendie, S., (2019). The role of medical data in efficient patient care delivery: a review. *Risk Management and Healthcare Policy*. URL: https://dovepress.com/by 173.48.128.71

Cowie, M. Blomster, J., Curtis, L., Duclanx, S. Ford, I., Fritz, F., Goldman, S., Jammohamed, S., Kreuzer, J., Leenay, M., Michel, A., Ong, S., Pell, J., Southworth, M., Stough, W., Thoeones, M., Zannad, F., Zalewski, A., (2017). Electronic health records to facilitate clinical research. *Clinical Research in Cardiology*, 106(1): 1-9. URL: https://doi-org.libezproxy2.syr.edu/10.1007/s00392-016-1025-6

Dinev, T., Hart, P., Mullen, M. (2008). Internet privacy concerns and beliefs about government surveillance – an empirical investigation. *Journal of Strategic Information Systems*. DOI: 10.1016/j.jsis.2007.09.002

Friedrich, M., Kohn, A., Wiedemann, G., Biemann, C., (2019). Adversarial learning of privacy-preserving text representations for de-identification of medical records. *National Center for Biomedical Computing*. URL: https://arxiv.org/abs/1906.05000

Garcia-Murillo, M, MacInnes, I., (2014). Cosi Fan Tutte: Why a right to be forgotten should not be pursued.

Garcia-Murillo, M., (2020). IST 618-Information Policy: Ethics lecture.

Hannah, K., (2020). Can we ever trust Google with our health data? FT.com. Retrieved on 3/15/20 from https://search.proquest.com/docview/2341964459?accountid=14214

Rothstein, M., Tovino, S., (2019). Privacy risks of interoperable electronic health records: segmentation of sensitive information will help. *The Journal of Law, Medicine, and Ethics*. DOI: 10.1177/1073110519897791.

Schneier, B., (2017). Click here to kill everyone. New York Magazine.

Schultz, R. A. (2005). Contemporary issues in ethics and information technology: IGI Global (Chapter 2)

Swire, P., (1997). Markets, self-regulation, and government enforcement in the protection of personal information, in privacy and self-regulation in the information age by the U.S. department of commerce. *SSRN Electronic Journal*. DOI 10-2139/ssrm11472

USFHealth (website), 2020. Federal Mandates for Healthcare: Digital Record-Keeping Requirements for Public and Private Healthcare Providers. Retrieved on 3/22/20 from URL: https://www.usfhealthonline.com/resources/healthcare/electronic-medical-records-mandate/