Why Healthcare Sucks at Cybersecurity

Andrew Sterner*

December 13, 2017

Abstract

Healthcare is uniquely vulnerable to cybersecurity threats. Due to consumer, internal and government pressure, electronic health records have been adopted to aid flow of patient information. This compounded with the explosion of the internet of things (IoT) and adoption of connected medical devices has lead to a corresponding increase in hacks and near misses. These incidents range from serious information leaks to possible denial of medical service for patients. The threats are grave and the consequences cannot be over stated. Unfortunately these attacks don't seem to be going away. Healthcare organizations seem to be unable to stop the tide of attacks. This article explores the policy that has lead to this crisis, unique vulnerabilities that healthcare faces and suggests possible solutions.

*Mentored by Ming Chow

Contents

1 Introduction

The state of cybersecurity in healthcare is dire. With practically universal adoption of electronic health records (EHRs) and increasing reliance on connected technology there has been a worrying trend of information leaks, hacks and near misses. Attacks such as the WannaCry ransomware attacks highlight the possibility of vulnerabilities that could cripple essential healthcare infrastructure.

In 2015, a single hack on Anthem Inc. compromised 79 million EHRs [11]. To rephrase, a quarter of the population of the United States had their medical records stolen. Since 2015 there have been no (known) breaches of that scale, however there is a clear and consistent increase in number of breaches per year. This issue isn't going away. Despite increased spending and legislation it's hard to see an end in sight without deep institutional and cultural changes.

Legislation passed during the Bush and Obama administrations has been incredibly successful in promoting the adoption of EHRs. These acts were written with the intent of bringing our healthcare system into the 21st century and to protect patient privacy. However, the enacted policy fails to preempt attacks, and contributes to reactionary culture. The merits of EHRs are enticing, but rapid development has lead to endless vulnerabilities. Electronic health systems were adopted before an IT support system existed to effectively address implementation or security. In fact many small healthcare organizations can't afford IT of any kind. The current system of patch-and-pray rapid development leads to buggy software which in many cases was not even tested for security issues. Furthermore there exists a culture of healthcare providers and application developers which doesn't understand or doesn't care about security threats. This culture breeds vulnerabilities from weak passwords to phishing risks. To have some semblance of healthcare cybersecurity we need serious culture change in those developing healthcare technology and those using it as well as stronger regulations on those handling sensitive data.

2 To the Community

Have you ever seen a Doctor? Do you have health insurance? Well then there's a good chance that private information about you is in the hands of

a hacker – or whoever they sold it to. If you are not worried about your personal medical information in the hands of a malicious party or the public (nice enhancements Dave!), there's much more to be concerned about. Stolen records often include financial information. This means access to your Social Security Number, credit cards as well as possibly the first street you lived on or your mothers maiden name. This information not only gives hackers possible direct access to lines of credit, it allows them to impersonate you, to apply for credit cards in your name or possibly use your information for medical fraud. Accenture predicts that 25% of patients who have their data stolen will be the target of some kind of identity theft [1]. This detailed data can be exploited in too many ways to name.

If you're hoping that your information has not been compromised, think again. Since they started keeping track in 2009, HHS has tracked 173 million stolen records [11]. That's more than half the population of the United States, and that's just what is known and reported. There is a likelihood there are leaks we haven't caught yet, and most experts believe that these leaks aren't going away any time soon.

3 Major Legislation

The lack of proper information and enforcement of rules has lead to ineffective legislation surrounding healthcare privacy. Essential data such as estimates of losses caused by information leakages are notoriously hard to pinpoint. This is evidenced in a government report on the 2013 Target hack which had a range of $240 million to $4.9 billion in damages [16]. This lack of information compounded with a rapidly changing technological landscape makes it difficult to write lasting effective legislation.

The legislation that is passed allows entities with access to sensitive information too much latitude to develop their own privacy and security policies. At the same time enforcement of these policies is arbitrary and retroactive. The agency in charge of the enforcement of HIPAA is the Office of Civil Rights (OCR). Correctional or technical action taken by the OCR in 17% of reported cases in 2003. Enforcement peaked in 2013 at 43% and seems to be on a rise again. Corrective action has ramped up as huge data breaches have been reported to make examples of offending entities. This reaction has led to a scramble to fix gaping weaknesses but it is too late. We are now patching the system rather than ensuring it was secure as it was being

developed.

The next sections summarize and analyze two major pieces of legislation in regards to EHRs: the Health Insurance Portability and Accountability Act (HIPAA) passed under Bill Clinton in 1996, and a major addition to these rules, the Heath Information Technology for Economic and Clinical Health Act (HITECH).

3.1 HIPAA

Title II of HIPAA dictates how sensitive "protected health information" (PHI) is handled and secured. This can be broken into two sections: the privacy rule and security rule.

3.1.1 Privacy Rule

This rule outlines who has access to PHI. In short you, law enforcement and your healthcare providers have access to your PHI. However, your healthcare provider can share this information with various "business associates" without your consent [4]. For example, those with access to PHI can distribute this data:

- "To pay doctors and hospitals for your health care and to help run their businesses"
- "With your family, relatives, friends, or others you identify who are involved with your health care or your health care bills, unless you object"
- "To make sure doctors give good care and nursing homes are clean and safe"

Other reasons include mandatory rules for police reporting and for protection of the public health [6].

While this policy allows more efficient care (you don't need to sign HIPAA disclosure forms for each insurance charge), it has created an elaborate web of entities that have access to PHI. The number of entities that were expected to apply for access to this information was estimated at 701,325 in a 2010 HHS report [10]. These entities employ millions of employees and a patchwork of systems that we trust to safely handle this sensitive information. It is easy to

imagine how one weak link can expose a disastrous amount of information, and there are too many attack surfaces to protect.

Organizations are supposed to follow a "minimum necessary" requirement, but the minimum shared information is determined by the parties sharing the information which does not allow effective enforcement of this rule. The privacy rule dictated by HIPAA is too lax in the modern information sharing era. These rules need to be rewritten to hold entities responsible for reasonable disclosure of data, and to limit the entities this data is released to.

3.1.2 Security Rule

The security rule attempts to standardize requirements for security of electronic PHI. It generally requires a risk analysis and implementation of security "safeguards". These are grouped into three categories. "Administrative safeguards" require the designation of a "security official", training of workforce in safe practices, and security evaluation [5]. "Physical safeguards" are required to limit access to PHI. "Technical safeguards" require the use of "access control", "audit controls" (which allow logging of access and activity), "integrity controls" and ensure "transmission security". A record of these policies must be kept, but there doesn't exist a system to ensure an entity is complying until a complaint is reported to the OCR. Additionally most of these rules are marked as "addressable" which means that the organization is allowed to implement these security practices as they see fit.

This self-policing with retroactive external reprocussions has contributed to, and has been enhanced by a lack of technical security knowledge. There is an absence of cybersecurity talent in general. Small medical practices are unlikely to have full time employees with an IT background let alone cybersecurity knowledge. It's not financially feasible to expect these organizations with small operating margins to really invest in cybersecurity. Even large organizations struggle with this. Entities surveyed by the Wall Street Journal revieled that their management has very little knowledge of cybersecurity [7].

The security rule requires protection against "reasonably anticipated threats to the security or integrity of the information" [5]. These protections will be ineffective until those making and enforcing the rules understand the threats enough to build an adequate defense.

Speaking to an an acquaintance who worked for an entity that handled PHI did nothing to allay my fears. They were given access to PHI before they

completed mandatory training. Without proper education and enforcement the breaches will not stop.

3.2 HITECH

The HITECH act was passed under President Obama as a compliment to HIPAA to facilitate the transition to EHRs. It provided $36.5 billion in funding to subsidize the adoption of EHRs [14]. $27 billion of this funding went to subsidies of up to $63,750 towards organizations that adopt "meaningful use" of EHRs [15]. Additionally in 2015, financial penalties kicked in for organizations that have not demonstrated use of EHRs. This act requires reporting of any PHI breach affecting more than 500 records to the OCR, to news media organizations and any individuals affected.

This legislation was incredibly effective, According to the HHS Office of the National Coordinator for Health Information Technology Basic EHR records have been adopted by 83.8% of hospitals as of 2015, a massive increase from 9.4% in 2008. 96% have certified EHR [12]. This is seen as a triumph of the Obama administration which pushed our healthcare system into the 21st century. While this is true, this rapid development occurred without enough consideration of the outdated privacy laws outlined in HIPAA. As evidenced by the continued rise of EHR breaches, HITECH did not do enough to protect patient privacy in a fast moving world.

4 Action Items

Medical data is especially valuable to hackers. As of 2015 medical records go for about $50 which is about 10 times the price for a single credit card [2]. This means that hackers will continue to try to find ways to exploit health technology. The threat will never go away, but the current state of affairs makes it much to easy for groups to steal data and threaten infrastructure. There is no single easy fix, the issue of cybersecurity is deeply institutional and therefore will take time to correct, but there are several steps we need to take to make the problem much less grim. We must hold application developers to higher standards, educate those using and benefiting from health technology, improve policy and consolidate sources of information.

4.1 Hold Developers to Higher Standards

According to Veracode, 80% of healthcare applications scanned have cryptographic issues. They also found that only 43% of vulnerabilities found in Veracode scans were fixed. This is unacceptable. This is sensitive personal information, not a wordpress blog. Developers need to take these security issues seriously, and at a minimum patch up issues found in simple security scans. These are complicated applications, there will be vulnerabilities and bugs, but many of the exploited vulnerabilities are simple and preventable. The top concern of healthcare organizations is of application vulnerabilities such as SQL injection. A different Veracode survey found that 60% of in-house applications aren't even tested for vulnerabilities [3]. These issues are found in every industry, and largely stem from computer science education that in many cases doesn't mention security. Developers need to understand that functional doesn't equal secure.

4.2 Educate Health Technology Consumers

The second step is educating those using health technology. A recent government Health Care Industry Cybersecurity Taskforce report found that "many providers and other health care workers often assume that the IT network and the devices they support function efficiently and that their level of cybersecurity vulnerability is low" [8]. Until this mentality is changed, no real progress will be made. Many issues in healthcare cybersecurity stem from employee and management ignorence and negligence. There are endless forms of social engineering such as phishing that employees need to avoid. There are cases where data is stolen or lost. For example, in 2006, a VA employee who had taken home data (without permission) had PHI of 26.5 million veterans stolen [9]. Recently, WannaCry ransomware paralyzed hospitals in the British NHS. This attack would not have happened if computers were simply patched [13]. These unpatched computers as well as legacy systems are prolific in healthcare. Without proper knowledge these systems can serve as access points to disrupt entire systems. We won't be able to stop malicious providers stealing information, but we can educate and stop easily preventable incidents.

4.3 Consolidate Rules and Guidance

The guidelines, and repercussions written to secure our healthcare system are obsolete and ineffective. We must provide much more stringent rules that are informed by cybersecurity experts with input from the private sector. The Health Care Industry Cybersecurity Taskforce is one such effort to overhaul legislation. Its members include the CISO of Anthem Inc. and the Health Information Technology Officer of Symantec Corp, experts in the field. This taskforce is advocating for the nomination of a "Cybersecurity leader for sector engagement" who will lead policy changes and serve as an interface between HHS and the private sector.

Legislation needs to remove the arbitrary rules defined by the organizations themselves and allow proactive enforcement of privacy protections. Current rules give too much leeway to healthcare organizations to define threats and their defenses. This leads to an enforcement scheme that is retroactive and causes healthcare organizations to default to a patch-and-pray development scheme. Rules that mandate security audits such as scans and penetration testing could potentially remove low hanging fruit. Until this happens we will be stuck in the cycle of scrambling to plug holes rather than building applications consumers can trust.

5 Conclusion

There is no foreseeable end to cybersecurity threats, especially in healthcare. However, the current state of security is unsustainable. The HIPAA and HITECH acts while effective in some areas, don't do enough to protect patient data. In fact these acts contribute to a prevalent patch-and-pray culture. Additionally it doesn't fix deeper defects due to lack of developer and provider knowledge surrounding healthcare. To fix these outstanding issues we must hold developers to a higher standard, revise current policy and educate all involved in healthcare from patients to providers.

References

[1] Accenture. *Cyberattacks Will Cost U.S. Health Systems $305 Billion Over Five Years, Accenture Forecasts*. 2015. URL: https://newsroom.accenture.com/news/cyberattacks-will-cost-us-health-

systems-305-billion-over-five-years-accenture-forecasts.htm.

[2] Arthur Allen. *Billions to install, now billions to protect*. 2015. URL: https://www.politico.com/story/2015/06/health-care-spending-billions-to-protect-the-records-it-spent-billions-to-install-118432.

[3] Doug Bonderud. *HIPAA Compliance and the Healthcare Supply Chain: Broken Links?* 2014. URL: https://www.veracode.com/blog/2014/10/hipaa-compliance-and-healthcare-supply-chain-broken-links.

[4] Office for Civil Rights. *Summary of the HIPAA Privacy Rule*. 2013. URL: https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html.

[5] Office for Civil Rights. *Summary of the HIPAA Security Rule*. 2013. URL: https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html.

[6] Office for Civil Rights. *Your Rights Under HIPAA*. 2017. URL: https://www.hhs.gov/hipaa/for-individuals/guidance-materials-for-consumers/index.html.

[7] Katie Dvorak. "Board Members at Healthcare Orgamizations Lack Understanding of Cybersecurity Risks". In: *FierceHealthIT* (2015).

[8] Health Care Industry Cybersecurity Task Force. *Report on Improving Cybersecurity in the Health Care Industry*. Report to congress. Department of Health and Human Services, 2017.

[9] Judy Foreman. "At risk of exposure". In: *Los Angeles Times* (2006).

[10] US Department of Health, Human Services, et al. "Modifications to the HIPAA Privacy, Security, and Enforcement Rules Under the Health Information Technology for Economic and Clinical Health Act; Proposed Rule. 75 Fed". In: *Reg. 40868, 40893-40894 (July* 14 (2010).

[11] HHS. *Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information*. 2017. URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

[12] MPH JaWanna Henry et al. *Adoption of Electronic Health Record Systems among U.S. Non-Federal Acute Care Hospitals: 2008-2015*. 2016. URL: https://dashboard.healthit.gov/evaluations/data-briefs/non-federal-acute-care-hospital-ehr-adoption-2008-2015.php.

[13] Microsoft. *Customer Guidance for WannaCrypt attacks*. 2017. URL: https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/.

[14] R O'Harrow. "The machinery behind health-care reform". In: *Washington Post* (2009).

[15] Robert Pear. "Standards issued for electronic health records". In: *New York Times* 13 (2010).

[16] N Eric Weiss and Rena S Miller. "The target and other financial data breaches: Frequently asked questions". In: *Congressional Research Service* (2015).