Sharing the Blame in the Epidemic of Healthcare Data Breaches

Vivian Hong
May 7, 2018

Abstract

The issue of cybersecurity in healthcare has become increasingly apparent and relevant in recent years with the appearance of shocking statistics (yet unfortunately few mainstream headlines) detailing healthcare as the industry that has exposed the most social security numbers (SSNs), has had the most records exposed by employee error/negligence, and has been the most targeted by hacking, skimming, and phishing attacks. Many of these statics do not even include data breaches that only involve usernames, passwords, and/or emails as they usually do not qualify for most data breach notification laws[5]. Additional to these alarming reports detailing data breaches of all types, are the more conspicuous rise in medical device attacks (heart rate monitors, MRI scanners, medical tablet computers, drug pumps, defibrillators, pacemakers, etc.), reports of healthcare facility network tampering that result in physical harm or fatalities, and political disputes surrounding new technology and access to medical information (i.e. workout band deals from insurance companies and the implications on pre-existing condition exceptions, etc.). Despite the (admittedly understandable and sometimes reasonable) greater hype around these latter issues, large scale data breaches in health care have a much greater impact (quantifiably), yet are discussed far less and are thus severely lacking in robust analysis and potential solutions.

This paper will focus on the conditions surrounding largescale data breaches in health care—although it should be noted that these issues also contribute to the security concerns surrounding medical device attacks, internet facing health data, and facility network vulnerabilities. I aim to discuss and work towards synthesizing just a few of the sometimes disparate conditions that have led to this reality of the healthcare industry greatly lagging behind other industries in securing data and safety. The aspects of insecurity in healthcare data that will be addressed are HIPAA (and post-HIPAA) compliance complications, the reality of the infrastructure (third party handling, etc.) and hierarchies of priority (education, incentives, approach), the problem with the healthcare specific CIA triad[9], and the gap in existing software to accommodate the level of exception handling necessary specifically in healthcare that all contribute to position healthcare as one of the most targeted and least protected industries regarding data breaches

Introduction

Data breach headlines have become one of too many familiar recurring news stories that seemed to have lost any impact due to the repeated inundation, leading to the common mindset of "not if but when". When breaches on the scale of the 2017 Equifax breach (which affected *at least* 143 million Americans) can become five minute hot topics that fade (for those not dealing with the immediate repercussions of personally compromised SSNs) into the shadow of the next scandal, the lack in visibility of and knowledge around the data insecurity surrounding healthcare can begin to be rationalized. Even outside of lay-public awareness, there are difficulties in bridging the gaps in the understanding of this issue and its complete permeation, especially in healthcare, a field that has not been tied to data exposure in the realm of public perception, despite the reality of common insecurity.

Many experts on the technical side of these third-party software packages used by large medical providers and companies focus on the issues that come with large code bases and the seeming inevitability of bugs and flaws, whether through human error or insecure programming practices/design. Those involved more directly in the healthcare field tend to have a lack in knowledge about technical security, and a deficiency in focus on security practices due to the very nature of medical care priorities. Governmental regulation is lacking as well, through policy that fails to adequately equip, motivate, and enforce large sweeping restrictions that only rhetorically cover all bases, but offer no real solution.

After presenting the major contributors (and there are many) to this large-scale insecurity, a specific case study will be analyzed to demonstrate no only the factors *within* groups that lead to these issues, but also the factors *between* groups that have ensured persistence of vulnerability. This paper would be remiss if it did not provide potential solutions, or at least avenues to investigate, so a variety of ideas for addressing the problem will be presented at the close. To conclude, an example of respected healthcare data-exchange software will be analyzed in the context of the bigger picture.

To the Community:

Despite being one of the less flashy issues in cybersecurity today, especially when considering where general social-political concern currently lies, the epidemic of data breaches in healthcare is undeniable, massive in scale, and of incredible consequence to individual (physical and otherwise) and societal safety and security. The overwhelming breadth and depth of vulnerability within healthcare is, in many ways, built into the very model of healthcare. Unquestionably, issues lie within software used by healthcare providers and corporations, however it would be careless to simply fault and target buggy and/or flawed code without considering the multitude of compounding factors that contribute to this staggering insecurity in one of the most important, pervasive, and sensitive fields. The response must be a holistic one, necessarily integrating technical, systemic, and social/behavioral changes. Especially when many people have implicit trust in healthcare organizations and expectation that respected institutions can deliver on their confidentiality promises, despite the truth being wholly otherwise, awareness and understanding of this issue becomes paramount for experts (within and outside of tech) and for patients and software users. Why this matters is simple: insecurity in healthcare is not a confined issue; security of financial information, permanent identity, and other types of leverageable information, as well as physical health and well-being, all comprise the core of the vulnerability impact.

1 Defining the Problem of Data Security in Healthcare

To start, a clear identification of contributors to the data breach problem in healthcare is crucial. This includes the impact of macro reasons for data breaches (human-level motivations, etc.), the inherent vulnerability (and perhaps incompatibility of security) in healthcare system priorities, and the increase in

exposure to cyber-attacks (exacerbated by policy which insufficiently regulates and improperly incentivizes).

1.1 Big-Picture Social Motivation/Explanation

As a starting point, the incredibly high rate of targeting in the health care industry can be loosely explained by a simplified positing: *soft target meets high-value information and yields highly vulnerable interaction.* This immediately points to more malicious motivations, the most obvious being that of financial gain, through acquisition of information necessary for patient care: SSNs, financial credentials, and other identifying personal information. The sensitive nature of healthcare information, that not only includes permanent identification information, but also contains private health information (physical, medicinal, etc.), leads to the value and impact of this information when involving high profile people. The usage of ransomware in data breaches has probably garnered the most public attention, as its effects are devastating to both individuals and companies. Large-scale data corruption for purposes of political or personal gain and threats of DDoS attacks as blackmail, revenge, or activism also contribute as motivating factors[6]. It is additionally important to point out that data corruption does not only potentially affect identity security, but also physical safety, as unauthorized access to healthcare data allows for manipulation of data, such as test results and blood type documentation, or permits scraping of information about medical device implants for further damaging action, such as device hacking.

Aside from these more malicious attacker-based motivations, are also the *unintentional* insider actions comprised of both error and negligence from the employee side[6]. The high rate, specifically within healthcare, of this sort of misstep being responsible for breaches, bridges into the next section which touches upon inadequacy in transmission of knowledge and training about security within non-technical (technical, in this case, referring to software-centric) groups in the field of healthcare.

1.2 Inherent Healthcare-Specific Systemic Vulnerabilities

The complexities involved in this part of the discussion make it difficult to succinctly present all components without losing the specificity necessary to detail the smaller interactions that lead to a larger "culture". This will not be a comprehensive explanation but will attempt to at least give an idea of the multiple contributing factors to a systemic inadequacy.

The CIA triad, a guiding model comprised of "Confidentiality Integrity Availability", is considered by many to be the foundation of good security policy. It is often depicted as an equilateral triangle, with equal weight being given to the three cornerstones of the principle—metaphorically apt, the mathematical restraints on angles in a triangle describe how giving more importance to one is to take away from the others. The priorities in healthcare naturally emphasize patient care, which is contingent upon obtaining correct patient information (personal health history, identity, etc.). High quality health care often relies on the availability of this information, thus necessarily skewing the CIA triad in the healthcare industry[9]. This emphasis of availability and subsequent reduction of integrity and confidentiality (despite HIPAA, which will be touched upon later) is especially dangerous when combined with the sensitive nature of personal information generally given to healthcare providers. This healthcare specific CIA triad gives a big picture overview of the inherent tension between good healthcare and good security, and shows how treating them as unrelated issues misses the point.

One of the biggest correctable errors within this group of inherent vulnerabilities, is the level of knowledge, training, and awareness that healthcare workers who interact with patient data possess. Even basic physical security precautions are not imbedded in healthcare culture/common practice, despite the sensitivity of the data being dealt with. Basic precautions are not incorporated in training, and result in prevalence of easily avoidable vulnerabilities, such as physically exposed passwords, patient data left open (not logging out), and responses to phishing emails. This issue can be partially attributed to lack in understanding of security within the field and perhaps a failure on the part of the third-party sources of

security for these healthcare providers. Lack of communication of these important behavioral changes is also pervasive. Furthermore, the transfer to digital records has been a recent one, and much of the healthcare industry has been slow to recognize security as a leading issue in the field.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act are policies that theoretically ensure the protection of patient confidentiality. In reality however, especially in the face of new technologies being rapidly incorporated into healthcare every day, a multitude of issues arise with insecurity in healthcare that are improperly addressed by the regulations within these acts. These issues and great potential (or already exploited) vulnerabilities are often simply responded to with a vague sentiment that HIPAA covers all bases when dealing with patient confidentiality.

One of the more basic issues lies in inadequate compliance with HIPAA and HITECH regulations, and failure to ensure compliance by regulating bodies[8]. According to some, top concerns regarding compliance are rapidly evolving technology, inadequate employee training, and external threats[11]. New technologies have not incorporated proper protection on systems and equipment containing sensitive data. The technical side of this issue is laden with the general difficulties of proper data protection, prevalent throughout cybersecurity, however healthcare specific technical fixes are also paramount. Additionally, many regulations fail to be effective as they often list requirements without offering solutions for accommodating the standards. Many of the more reliable data-security measures currently available make information access more difficult and time-consuming, decreasing productivity and effectivity of organizations, despite offering potentially better adherence to security policy. This sort of restriction is difficult to prioritize without direct incentive involving quality of patient care (although data vulnerability puts potentially millions at risk, in a less immediately concrete fashion).

An additional incentive issue lies in the lack in motivating enforcement. Most industries allow for the cybersecurity costs to be pushed directly onto the consumer, however healthcare organizations do not have this ability. There is a large financial barrier to compliance because of the demand on resources, manpower, and money. It is often more inexpensive for organizations to suffer consumer and monetary losses (fines from the government) from breaches, than to invest in loss prevention[8]. The ethical inadequacies here cannot compare to the monetary needs of organization whose primary priority is physical health of patients. Organizations also lack resources, knowledge, and training regarding extreme susceptibility to data breaches, largely because of complete outsourcing of this issue to third party organizations without further communication to employees within the field.

Post-HIPAA compliance issues are also abundant. The focus on patient health information (PHI) is only one part of the whole issue but is not addressed by regulation. Additionally, existing regulations are not conducive towards increasing resilience. The usage of HIPAA as an all-in-one fix, fails to frame the risk as an organization-wide issue, enabling the continued insecurity. Security priorities and circumstance of organizational objectives are not aligned[8]. Stepping away from the framework HIPAA induces allows for a reexamination of the interaction between security and administration of care.

More practical inherent issues within healthcare lie in limited resources, lack in accountability (often due to organizational fragmentation in security issues), public and private sector inconsistencies, and lack in policy and research. Overall infrastructure is insufficient and monetary incentive (for industry stakeholders) is nonexistent when looking at practical profit-margin discrepancies.

1.3 Increased Exposure to Cybersecurity Threats

Despite medical technology being an innovation hot spot, the continuous advancement has not been matched with equal security considerations[4]. This uptake in rate of relevant technological advances may be exciting for the potential in patient care, yet the vulnerabilities that come with it can have devastating consequences for these same patients. This issue is additionally exacerbated by federal initiatives[4,9] that

promote the use of this new healthcare technology without equal incentive for uptake in security. The total sum of these factors has led to greater exposure to cyber-attacks.

2 Taking a Closer Look at WannaCry

Within recent years, healthcare data breaches on the scale of hundreds to millions have been accumulating at an alarming rate. These breaches have been attributed to missteps ranging from improperly closed links to hardware theft to ransomware attacks. Furthermore, the responses from these organizations often simply consist of "a year of free credit monitoring to patients and a review of IT practices". One breach, however, has stood out among them all, and has been dubbed by many as the worst data breach of all time—namely, the 2017 Wanna Decryptor ransomware ("WannaCry") variant attack on the National Health Service (NHS), which runs UK hospitals and other medical-care institutions. It is also, in many ways, emblematic of the issues of cybersecurity in healthcare.

2.1 The Basics

The event is well summarized by CSOonline: "WannaCry is a ransomware worm that spread rapidly [across] a number of computer networks in May of 2017. After infecting Windows computers, it encrypts files on the PC's hard drive, making them impossible for users to access, then demands a ransom payment in bitcoin in order to decrypt them"[3]. NHS was only one of multiple high-profile systems infiltrated. Additionally increasing the buzz around this large data breach were (1) suspicions that this Windows vulnerability had been previously discovered by the U.S. National Security Agency (NSA) and (2) potential links to the cybersecurity organization Lazarus Group, an group commonly thought to be linked to the North Korean government.

WannaCry infected computers through exploiting a specific Windows protocol, allowing outside code to be executed. Supposedly, the NSA found this vulnerability long before the breach occurred and had even developed a program called *EternalBlue* in order to exploit it[3]. This code was in turn stolen. Microsoft, however, had developed a patch for this issue over a month before the data breach, but many systems had not updated at the time of the attack. Experts who analyzed the ransomware found it easily dissectible[3] and less sophisticated than assumed, despite many reports stating its complexity[2] (largely by pointing to the still un-broken encryption).

2.2 The Response

Much of the reporting on this attack, aside from its staggering impact and its salacious details (regarding the NSA and North Korea), focused on the technical aspect—how powerful this ransomware is, what hackers were able to exploit, and how this malware works. All of this information is valuable, yet pointing exclusively to it glosses over the healthcare industry's systemic lacking. This diverts attention from fixable issues involved in this, and many other, breaches. Most readers walk away from stories about this breach of over 50 UK hospitals and 150 countries[6] feeling like the only solution is to somehow stay one step ahead of hackers, an ask that is both difficult and externalized from healthcare organizations. Technical inadequacies are important to address, but they are far from the only change necessary. Insider error causes the majority of data breaches— generally inadvertent employee mishaps, rather than malicious insider incidents, as might be expected. Understanding how this malware functions does give insight into exploitable bugs or flaws[14], yet stopping here fails to capture the whole picture that would be much more successful in informing the way for effective prevention and response.

The two main targets of blame were the Lazarus Group and Microsoft. Additionally, some blamed the NSA for not reporting the vulnerabilities they discovered[13]. These are understandable errors/intentional actions to hone in on, however, they are not the only, or even largest source of insecurity in this situation. What many discussions of this breach did not touch upon, were the existence of patches for Windows XP prior to the breach[13] that had simply not been updated on the NHS computers. Many of these computers had not updated their versions of Windows XP for three years, and

had missed important patches that may have lessened the widespread impact of this attack. Despite this patch being flagged as critical, it was not implemented, as no protocols for keeping up to date with software were set in place. These systems also had no safe backups of important data and documents, making response to potential (and, at this point, probable) attacks especially difficult.

Additionally, the NHS is known to be underfunded, and the existing budget for security, specifically, is less than adequate. Their policy for allocation understandably focuses on things such as equality of healthcare access, alignment with patient needs, growing and sustaining the NHS[1], etc. Though focus on patient care is necessary and important, complete lacking in acknowledgement of security in healthcare is unacceptable. As a pressing issue in and dangerous component of healthcare, security cannot be deemphasized. Estimates on individual NHS trust spending on cybersecurity ranges from £0-£100,000/year, with an average of only £23,040 annually per individual organization[10]. IT generally only receives 1-2% of their annual budget[6]. Only 10% of NHS organizations have followed even the most basic encryption recommendations by experts[10]. The emphasis and allocation of the budget within security also tends to be on prevention through software alone[7], with little consideration for user education, updating of existing infrastructure, security information, or incident response.

Healthcare data often gets equal security emphasis as other parts of the government, despite the data being much more sensitive. Governmental consequences of these breaches are often confined to fines (that may be large but are still not proportional to the amount of damage caused[8]). Patients also often don't have any other option for care and have little agency when breaches occur. The NHS has launched a Care Computer Emergency Response Team (CareCERT) by requirement and commission by the Department of Health. While this step is important in the clearly lacking technical support, the many politicians touting this move as a "milestone" are allowing an externalized solution from the systemic operations within the industry to serve as a complete fix. While technical support should increase, so should the practices in the user end of this technology as well as the understanding of these practices.

2.3 Summary of Contributing Factors

The short of "what went wrong?" in the WannaCry breach consists of three overarching adequacies: (1) technical shortcomings comprised of general cybersecurity concerns, (2) systemic and behavioral norms in the healthcare sector that should be unacceptable in the climate of today's cybersecurity risks, and (3) governmental regulation, response, and focus concerning cybersecurity in healthcare. Not only do the risks need to be more widely acknowledged and given more than a PR/surface-level fix, but the whole approach in understanding potential solutions must be more holistic.

3 Addressing the Problem

The following section will be a compilation of general changes, some of which may seem obvious (yet are still not implemented), that should be considered by healthcare organizations in order to prevent, address, and respond to data insecurity in the field. These suggestions for moving forward include augmentations at all levels of the issue, from technical changes to improvement in communication. The needs of healthcare security are specific and should be addressed as such.

Incentive is currently a large barrier to improvement. Despite the creation of groups that prioritize security at both the government-level and organization-level, financial incentive often lies in incorporating new technology rather than in securing technology[4]. Without financial support for increased data security or increased financial consequence for breaches that outweigh cost of prevention, healthcare providers can hardly be expected to prioritize something with an already lower level of awareness than the more obvious problems in healthcare. Collaboration with healthcare stakeholders on protection of sensitive data should be increased, and general financial incentive should be employed.

Additionally, regulations that do exist tend to be insufficient in providing avenues for compliance without compromising physical care of patients. On this end, policy makers should be more focused on

developing specifically relevant common security standards[6,9] for the healthcare sector. Clear procedures should be set in place at the organizational level and should cover all aspects of data insecurity, not simply what provides a reassuring sound bite. An alternative nationally recognized/implemented patient identification system should also be considered[9], as the usage of SSNs puts permanent sensitive information at too great a risk.

Finally, on the technical level, many existing security measure should be implemented and maintained within healthcare organizations. Based on the vulnerabilities that are commonly exploited in these institutions, recommendations consist of measures involving network security, malware prevention, risk management, observing updates, physical security (ex. limited access to removable hardware), consistent monitoring, user privilege regulation, whitelisting, testing, encryption, virtual local area network implementation, protection against deauthentication attacks, and incorporation of regular assessments[6]. At the crux of this technical component are user education and awareness *and* prioritization by organization leaders, because despite the existence of these technological practices and fixes, proper usage and prevention through these changes cannot occur without intentional employment.

Conclusion

A microcosm of the larger issue will serve to close, using the example of CONNECT to demonstrate the permeation of security deficiency. Originally developed by federal agencies in the pursuit of secure health information sharing and data exchange, CONNECT is a now open source software used in more than 2,000 organizations ranging from the local to national level[12]. This software solution won many awards and has facilitated important work. It was approved for meeting the standards of the National Health Information Network by the Office of the National Coordinator for Health Information Technology (ONC), the highest-level administration of health IT and a position created through executive order and mandated through HITECH[12].

While this software does not necessarily have all the glaring issues that this paper has previously discussed about other instances, a closer examination of the software raises a few rather alarming questions, especially given its glowing reputation. As much as open source software is extremely powerful and widely used by top developers, there are security risks that come with it. Large attack surfaces, fragmented vulnerability information, and lack in awareness all contribute to this.

Running a simple VeraCode static scan (which may not detect all shortcomings) on this software reveals at least six medium-level flaws (refer to attached supporting material). These include CRLF injection, cross site scripting, cryptographic issues, directory traversal, encapsulation, and improper neutralization of HTML injected scripts. For a lower policy evaluation, these flaws may not have been as significant, but with the level of importance of the data being handled by this software, these flaws are both surprising and troubling. Additionally, users should implement the most recent versions, as older versions may show even more vulnerabilities, and find secure ways of integrating this software within existing frameworks. Despite the federal involvement, not only in approving and endorsing this software, but also in producing it, there seems to be a lower than expected standard of security.

In all likelihood, of widely used data-exchange software, usage of CONNECT may be generally safe and perhaps even relatively more secure. This should not be the standard, however, as a simple static scan revealed several exploitable flaws of considerable concern. Other more widely used healthcare data-exchange software packages, even those utilized by powerful and respected institutions (universities, hospitals, government groups), often contain many easily exploitable vulnerabilities, rooted in anything from dependency issues to problematic design to anything in-between. The issue of cybersecurity in software is not solely a security expert problem— the issue requires organizational reprioritization and behavioral changes, and governmental monetary/policy reconsiderations as well.

References

[1] (n.d.). Retrieved from https://www.england.nhs.uk/allocations/
[2] Davis, J. (2017, May 12). UPDATED: Hospitals in UK National Health Service knocked offline by massive ransomware attack. Retrieved from http://www.healthcareitnews.com/news/updated-hospitals-uk-national-health-service-knocked-offline-massive-ransomware-attack
[3] Fruhlinger, J. (2017, September 27). What is WannaCry ransomware, how does it infect, and who was responsible? Retrieved from https://www.csoonline.com/article/3227906/ransomware/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html
[4] Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. K. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technology and Health Care,25*(1), 1-10. doi:10.3233/thc-161263
[5] Leventhal, R. (2017, January 24). Report: Healthcare Sector Hit Hard in 2016 by Data Breaches. Retrieved from https://www.healthcare-informatics.com/news-item/cybersecurity/report-healthcare-sector-hit-hard-2016-data-breaches
[6] Martin, G., Martin, P., Hankin, C., Darzi, A., & Kinross, J. (2017). Cybersecurity and healthcare: How safe are we? *Bmj*. doi:10.1136/bmj.j3179
[7] Matthews, E. D.,U.S.A.F.(R.E.T.). (2017). I just wanna cry again, this time over ransomware. Signal, 71(11), 56. Retrieved from https://login.ezproxy.library.tufts.edu/login?url=https://search.proquest.com/docview/1923220433?accountid=14434
[8] Mohammed, D., Mariani, R., & Mohammed, S. (2015). Cybersecurity Challenges and Compliance Issues within the U.S. Healthcare Sector [Abstract]. *International Journal of Business and Social Research,5*(2), 55-67.
[9] Murphy, S. (2015). Is Cybersecurity Possible In Healthcare [Abstract]. *National Cybersecurity Institute Journal,1*(3), 49-62.
[10] Reeve, T. (2016, November 17). Inadequate cyber-security budgets 'putting NHS patients at risk'. Retrieved from https://www.scmagazineuk.com/inadequate-cyber-security-budgets-putting-nhs-patients-at-risk/article/573932/
[11] Snell, E. (2016, January 25). What are Top HIPAA Compliance Concerns, Obstacles? Retrieved from https://healthitsecurity.com/news/what-are-top-hipaa-compliance-concerns-obstacles
[12] The CONNECT Open Source Solution A Gateway to the ... (n.d.). Retrieved from https://www.healthit.gov/sites/default/files/pdf/fact-sheets/connect-open-source-solution.pdf
[13] WannaCry: Who's to blame for worst ransomware attack ever? (2017, May). Web User, , 8-9. Retrieved from https://login.ezproxy.library.tufts.edu/login?url=https://search.proquest.com/docview/2010820113?accountid=14434
[14] Woollaston, V. (2017, May 16). Wanna Decryptor ransomware appears to be spawning and this time it may not have a kill switch. Retrieved from http://www.wired.co.uk/article/wanna-decryptor-ransomware