What Can We Learn about Healthcare IT Risk from HITECH? Risk Lessons Learned from the US HHS OCR Breach Portal

Suzanna Schmeelk, Denise Dragos, and Joan E. DeBello
St. John's University
{schmeels, dragosd, debelloj}@stjohns.edu

Abstract

The healthcare system in the United States has a sophisticated and an industry-unique set of legal requirements. At the Federal level, healthcare entities, which capture personal identifying information (PII) and also financially bill customers, are under two major laws Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health Act (HITECH). The HITECH law requires public notifications of healthcare breaches consisting of 500 or more individuals. The notifications are posted to the US Health and Human Services (HHS) Office of Civil Rights (OCR) Breach Portal for the public to review. This research analyzes the previous year of data posted to the HHS OCR portal to gain empirical insights into healthcare IT risks. As risk informs budget, insurance allocations, and best practices, the real-live evidence analysis gives strong indicators of where stronger mitigating controls should be incorporated into the organizational Information Systems (IS) and overall healthcare infrastructure.

1. Introduction

Healthcare entities are under different laws at different levels of the government hierarchy—International, Federal, State, and local. The laws are essential since health is considered a basic human right; humans from all over the planet can potentially visit any healthcare entity (United Nations, 2020). At the Federal level in the United States, there are two predominate laws for healthcare entities, the Health Insurance Portability and Accountability Act (HIPAA) and the *Health Information Technology for Economic and Clinical Health Act (HITECH)*. HIPAA was passed by Congress in 1996. HIPAA was designed to achieve the following: (1) Provide the ability to transfer and continue health insurance coverage; (2) Reduce health care fraud and abuse; (3) Mandate industry-wide standards for health care information on electronic billing and other processes; and (4) Require the protection and confidential handling of protected health information. In 2009, the HITECH Act became part of the American Recovery and Reinvestment Act (ARRA). ARRA was created to motivate the implementation of electronic health records (EHR) and supporting technology in the United States (U.S. Department of Health and Human Services (HHS), 2013).

One of the requirements of HITECH is the public notification of healthcare breaches of personal identifying information (PII) if a breach effects 500 or more individuals. When a healthcare breaches this number of individuals, they can also be fined as part of a corrective action plan. Both the notifications and the investigations can cause serious financial burdens exacerbated by both reputational damages and required infrastructure improvements. In addition, patients whom have had their information breached may be at higher risks of identity theft.

To improve mitigations against data breaches, this research examines the public notifications of PII breach trends to inform the healthcare entities of the most current risks around the United States. These current risk trends inform organizations as to where they should be deeply (re)considering and (re)budgeting for risk mitigations (i.e. NIST 800-53 risk controls (NIST, 2020)) to protect their patients and their overall healthcare entity from data breaches.

2. Literature Review

There is very little literature in the cybersecurity and computer science domain considering the risks learned from an examination of the empirical data reported on the US HHS OCR Breach Portal. Schmeelk (2019a) and Schmeelk (Schmeelk, 2019b) analyzed the breach data on a 1-year interval between May 1, 2018 through May 1, 2019. The analysis reported on trends from breach factors reported to the government to further inform cybersecurity patient health data risk management.

URI: https://hdl.handle.net/10125/71101
978-0-9981331-4-0

Dolezel and McLeod (2019) examined the Department of Health and Human Services breach reporting portal public dataset from the first record on October 21, 2009 until October 8, 2018. Specifically, they analyzed the relationship between data breach characteristics and the number of individuals affected as protected by the HITECH law. The analyses revealed that the hacking/IT incident breach type and network server breach location were the most significant predictors of the number of individuals affected. Their analysis showed that geographic region of a breach occurrence was insignificant.

Bai, G., Jiang, J. X., & Flasher, R. (2017) examined the hospital risk of data breaches from the data reported to the HHS OCR between October 21, 2009, and December 31, 2016. Their research found that of the 1798 data breaches were reported, 1225 breaches were reported by health care providers. Additionally, there were 257 breaches reported by 216 hospitals in the data with at least 33 hospitals involved in more than one breach. Of the breaching hospitals, the median number of beds was 262 and 52 hospitals were major teaching hospitals.

Liu, V., Musen, M. A., & Chou, T. (2015) evaluated 949 breaches from the public HHS OCR HITECH breach dataset. The breaches affected more than 29 million records between 2010 and 2013. The researchers found that six breaches involved more than 1 million records each and the number of reported breaches increased over time. All states were reported to have breached. The researchers adjusted the breach numbers per state with the population estimates without finding significant patterns of state populations and breaches.

3. US HHS OCR Data Breach Portal

As required by section 13402(e)(4) of the HITECH Act, the HHS OCR Secretary must post a list of breaches of unsecured protected health information (e.g. patient health identifiers (PHI)) affecting 500 or more individuals. This portals main page lists all breaches reported within the last 24 months that are currently under investigation by the Office for Civil Rights (OCR).

Currently the portal posts the following information: Breach Submission Date, Type of Breach, Location of Breach, Type of Covered Entity, State, Business Associate Present, and optionally a Description. The types of breaches are listed the following categories: Theft, Hacking/IT Incident, Unauthorized Access/Disclosure, Improper Disposal, Loss, Unknown, and Other. The locations of breaches are listed in the following categories: Desktop Computer, Electronic Medical Record, Email Laptop, Network Server, Other Portable Electronic Device, Paper/Films, and Other.

4. A Look Back Risk Analysis

This section reports on the last full 12-months of reported HHS OCR patient data breach information to inform on future risk trends and potential mitigations.

4.1. Analysis By State

Analyzing the full year of data breach records by state provides insight into which states were the riskiest last year. The previous 1-year of data, as seen in Figure 1, indicates that Texas had 51 self-reported breaches, the most self-reported breaches of the states. California was second in the number of data breaches, self-reporting 41 data breaches. Of the self-reported breaches, Puerto Rico, West Virginia, Wyoming, District of Columbia, and Rhode Island only reported one breach each. The states of Idaho, Mississippi, New Hampshire, North Dakota, South Dakota, and Vermont did not self-report any breaches within the one-year interval.

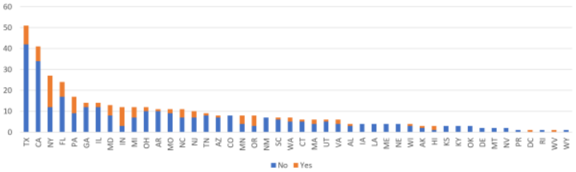

Figure 1: Data Breaches by States with BAAs

4.2. Analysis By Individual

The number of breaches is not connected to the number of individuals potentially compromised in a breach. Examining the previous year of data breaches of individuals across the states, the District of Columbia, and Puerto Rico, we see that the top five states with the most affected individual's records were the following: Minnesota breached the PII of 11,590,390 individuals, Texas breached the PII of 2,419,342 individuals, California breached the PII of 1,042,144 individuals, Florida breached the PII of 832,286 individuals and Oregon breached the PII of 747,173 individuals. A chart can be seen in Figure 2.

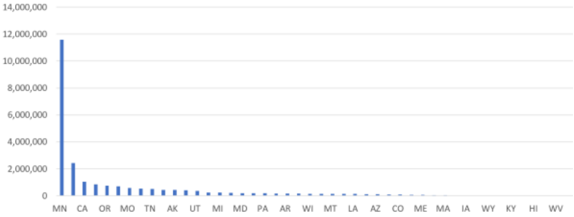

Figure 2: Data Breached Individual PII by States

4.3. Analysis by BAA

Business Associate Agreements (BAAs) should be put in place to protect a covered entity (i.e. health plans, health care clearinghouses, and certain health care providers) whenever an outside entity performs actions or functions on their behalf. The HIPAA Privacy Rule only applies to covered entities, it requires that a covered entity obtain satisfactory assurances from its business associate that the business associate will appropriately safeguard the protected health information it receives or creates on behalf of the covered entity. The satisfactory assurances must be in writing, whether in the form of a contract or other agreement between the covered entity and the business associate. After a breach originating with the business associate, if no BAA is in place, then both the business associate and the covered entity face corrective actions and fines.

Figure 1 shows the split histogram of breaches where a BAA is present (histogram top orange color) and where a BAA is missing (histogram bottom blue color). As can be seen, most breaches were reported without a BAA. Specifically, of the 416 breaches reported between June 2019 and June 2020, no BAAs were present in 308 breaches and 108 breaches did indeed have BAAs in place. This shows that there is higher risk that BAAs are not in place; the empirical evidence should justify budgeting for better processes to ensure that business associates conform to BAAs prior to processing PII on the covered entities' behalf.

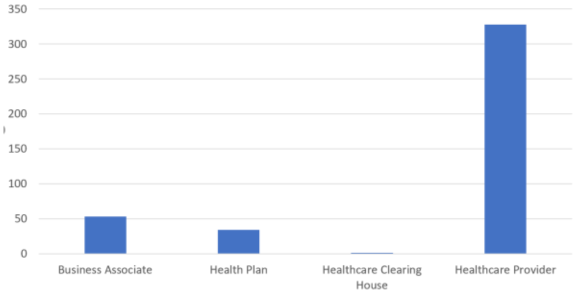

Figure 3: Breach Entity Data Breach Count

4.4. Analysis By Breach Entity

Data breaches can occur within a health plan, health care clearinghouse, certain health care providers, and business associates. Figure 3 shows the count of data breaches per entity from June 2019 to June 2020. As can be seen, the highest risks are from healthcare providers. Specifically, the breach count per entity is as follows: Business Associates reported breaches 53 times, Health Plans reported breaches 34 times, Healthcare Clearing Houses reported breaches one time, and Healthcare Providers reported breaches 328 times. Clearly, Healthcare providers are the entities that still need to allocate more budget and time to the protection of patient PII.

4.5. Analysis by Breach Source

The breach portal categorizes breaches by source into five categories, as seen in Figure 4. By far, the predominate methodology of loss of patient PII was hacking/IT incident. Specifically, the reports for the year were the following: Hacking/IT Incident reports totaling 264 breaches, Improper Disposal totaling 12 breaches, Loss totaling 11 breaches, Theft totaling 27 breaches, and Unauthorized Access/Disclosure totaling 102 breaches. The evidence shows that healthcare budgets should emphasize and perhaps increase budgets for mitigating controls of hacking/IT incidents and unauthorized patient PII access/disclosure.

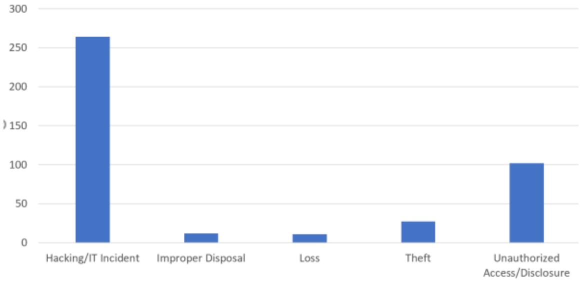

Figure 4: All Covered Entities by Breach by Type

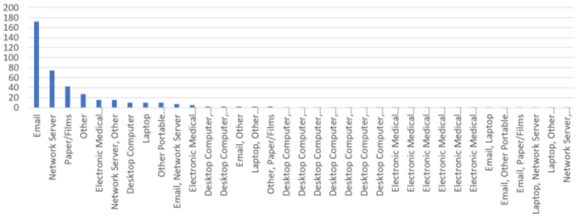

Figure 5: All Covered Entities by Breach Location

The breach portal categorizes breaches by location into approximately 35 categories, as seen in Figure 5. The top sources of the 416 reported data breaches were the following: Email had 172 reported breaches, Network Server had 74 reported breaches; Paper/Films had 42 reported breaches; Other had 27 reported breaches; Electronic Medical Records had 15 reported breaches; Network Server, Other had 15 reported breaches; Desktop Computer had 10 reported breaches; Laptop had 10 reported breaches; Other Portable Electronic Device had 10 reported breaches; Email, Network Server had 7 reported breaches; and Electronic Medical Record, Network Server had 5 reported breaches. All the rest had one or two reported breaches in their source category. This information shows that healthcare privacy and security budgets should amply include mitigating controls around email, network servers and the process for the disposal of paper/films records.

4.5.1 Analysis by Health Plan

Managing risk in Health Plans is different than other covered entities as the risk threats and risk impact are different than other breached entities. An examination of the breach sources only within the Health Plans 34 reported breaches reveals that there were only three categories of breaches reported as follows: Hacking/IT Incident reports totaling 19 breaches, Unauthorized Access/Disclosure reports totaling 13 breaches, and Theft reports totaling 2 breaches. A histogram of the breaches by category can be seen in Figure 6.

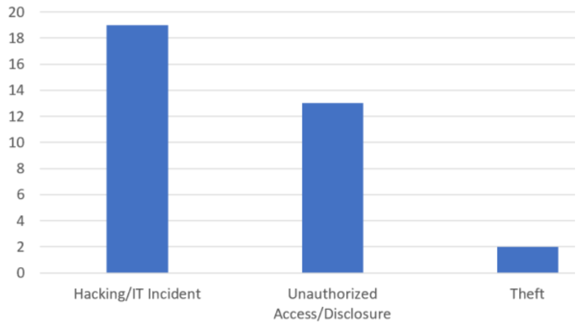

Figure 6: Health Plan by Breach by Type

Health Plans reported 34 breaches of which the most breach (i.e. 13) were sourced from email. Each category of Network Server and Paper/Film breaches were reported as the source of five breaches. All the other breach source categories had three or less reports. A histogram of the breach categories for Health Plans can be seen in Figure 7.

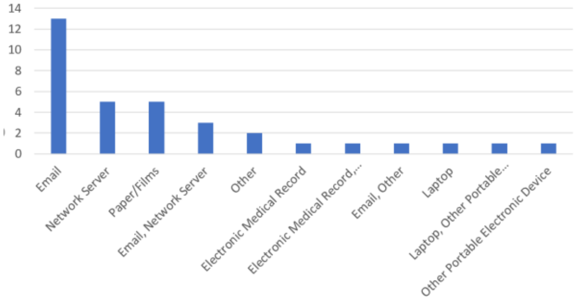

Figure 7: Health Plan by Breach Location

4.5.2 Analysis by Clearing House

Clearing Houses have different risks from the other covered entities as the processes, procedures and actual stored patient PII may be different than the other entities. An examination of the one reported data breach within the Clearing House category, specifically a breach reported on March 20, 2020, by the Georgia Department of Human Services for 500 individuals, indicates that the data was loss through Paper/Films categories, perhaps during an improper disposal of records. Interestingly, in this particular case, the breach was not technology related for the data indicating that mitigating process controls should be amply budgeted for in Clearing Houses.

4.5.3 Analysis by Business Associate

Business Associates also have unique risks as the risk elements of threats and impacts are different than other entities. Business Associates reported 53 breaches between June 2019 and June 2020. Of the reports, the two highest categories of breach types were Hacking/IT Incident with 39 reports and Unauthorized Access/Disclosure with 11 reports, as seen in Figure 8.

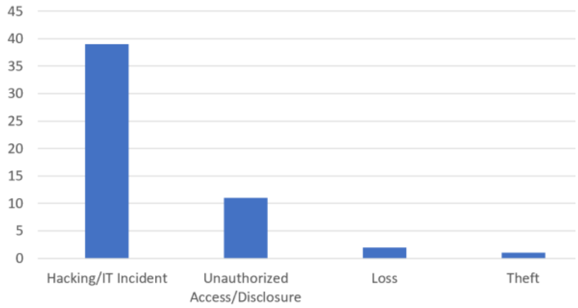

Figure 8: Business Associate Breach by Type

Business Associates reported that the most breaches occurred via Email with 27 reports. The Network Server category had the second highest number of 12 reports. The other categories had only one or two reports over the year, as seen in Figure 9.

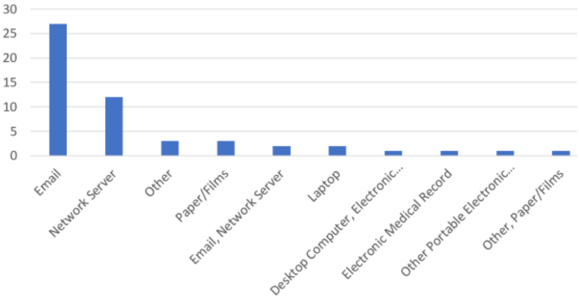

Figure 9: Business Associate by Breach Location

4.5.4 Analysis by Healthcare Provider

Healthcare Providers (HP) report 328 breaches from June 2019 to June 2020. The highest category of breach type was Hacking/IT Incident with 206 reports followed by Unauthorized Access/Disclosure with 78 reports. A histogram of the reports can be seen in Figure 10.

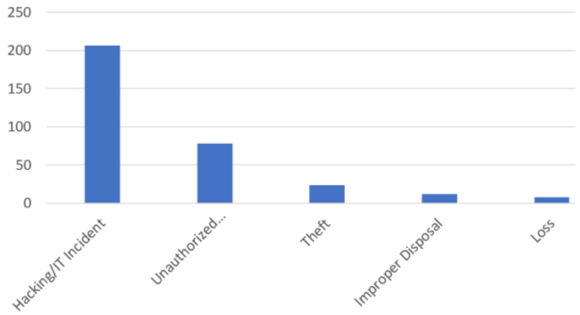

Figure 10: Healthcare Providers by Breach Type

Healthcare Providers breach reports indicate that Email was the number one source category at 132 reports. Then, Network Servers were the second most breach reported sources with 57 reports. Finally, Paper/Films were the third highest breach sources with 33 reports. A histogram of the reports can be seen in Figure 11.

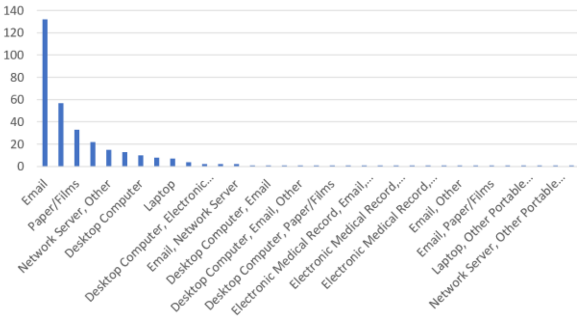

Figure 11: HP by Breach Location

4.5.5 Entity Analysis Source Summary

Examining each breach entity independently informs on the variations needed for risk management in the different entities. Healthcare Providers clearly breach data from many different categories of locations than the other entities. However, all the entities share some of the top three breach types and sources.

4.6. Case Studies: Top Breach Individuals

During June 2019 – June 2020, there were three top breaches. First, Optum360, LLC., a Business Associate headquartered in Minnesota reported the breach of 11,500,000 individuals on July 1, 2019 due to Hacking/IT Incident of their Network Server. They did have BAAs in place for their patient data.

The second largest breach of the year interval, was from Clinical Pathology Laboratories, Inc., which is a Healthcare Provider headquartered in Texas. They reported the breach of 1,733,836 individuals. on July 15, 2019 from Hacking/IT Incident on their Network Server. There were no BAAs in place.

The third largest breach of individuals reported during the 2019-2020 interval was from Health Share of Oregon, which is a Health Plan headquartered in Oregon. The plan reported a breach of 654,362 individuals on February 5, 2020 from Laptop Theft.

4.7. Case Study: State with Most Breaches

Texas self-reported the most breaches in the June 2019-2020 interval with 51 reports. Of the reports, Healthcare Providers consisted of 46 reports, Business Associates with 4 reports, and one Health Plan report. The reports of breach categories in the Texas Healthcare Providers matched the same distribution as the reports across the country seen in Figure 4. Interestingly, examining the breach sources in the Healthcare Providers in Texas showed that the number one reported breach sources was the Other category with 15 reports, as seen in Figure 12.

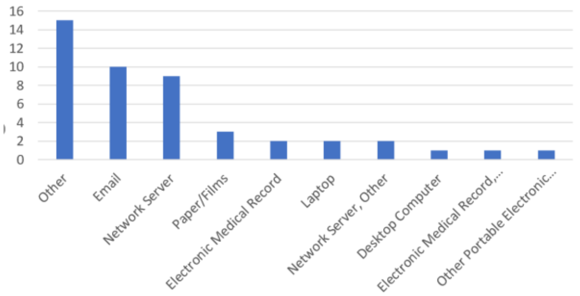

Figure 12: Texas HP by Breach Location

4.8. Case Study: Breach State with Least

Six states--Idaho, Mississippi, New Hampshire, North Dakota, South Dakota, and Vermont--did not self-report any data breaches within the one-year interval to the HHS OCR. Three states, the District of Columbia, and the Puerto Rico Territory all self-reported only one breach within the interval.

In Puerto Rico, the Intramural Practice Plan of the Medical Sciences Campus of the University of Puerto Rico reported a breach on September 16, 2019. The entity is considered a Healthcare Provider. The self-report indicated that 439,753 individuals were affected from a Hacking/IT Incident of a Network Server. There was not a BAA in place, but perhaps one was not necessary. Finding any further public information about the breach was not possible.

On December 12, 2019, a Business Associate in the District of Columbia named Service Benefit Plan Administrative Services Corporation reported a breach. They reported 11,536 records were involved in an Unauthorized Access/Disclosure of the Network Server. They reported having BAAs in place.

The Personal Touch Home Care of W. VA, Inc, a Healthcare Provider headquartered in West Virginia reported a breach on January 28, 2020. The breach involved 1,169 records from a Hacking/IT Incident of a Network Server and Other category. They report that BAAs were in place.

In Wyoming, the Healthcare Provider Cheyenne Regional Medical Center reported a breach on December 10, 2019. The Hacking/IT Incident breached 17,549 records sourcing from Email. The organization reports not having a BAA in place; however, perhaps none were needed.

In Rhode Island, the Rhode Island Ear, Nose and Throat Physicians Inc., reported a breach on August 16, 2019 involving 2,943 records. The entity is considered a Healthcare Provider, whom fell victim to a Hacking/IT Incident of their Network Server. A BAA was not reported in place, but perhaps one was not needed.

5. Discussion and Future Work

Risks, threats, and impact change over time. It is essential to review the notifications posted to the HHS OCR portal on an annual basis to inform current best practices for covered entities. This paper contributes an analysis of risks reported to the portal between after June 30, 2019 until June 30, 2020. We found that the number of self-reported breaches has no correlation with the number of records involved in a breach. In the self-reported breach scenarios, a breach could involve over 11+ million individuals; whereas another breach could involve the public disclosure of the minimal 500 records. Our analysis showed that different breach entities may have different risks involving breach type and breach location, informing entity operations for mitigating risks. Lastly, we recommend a few updates to the HHS OCR portal including more information on exactly what type of PHI was breached (e.g. photos, email addresses, EMRs, etc.) Currently, the burden is on the entity to publicly disclose to patients what was lost, but the US industry at large would benefit from knowing this to help developer further mitigating controls. Another potential portal update would be to indicate if a BAA was indeed necessary, as a BAA is not always necessary. Therefore, the portal's current state, where there exists a binary categorical category for the presence of a BAA, may not be interpreted accurately from a risk perspective when a breach does not involve a business associate and indicates that a BAA was not present. In this case, a BAA would not need to be present if no outside entity was involved in the reported breach.

6. Conclusions

The healthcare industry has moved to a risk management model, perhaps due to the Federal requirement of risk assessments for systems and processes involving PHI. Currently the healthcare industry has not yet adopted a standard risk framework library (Schmeelk, 2020). The adoption of such a framework would help unify associated breach cost estimates for insurance purposes and improve ad hoc risks assessments from reporting entirely different findings. Lastly, adding additional elements to the public notifications such as the type of PII breached and if a BAA was necessary, could improve industry's response to developing more accurate mitigating controls. Data breaches can lead to identify theft which is a big problem for many individuals. The more we focus our research on why data breaches are still occurring, the sooner we can mitigate the risks and lower the number of affected individuals.

7. References

National Institute of Standards and Technology (NIST), (2020). NIST Special Publication 800-53. Retrieved November 17, 2020, from: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

Bai, G., Jiang, J. X., & Flasher, R. (2017). Hospital Risk of Data Breaches. JAMA internal medicine, 177(6), 878–880. doi:10.1001/jamainternmed.2017.0336

Dolezel, D. & McLeod, A. (2019). Cyber-Analytics: Identifying Discriminants of Data Breaches. . Perspectives in Health Information Management(16(Summer):1a).

Liu, V., Musen, M. A., & Chou, T. (2015). Data breaches of protected health information in the United States. JAMA, 313(14), 1471–1473. doi:10.1001/jama.2015.2252

Schmeelk, S. (2020). Creating a Standardized Risk Assessment Framework Library for Healthcare Information Technology. HICSS-53: Hawaii International Conference on System Sciences (HICSS), Maui, Hawaii, USA

Schmeelk, S. (2019a). Where is the Risk? Analysis of Government Reported Patient Medical Data Breaches. In IEEE/WIC/ACM International Conference on Web Intelligence - Companion Volume (WI ’19 Companion). Association for Computing Machinery,. New York, NY. doi:https://dl.acm.org/doi/10.1145/3358695.3361754

Schmeelk, S. (2019b). Identity Theft: Anatomy of a Data Breach. New York, New York: Parsons - The New School for Design.

U.S. Department of Health and Human Services (HHS). (2013, July 26). HITECH Act Breach Notification Guidance and Request for Public Comment. Retrieved July 11, 2020, from https://www.hhs.gov/hipaa/for-professionals/security/guidance/HITECH-act-breach-notification-guidance/index.html

United Nations. (2020). The Universal Declaration of Human Rights. Retrieved November 17, 2020 from: https://www.un.org/en/universal-declaration-human-rights