

**Balancing Care and Privacy: A Competition for Security Standards Governing Electronic Medical Records**

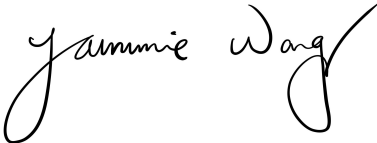
A Research Paper submitted to the Department of Engineering and Society


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

Jammie Wang  
Spring, 2021

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

Signature  \_\_\_\_\_ Date 5/4/2021  
Jammie Wang

Approved  \_\_\_\_\_ Date 5/4/2021  
Hannah Rogers, Department of Engineering and Society

## **Abstract**

Patient privacy is becoming an increasingly important issue due to the digitalization of patient information and the benefits it provides. Cyberattacks on digital systems have only become more common. In the competition to change security standards governing electronic medical records, physicians seek to achieve a compromise between patients, advocacy organizations, and larger corporations that operate for profit, yet corporations will ultimately play a larger role in the formation of new laws due to their existing financial resources and the need to ensure future profit. Examining this competition through the wicked problem framework, there is no correct solution to how much privacy a patient is entitled or not entitled to. However, negative past experiences with HIPAA have driven patients and privacy advocacy organizations to push for privacy law reform, with organizations suggesting an overarching privacy standard that would fill possible loopholes in HIPAA as the technology continues to develop. Hospitals and insurance companies have spent significant amounts of money lobbying to keep privacy laws as they are. A vast majority of healthcare providers have already adopted EHRs, and the benefits from analyzing patient data are only increasing. This indicates a shift in the power dynamics between patients and large healthcare entities in the near future, where patients will begin to speak louder about privacy reform, yet corporations will ultimately still have control over the use of patient data due to the promise of better healthcare with more advanced EHR technology.

## **Balancing Care and Privacy: A Competition for Security Standards Governing Electronic Medical Records**

The initial development of electronic health record (EHR) systems in the 1960s and 1970s provided numerous benefits to the healthcare community. Hospitals were able to transfer patient electronic medical records between one another and send information to insurance companies faster. With further development of this new technology, patients gained faster access to their personal health information and better communication resources. For the medical community, the digitalization of patient medical records increased healthcare accessibility and has been shown to result in a significant increase in patient safety and improved continuity of care across a fragmented healthcare system (Pagliari et al., 2007). However, with the development of electronic medical records, privacy is becoming an important issue. Among the 4,000 cybercrimes reported to the FBI daily, only three arrests occur within every 1,000 reports (Garcia & Hindocha, 2020). Patient data is becoming increasingly valuable due to new technologies that rely on data for development. The use of big data in healthcare analytics allows hospitals to predict patient loads to improve staffing efficiency, prevent opioid abuse by identifying patient risk factors, and research labs have even been able to identify potential cures for certain types of lung cancer through the use of patient data. Despite these benefits, maintaining patient data privacy is an essential concern that must be addressed.

Laws passed by the government aim to dispel some of the debate surrounding patient privacy by establishing certain standards caregivers, hospitals, and insurance companies must follow. HIPAA, passed in 1996, ensures that health information is private unless the patient consents otherwise. The HITECH Act, passed in 2009 by President Barack Obama, refined the language in HIPAA to further ensure compliance to privacy standards. However, unlike HIPAA,

the HITECH Act also served to promote the development and use of health information technology, most notably EHRs (HIPAA Journal, 2020). In the competition to change security standards governing electronic medical records, physicians seek to achieve a compromise between patients, advocacy organizations and large corporations, yet corporations and their representative organizations will ultimately play a larger role in the formation of new laws due to their existing financial resources and the need to ensure future profit and research.

### **STS Framework and Research Method**

There is no fixed answer on how “private” data should be. Privacy can exist on a spectrum. On one end, there can exist a system where a patient has absolute privacy and the medical data is never used or shared with anyone except the patient and the healthcare provider. This is likely what patients would imagine privacy to entail. On the other end of the spectrum, a hospital may use all the patient’s information in research to better improve care services, which is likely more ideal for hospitals or insurance companies who rely on patient data. As a medium ground, a hospital may have limited use of a patient’s medical information. For example, the hospital may be authorized to use a patient’s treatment information, the cause of their condition, etc. for research purposes, but they would not be authorized to have access to a patient’s name, birthday, or other identifiable information about the patient. But at what point on the spectrum could a hospital place the right to privacy over the potential to save a human life, if at all? What if the patient is in an emergency situation and required immediate care?

Hospitals, healthcare facilities and physicians require a certain amount of medical history data to properly function and treat the patient. Insurance companies also require a certain amount of information in order to reimburse patients for treatments and to determine benefits that will be covered by insurance. Patients are allowed a right to privacy, and must consent to the release of

their information by law. Such conflicts between these groups are everlasting and the “correct” answer is constantly a subject of debate. There are many potential opportunities for compromise, yet there is no singular solution to this issue. Since the privacy of electronic medical records can never be solved through a classic scientific approach, this issue can be examined through the Wicked Problem framework (Rittel & Webber, 1973).

According to Rittel & Webber (1973), societal problems are inherently wicked because the problem is ill defined and there is no "correct" solution. Privacy in particular is a public policy issue in healthcare, which is societal in nature and has no true solution. This problem also requires deep ethical consideration because ultimately, the law must balance rights/autonomy ethics and common good ethics. At what point can we sacrifice individual privacy rights for the common good, and vice-versa? Thus, without a fixed answer and a circular debate between relevant parties, privacy of electronic medical records fits the main telltale of a “wicked problem.” Regulating the privacy of electronic medical records also fits other characteristics of wicked problems. There is no definitive formulation of privacy outside the context of law. Privacy sometimes refers to consent; other times, it may refer to restricting spread of all information. This issue also has no stopping rule because there is no perfect solution or logical stopping point to the problem. Since the initial passing of HIPAA, there has been continuous work on reforming privacy laws as the technology continues to develop. Likewise, we also have no way of testing if the current privacy law is a solution to the privacy issue. Every iteration of the law is a "one-shot operation" since the industry will need to spend significant capital to update existing procedures and infrastructure to comply with the update. Patient lives are also constantly being affected by the newest regulations. Digital privacy is particularly unique because this is a new technology that has never been seen before in history. These privacy issues

can also be viewed as a symptom of the current power dynamic between the government and healthcare institutions. However, since this power dynamic is constantly evolving as the technology develops, older privacy norms no longer suffice to protect patients. Society must continue to rethink and revise the privacy standard to fit the modern context by evaluating new risks that comes with this developing technology.

The primary research method is through literature review. This includes obtaining sources that document past incidences of lobbying from healthcare organizations, identifying incidences of privacy violations on an individual level through news reports, and distinguishing notable organizations that advocate for privacy compliance measures or push for patient privacy reform.

### **Patients and the Health Insurance Portability and Accountability Act**

Patients have a right to privacy when it comes to their medical history and current treatments. Their right to privacy is defined under the Health Insurance Portability and Accountability Act, more commonly known as HIPAA. This act ensures that healthcare systems, physicians, care facilities, and insurance companies take responsibility for HIPAA violations, which may include not restricting access to patient records, failure to perform risk-analysis and lack of risk management, denying patient access to their own health records, failure to implement encryption on devices that contain sensitive patient information, releasing information without authorization, etc. There are many other possible violations that fall under the jurisdiction of this law. Generally speaking, HIPAA encompasses most cases of violations of patient privacy. However, many patients argue that HIPAA is no longer sufficient for protecting their personal health information as a direct result of negative personal experiences. A compilation of HIPAA violations by Ornstein (2015) includes stories of an unauthorized nurse examining a family member's medical records, a local hospital sharing details about an 11-year-old child's suicide

attempt, and even a patient care technician that made a public Facebook post about a patient's HIV-positive result. Patients interviewed by Ornstein (2015) reported that they no longer felt safe under current HIPAA laws. More recent violations during the COVID-19 pandemic include a nurse sharing confidential hospital information over Facebook posts, and another nurse who revealed the name of a dead patient on camera (Clark, 2020). By bringing awareness of these violations through the media, this serves as a way of bringing reform to current patient privacy laws. These negative experiences have demonstrated that HIPAA is no longer enough to ensure that privacy is preserved. Clark attributes many of these violations to lack of professional training from their respective healthcare facilities.

### **Advocacy Organizations and Privacy**

Many healthcare facilities are negligent in ensuring that patient data are properly protected, and any complaints usually take many months to investigate. According to HIPAA Journal (2020), HIPAA violations may be persistent in an organization for months or even years before they are properly investigated and the violators are penalized for their negligence. Patient advocacy organizations recognize this, and while some accept this is the current state of law, others push for legal reform. Although some patient advocacy organizations only inform the patient of their current rights, due to the insufficiencies of HIPAA, many advocacy organizations also wish for stricter laws to hold violators accountable, and further protect patient privacy. The American Patient Rights Association offers guides and advice to patients and members of their organization about what legal rights to privacy they have under HIPAA, and how to best ensure that their medical information remains private (Hunt, 2019). Likewise, the Empowered Patient Coalition (2017) offers guides and advice on how to report medical privacy violations should it ever happen. Both of these organizations focus on patient privacy rights as essential information

that every patient is entitled to know, yet they do not argue that current laws are not enough to protect patients.

Meanwhile other organizations, such as the Center for Democracy and Technology take a more proactive stance on patient privacy. The CDT (2009) argues that HIPAA is no longer enough to ensure patient privacy, especially since it does not offer explicit protection to healthcare information that passed through personal health record (PHR) vendors. Examples of such vendors for Medicare include major companies such as Google, Health Trio, Passport MD, etc. who manage large amounts of digital private health information. Since HIPAA was passed in response to health records that flowed through a traditional healthcare system, HIPAA is susceptible to many loopholes that these companies could potentially exploit because electronic health records are a relatively new technology. The CDT believes that PHRs “should be governed by a comprehensive framework of privacy and security protections” which would remove these potential loopholes. Similarly, the Confidentiality Coalition (2020) also believes that there should be a comprehensive framework for patient privacy. They strongly advocate that “Congress should establish a single national privacy and security standard for all health information not subject to HIPAA,” which would solve the issue of possible loopholes in HIPAA with the development of new technology such as electronic health records. In addition, they also push for the disclosure of health information should be “written in a meaningful and understandable manner” and be easily accessible, which would help prevent a majority of patients from being confused by legal jargon surrounding patient privacy. Such patient advocacy organizations such as the CDT and Confidentiality Coalition not only inform patients of the current rights, but they also push for reform. However, these organizations often have insufficient power in the creation of laws, but hope that by bringing awareness to this issue, more



people will advocate for privacy reform, which may eventually cascade into laws. Since government entities have an incentive to pass laws that benefit the citizens and align with the moral ideals of the Constitution, passing a patient privacy law such as HIPAA was inevitable despite the pushback from insurance companies and hospitals.

### **Hospital and Physician Responsibility Towards Maintaining Privacy**

Hospital and care facility employees are typically bound by company or hospital policy to adhere to HIPAA. These employees include all departments in the health system, which may include departments that normally do not interact directly with patient care and diagnosis, such as scheduling or billing departments. Usually, health facilities will implement various levels of access control to ensure that employees will only be able to access data relevant to their positions. However, HIPAA violations can occur due to both hackers and accidental exposure of information from the employees. For instance, the hospital would be held liable for a HIPAA violation if a data breach occurred because the hospital system failed to implement encrypted emails. But in some hospital/corporate hacks, hospitals and care facilities are not held accountable by HIPAA or the HITECH Act if an investigation deems that they have done everything they can to protect patient data and the data breach was unavoidable. Thus, most patient complaints of HIPAA violations are a result of human error and the accidental exposure of private information.

Physicians in particular must take extra precautions to avoid HIPAA violations. Physicians are also ethically bound to maintaining patient privacy, which is usually emphasized by professional physician organizations, which many physicians are a part of. They also face numerous legal challenges during the implementation of EHRs (Gunter & Terry, 2005). Because they have a responsibility to be caregivers and learners at the same time, physicians are put into a

particularly difficult situation where they must share information about patients to learn from one another, but maintain patient privacy to comply with HIPAA at the same time. According to Whiddett et al. (2006), patients typically trust physicians, but not other stakeholders. This trust is not obtained easily, and has numerous legal repercussions if broken. Thus, physicians are a perfect example of how a compromise can be made between the desires of patients and hospitals and insurance corporations. Physician organizations focus on ways to support their learning while still maintaining privacy. For example, the Radiological Society of North America teaches their physicians how to erase sensitive metadata from images (RSNA, 2020), which allows data to be used safely while preserving patient privacy.

### **Privacy Breaches**

There are many reasons why a privacy breach may happen. Many times, it is simple carelessness on a health employee's part. In these situations, normally there is no beneficiary of this data leak. However, other times it may occur due to poor implementation of security measures in a healthcare system. Failure to use basic security tools such as encryption, password protection, lack of access control, etc. are all reasons that a hacker may be able to successfully breach a system and steal important patient information. The healthcare entity faces repercussions from HIPAA in these situations. Kellerman, chief cybersecurity officer of Carbon Black, tells Steger (2019) that the healthcare industry has some of the worst cybersecurity practices worldwide because they are too reliant on methods that do not stop modern-day cyberattacks. Hackers who are able to obtain patient information will usually leverage the data against individuals to extort a financial payoff (Steger, 2019). They may also attempt to commit fraud or long-term identity theft depending on the amount and type of information stolen, which results in extremely negative impacts on a patient's life. Steger (2019) reported that the "value of

medical information on the dark web has surpassed that of credit card and social security numbers.” This makes medical information extremely valuable, yet also extremely dangerous in the wrong hands.

### **Hospital and Company Pushback Against New Privacy Laws**

Despite the possibility of compromise and the danger of leaked medical data, hospitals, health insurance companies, and health organizations actively push back against the idea of patient privacy for a variety of reasons. Complying with new privacy laws requires financial investments into security infrastructures. According to Bowers (2001), healthcare providers and organizations pushed back during the early years of HIPAA because many healthcare organizations were looking to reduce their expenditures in order to ensure financial survival. In addition, healthcare providers were concerned that HIPAA would impede the ability to treat their patients in a timely manner due to the new regulations and procedures needed in order to gain access to patient information. Furthermore, many experts in the healthcare community pushed back against HIPAA in fear that new privacy laws would inhibit research and other current developments in the health industry. A letter collectively sent and signed by multiple representatives of research universities, medical schools, hospitals, scientific societies, pharmaceutical research, medical device, and biotechnology firms, stated that "the rule, unless substantially amended, will harm patients and scientific innovation by creating significant obstacles to the conduct of biomedical, epidemiologic, health services, and other research." They also believed that the restrictions imposed would severely impact the "ability to conduct clinical trials, clinico-pathological studies of the natural history and therapeutic responsiveness of disease, epidemiological and health outcome studies, and genetic research" (Inside CMS, 2001,

p. 15). This concern is still persistent today as EHR technology continues to evolve and more uses are found for patient data with the growing importance of big data.

Lobbying from the healthcare sector increased exponentially in the years after HIPAA was passed. Since HIPAA was passed in 1996, the number of lobbying organizations increased by 50% between 1997 and 2000 (Landers & Sehgal, 2004). Although the details of lobbying activities are undisclosed, many of the top spenders during that time were insurance companies and hospitals, who also happened to experience a large growth in lobbying expenditures from 1997 to 2000. Furthermore, according to Inside HCFA (2000), providers and insurers complained to Congress about a number of issues regarding the implementation of HIPAA. One complaint argued that conflicting requirements for privacy between the state and federal level made implementing security measures difficult. Providers and insurers also noted the lack of time to comply with the new regulations. They also indicated that by implementing new security measures, providers and insurers would be placed under financial burden due to Congress underestimating the cost of implementation (Inside HCFA, 2000). The deadlines and requirements for compliance were then modified to further accommodate providers and insurers.

Despite the semi-successful initial pushback against HIPAA, providers and insurers have found other ways to jump through loopholes in HIPAA. As previously mentioned, HIPAA laws become blurry when vendors enter the equation. Prudential (2017), a large insurance company, states that “we may also use and disclose Protected Health Information for our health care operations” which typically includes hiring third-party vendors to process patient data. With third party vendors able to access patient data without explicit patient authorization, insurers have no reason to ensure compliance with HIPAA beyond what is explicitly stated in the law, which does not extend to third party vendors in spite of the clear potential for a violation.

After the passing of HIPAA, providers and insurers lobbied to ensure more favorable outcomes in Obama's HITECH Act in 2009. The Disease Management Association of America (DMAA) argued that the new privacy laws in the HITECH Act was "extraordinarily burdensome for patients and providers" and that it could potentially "force a delay in healthcare and medical services delivery". Other groups that lobbied against the new privacy regulations included the American Clinical Lab Association, American Hospital Association, the Association of American Medical Colleges, the Blue Cross Blue Shield Association, the Federation of American Hospitals, and many other major hospital organizations across America. These organizations urged Democrats to "drop privacy and security language" from the bill because preventing them from using or sharing electronic patient health information "undermined existing quality improvement initiatives" (Inside CMS, 2009, p. 15).

### **Prioritizing Developing EHRs Over Patient Demands**

Despite the prevalence of corporate and organizational influence in the development of privacy laws, patients demanding change often play a significant role as well. Patients bringing awareness to privacy issues encourage lawmakers and hospitals to promote stricter privacy guidelines. Hospitals and other care facilities in particular have an incentive to abide by privacy laws in order to avoid legal trouble from the HHS Office of Civil Rights. With more patients becoming aware of the right to privacy under HIPAA, more complaints are also being filed with the Office of Civil Rights, leading to more thorough legal restrictions on privacy, as seen through the HITECH Act. This demonstrates that large groups of patients are able to make a significant change in the legal system with enough support. Despite this, the HITECH Act still favors hospitals and insurance companies because EHRs are still a developing technology. Limiting the usage of this new technology too much will ultimately hinder the development of EHRs because

hospitals and corporations will have less of an incentive to invest in it. Without investment capital, the growing usage of EHRs will become constrained despite it being proven to be a beneficial technology.

### **Potential for Compromise**

The anonymization of contact tracing data during the COVID-19 pandemic provides valuable insight on how a compromise can be achieved between patient privacy and health industry needs. The American Health Information Management Association states that “providers will need complete visibility into their patient populations in order to track infection patterns,” yet this data must also be anonymized to protect individual patients, which is a seemingly daunting, yet achievable task for physicians and engineers working together on contact tracing technology (Cidon, 2020). This technology relies on identifying individuals by tokens over Bluetooth, and maintaining a database of tokens that you have come into contact with. Implementing the technology in such a way allows the rights of the individual and autonomy to be respected, while also operating for disease prevention and the common good. Although this is neither a perfect nor universal solution to the wicked problem of patient privacy in electronic medical records, it does address a possible solution to organization concerns about utilizing patient data for research. This fails to account for situations where having quick access to individual patient data improves hospital efficiency, but it does provide hope for compromise.

### **The Future of Privacy**

With the continued development of digitized health records, patients and privacy advocacy organizations aim to increase awareness of the lack of privacy in the healthcare system. Although physicians demonstrate that it is possible to achieve a compromise between privacy and functionality, hospital providers and insurers have a strong financial and scientific incentive

to prevent the implementation of new data security measures. Lobbying Congress to modify privacy laws in their favor have worked out in the past. Healthcare corporations will only have an incentive to continue developing EHR technology if Congress implements relatively loose privacy constraints. In the long term, patients may grow to have a larger say in the development of privacy laws with increased knowledge about their current rights, and through increased political activism.

Within the next 5 years, the power dynamic between healthcare workers and the caregiving facility is unlikely to change. Hospitals, research centers, and insurance companies are likely going to continue to fight to keep privacy standards as they are as big data is becoming an important theme in computing technology. However, with the increasing civilian awareness about data collection practices performed by companies, patients will begin to push for privacy reform across all aspects of society, which will include the healthcare sector. Yet with the potential for technological advancement and improved efficiency in care facilities, Congress will continue to support this technological growth by refraining from putting additional pressure on the healthcare sector to adapt to new security measures.

Since this is a wicked problem, there are many opportunities to find common ground and compromise with future iterations of privacy laws. It's also possible that Congress may decide to pass a universally applicable privacy law across all digital aspects with the rapidly growing number of cybercrimes on a daily basis. In the meantime, we have seen that compromise is possible during COVID-19 contact tracing. If we apply a similar model going forward to more problems, it's likely we can preserve an individual's right to autonomy in terms of privacy, and simultaneously obtain data for research purposes and the common good.

## References

- AHDI (2020). Association for Healthcare Documentation Integrity Code of Ethics. Association for Healthcare Documentation Integrity. [https://www.ahdionline.org/page/code\\_of\\_ethics](https://www.ahdionline.org/page/code_of_ethics)
- ACS (2020, March 23). American Cancer Society. Privacy Statement. <https://www.cancer.org/about-us/policies/privacy-statement.html#security-protection/>
- Angst, C. M., & Agarwal, R. (2009). Adoption of Electronic Health Records in the Presence of Privacy Concerns: The Elaboration Likelihood Model and Individual Persuasion. *MIS Quarterly*, 33(2), 339. Web of Science.
- Barrows, R. C., & Clayton, P. D. (1996). Privacy, Confidentiality, and Electronic Medical Records. *Journal of the American Medical Informatics Association*, 3(2), 139–148. Web of Science.
- BMC (n.d.). Boston Medical Center. Patient Confidentiality, Privacy, and Security Awareness. Boston University Medical Center. Retrieved September 17, 2020, from [http://www.bumc.bu.edu/isep/files/2014/08/HIPAA\\_Presentation.pdf](http://www.bumc.bu.edu/isep/files/2014/08/HIPAA_Presentation.pdf)
- CDT (2009, April 21). Center for Democracy and Technology. Personal Health Records - is HIPAA the Answer? <https://cdt.org/insights/personal-health-records-is-hipaa-the-answer/>
- Cidon, D. (2020, August 3). Patient Matching in the Era of COVID-19: Maintaining Control Over Patient Privacy and Data Governance. *Journal of AHIMA*. <https://journal.ahima.org/maintaining-control-over-patient-privacy-and-data-governance/>
- Clark, M. (2020, October 21). Real-World Examples of Social Media HIPAA Violations. Etactics. <https://etactics.com/blog/social-media-hipaa-violations>
- Confidentiality Coalition. (2020). Beyond HIPAA Principles. Confidentiality Coalition. <https://www.confidentialitycoalition.org/about/beyond-hipaa-principles/>



Durcevic, S. (2020, October 21). 18 Examples of Big Data In Healthcare That Can Save People.

Datapine. <https://www.datapine.com/blog/big-data-examples-in-healthcare/>

Empowered Patient Coalition. (2017, December 12). File A Privacy Complaint.

<https://empoweredpatientcoalition.org/report-a-medical-event/file-a-privacy-complaint/>

Frankenmuth Insurance. (2020, August 4). Company Privacy Notice - Frankenmuth Insurance.

<https://www.fmins.com/company-privacy-notice/>

Garcia, M., & Hindocha, A. (2020, June). Where Are We Now?: Examining the Trump

Administration's Efforts to Combat Cybercrime. *Third Way*. JSTOR.

Gopalakrishna-Remani, V., Jones, R., & Wooldridge, B. (2016). Influence of Institutional Forces

on Managerial Beliefs and Healthcare Analytics Adoption. *Journal of Managerial Issues*,

28(3/4), 191-209. JSTOR.

Gunter, T. D., & Terry, N. P. (2005). 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), e3. Web of Science.

HIPAA Journal. (2020, August 18). What is the HITECH Act?

<https://www.hipaajournal.com/what-is-the-hitech-act/>

Hunt, P. (2019, March 5). Protecting the Privacy and Security of Your Health Information.

APRA. <https://www.americanpatient.org/protecting-your-privacy-security/>

Inside CMS. (2001). HEALTH GROUPS LOBBY HHS FOR NEW RULE ON PRIVACY

MANDATES. *Inside Washington's FDA Week*, 7(33), 15–16.

<https://doi.org/10.2307/26708787>

Inside CMS. (2009). 'CONFIDENTIALITY COALITION' LOBBIES TO KILL PRIVACY

LANGUAGE. *Inside CMS*, 12(3), 15–16. <https://doi.org/10.2307/26680147>

- Inside HCFA. (2000). Providers May Step Up Lobby Against HIPAA-Driven Paperwork Changes. *Inside HCFA*, 3(4), 10–12. <http://www.jstor.org/stable/26694994>
- Ornstein, C. (2015, December 10). Small-Scale Violations of Medical Privacy Often Cause the Most Harm. ProPublica. <https://www.propublica.org/article/small-scale-violations-of-medical-privacy-often-cause-the-most-harm>
- Pagliari, C., Detmer, D., & Singleton, P. (2007). Potential of electronic personal health records. *BMJ: British Medical Journal*, 335(7615), 330-333. JSTOR.
- Pal, D., Arpanikanondt, C., Razzaque, M. A., & Funilkul, S. (2020). To Trust or Not-Trust: Privacy Issues With Voice Assistants. *IT Professional*, 22(5), 46-53.
- Pridmore, J., & Mols, A. (2020). Personal choices and situated data: Privacy negotiations and the acceptance of household Intelligent Personal Assistants. *Big Data & Society*, 7(1), 2053951719891748. Web of Science.
- Prudential. (2017, November). HIPAA Notice of Privacy Practices. Prudential Financial. <https://www.prudential.com/links/hipaa>
- Rittel, H. W. J., & Webber, M. M. (1973). Dilemmas in a general theory of planning. *Policy Sciences*, 4(2), 155–169. <https://doi.org/10.1007/bf01405730>
- RSNA (2020, July 17). Radiological Society of North America. Protecting Patient Information in Medical Presentations, Publications and Products. <https://www.rsna.org/-/media/Files/RSNA/Practice-Tools/RemovingPHI.pdf>
- Sacks, E. (2018, May 26). Alexa privacy fail highlights risks of smart speakers. NBC News. <https://www.nbcnews.com/tech/innovation/alexa-privacy-fail-highlights-risks-smart-speakers-n877671>

Schick I. C. (1998). Protecting patients' privacy. Health information networks raise new questions. *Health progress (Saint Louis, Mo.)*, 79(3), 26–31.

Steger, A. (2019, October 30). What Happens to Stolen Healthcare Data? HealthTech.  
<https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon>

Whiddett, R., Hunter, I., Engelbrecht, J., & Handy, J. (2006). Patients' attitudes towards sharing their health information. *International Journal of Medical Informatics*, 75(7), 530–541. Web of Science.