F. Lau et al. (Eds.)

© 2019 The authors and IOS Press.
This article is published online with Open Access by IOS Press and distributed under the terms of the Creative Commons Attribution Non-Commercial License 4.0 (CC BY-NC 4.0).

doi:10.3233/978-1-61499-951-5-218

Healthcare Data Are Remarkably Vulnerable to Hacking: Connected Healthcare Delivery Increases the Risks

Ross KOPPEL[a,1] and Craig KUZIEMSKY[b]
[a] *University of Pennsylvania, Philadelphia, PA, USA*
[b] *Telfer School of Management, University of Ottawa, Ottawa, ON, Canada*

Abstract. Healthcare data are attractive to cyber-criminals because they contain financial and personal data, can be used for blackmail, and most valuable, are ideal for fraudulent billing. They are also remarkably vulnerable to penetration because of the fluid and always-evolving nature of a patient's medical care and because of the number of clinicians, facilities and transactions required to connect patient care across multiple settings. The addition of mobile healthcare devices and connected healthcare delivery systems (e.g., wearables, monitoring devices, cell phone images) makes healthcare data more attractive but also more vulnerable. Wide variations of digital health use patterns complicates design security solutions for each context or clinician. In this paper we propose a set of connected healthcare patterns, and then discuss security challenges and potential solutions for each of the connected health patterns.

Keywords. Cybersecurity, mobile healthcare, connected healthcare delivery.

1. Introduction

Healthcare data—especially electronic health records—are worth ten to thirty times more on the black market than are credit card numbers. A cyber-thief can buy stolen bulk credit card numbers for anywhere from about $2.50 to $10 a number. In contrast EHR data are approximately worth up to $65.00 each. Why this difference? A credit card can be used once or a few times. But a healthcare record: 1. Has your credit card number anyway and your national insurance ID; 2. Can be used for blackmail; and 3. Most important—is the gift that keeps on giving if used by unscrupulous medical providers. Thus, a physician, or physiotherapist, or pharmacy can bill the government or an insurance company for millions of dollars. In the US, healthcare fraud cost is estimated at over $100 billion/year [1]. And the unscrupulous vendor or provider will know exactly the kind of services, procedures or supplies appropriate for each patient. The fraud is aided by incomprehensible (and intentionally opaque?) medical billing processes and the reality that a lot of sick people are not carefully examining the Byzantine paperwork that accompanies any medical event.

There are several reasons why healthcare data are vulnerable to security breaches. First is that today's medical infrastructure has been adapted from conventional

[1] Corresponding Author

computing, and was not designed with the needs of health care. Hence the current generation of micro-processor-based health care equipment is usually better suited to office-like and traditional data processing workflows than to clinical environments. This is especially clear in the use of passwords as an access control mechanism. Second, many of today's medical devices were first designed as stand-alone devices, not as networked components. They lack the basic functionality needed for their new role. Integrating legacy medical devices into the new networked architectures requires a large amount of new software and integration processes creates novel security problems that never existed for the stand-alone design. As an example, a stand-alone insulin pump assumes a single or at most a small number of login accounts for operators. In contrast, when networked, any of the patient's clinicians may need to log into the device, and so the authentication system needs to be re-worked from scratch to integrate into the facility's network-wide authentication framework.

Perhaps the most significant challenge is that modern healthcare delivery is defined by delivery models such as collaborative care delivery where people, processes and technologies need to be connected across multiple providers and settings. A patient may have several health records which must travel across all of these system boundaries to satisfy all of the clinical, scientific, and business objectives involved in that patient's care and billing. While a traditional model of healthcare delivery system has one patient record in one electronic system that is accessible by everyone, we know that is not the reality of healthcare delivery. At a micro level, attempts to manage complex care delivery such as chronic disease management and patient participatory medicine often require the connection of data from multiple systems or devices. At a macro level, there is also a desire to enable system wide analytics and learning, which requires access and analysis of data from multiple systems.

Healthcare IT promises—and often delivers–-faster, better, and more comprehensive medical care. But underlying those promises is the assumption that patient data in the IT systems are secure; and that the safety of the software used to collect, analyze, present and transfer that information is not easily compromised. Still, there are good reasons to doubt the data security of various models of healthcare delivery. Overall, it remains a challenge to define the security requirements for connected health systems, particularly when the ecosystem involves emerging technologies such as mobile devices [2]. While it is impossible to predict all possible patterns of connected health delivery, we can make general inferences about patterns of connectivity that would allow us to better understand security issues with connected healthcare delivery and how to prevent them. This paper addresses the above need and develops three connected healthcare patterns according to the formality and extent of connectivity. We then describe security challenges and potential solutions for each of the three patterns.

2. Modeling Connected Health Patterns

We propose a two-stage model: The first stage reflects the existing and emerging patterns of healthcare delivery that integrates the many different medical facilities and clinicians. We draw on our previous work of different telehealth delivery patterns [5]. The second stage addresses the security needs associated with each pattern. For this, we build on the research on security implications of healthcare devices within smart homes and with the use of mobile healthcare devices. We then seek to integrate the frameworks by analyzing the set of patterns and security considerations for the varying connected healthcare delivery configurations.

Connected healthcare delivery can be broadly defined as a consumer-centered healthcare delivery model that uses different information and communication technologies (ICT) to connect information sources and processes across the entire health care system [3]. In plain words, this is about how patients and medical systems' EHRs connect. There are substantial variations in the type and number of technologies used to enable that connectivity; and the technologies affect the security needs of each ICT type and complexity. Another consideration is the extent to which a system is formal or informal. A hospital EHR system is always a formal system, while an iPhone app is usually an informal system. Last, we must address the number of ICTs used to allow connectivity. The more ICTs used, the greater the degree of connectivity complexity.

2.1. Connected Health Patterns

Drawing upon the approach described above we develop three connected health patterns according to the number of ICTs and the degree of formality:

One-to-One – This is the most basic pattern. The provider has a formal EHR system and patients can access their records at home via the internet using a dedicated login screen. All patient data are viewed and transacted through the EHR. The One-to-One pattern is the least complicated as the connectivity complexity can be defined *a priori.*

One-to-Many – Patient data are accessed through more than one formal EHR system. This pattern would occur when patient data are exchanged through multiple systems such as a provider EHR and other HIT systems within a hospital or other clinics. One-to-many patterns are moderate in complexity as users may have multiple logins to enable system access or data may need to be integrated across multiple systems to provide a comprehensive picture of a patient's health.

Many-to-Many – Patient data are collected and exchanged through multiple apps and tools, both formal and informal. Patients may use Fitbits, iPhones or other apps to collect, store data, and transmit their healthcare information as well as accessing one or more formal EMR system from their provider(s). Many-to-Many configurations are the most complex because one can seldom predict the degree of connectivity that will occur as new connections may evolve through patient use of social media or other eHealth tools.

3. Results - Security Challenges and Potential Solutions for the Connected Health Patterns

3.1. One-to-One

Despite being the least complex of the connected health patterns, one-to-one connectivity is still prone to security breaches; and challenges can exist at individual and organizational levels. Individual level connectivity involves a patient or family member accessing data. It starts with creating secure passwords that are not shared with other individuals. Individuals also need to be aware of differences in security risks depending on the devices used to access their medical record.

A desktop or laptop computer typically is more secure than a smartphone, as a smartphone is not a single technology but rather many digital components, each which can be compromised [2]. Smartphone information usually travels through insecure and open communication channels. Patients also need to be aware that all inquiries and transactions about their data need to take place within the formal EHR system. Studies have highlighted how patients are increasingly using social media tools such as Facebook to show data or engage in communication about their health [4], or will use communication channels such as e-mail to communicate with providers. These actions turn formal systems into informal ones and increase security challenges accordingly.

At an organizational level, healthcare settings (e.g., hospitals) need to ensure they have technical safeguards such as data backups, firewalls et cetera for securing system access and transmitting data [6]. Healthcare organizations also need to have administrative security safeguards such as a security plan, protocols for how data can be accessed, and a strategy for how data will be anonymized for research and other purposes.

3.2. One-to-Many

One-to-many connectivity subsumes the security challenges from one-to-one connectivity while also introducing some new ones. Most significant is understanding how data will be integrated across multiple formal systems. Vulnerabilities are amplified when connectivity occurs across multiple systems, vendors, security safeguards and logins/access points. Multi-level connectivity also introduces challenges about what information the many systems convey when collectively combined. For example, some administrators believe that removing key personal identifiers is sufficient to anonymize patient data for system-wide analytics and learning. However, that effort may be defeated when the data from several sources are combined.

3.3. Many-to-Many

The design of human-computer interfaces of health devices focus only on each device's individual cyber security controls. However, critical here, the interaction of many devices linking to the EHR means security should incorporate *collective (network)* cyber security. That is, formal medical devices will interact with informal medical devices (e.g. Fitbits, heart rate monitors, smart phone apps) in *ad hoc* or even in intentional networks to create additional security vulnerabilities. Worse, available security settings seldom enable users to effect more complex security controls in network settings.

To address these issues, security must now address the reality of multiple users of devices (e.g., infusion pump used by many). Moreover, the security settings and controls should reflect use by different categories of users - adults vs. children; patients vs clinicians, as well as different types of connectivity (e.g. formal vs informal).

4. Recommendations

Addressing the above security challenges is an interdisciplinary endeavor. We present recommendations at two levels. At a technical level, medical devices should be designed with the functionality and controls to allow or prohibit the collection and transmission of data from the user or device to the EHR and/or to others (e.g. clinicians, parents).

At an administrative or policy level, we need to improve the often incomprehensible security instructions and explanations for network security both for individual devices and for one and many to many networks that require *collective (network)* cybersecurity.

To that end, instructions and control designs must be tailored to the many different levels of users' understanding needed to appreciate the network-level vulnerabilities. As with the tragedy of the commons, some solutions require policies that incorporate more than one developer and more than one user. That is, the combination of a large number of devices at least multiplies the danger of any vulnerability and potentially leads to new vulnerabilities. A user may be overwhelmed by this combination. Thus, while device developers have the responsibility to provide secure settings for their own devices, they will probably not be aware of the other devices in use, nor are they aware of shortcuts and workarounds which may be motivated by the connectivity of multiple devices. An important mismatch therefore is what the developer might consider adequate for safety thinking about their suite of medical devices. Addressing that mismatch needs a policy-level intervention that governs the integrated picture of medical security.

5. Conclusion

A fundamental system design challenge for connected health is that we often cannot predict requirements ahead of time due to the always evolving nature of connected health systems. This makes security monitoring and governance particularly challenging. Patients are increasingly willing to share their healthcare data assuming that the data will be shared securely, but managing healthcare security must address the growing complexity and connectivity of systems, participants and devices. As healthcare delivery shifts from hospital to community-based care, and patient participatory medicine becomes a driver of healthcare delivery, the number of connected health touchpoints will increase. Another issue is the role of social media involving healthcare and the growing pool of healthcare smartphone apps. All of these increase the number of touchpoints, the cybersecurity attack surface (vulnerabilities), and the potential for security breaches.

References

[1] Fraud Statistics | bcbsm.com, (n.d.). https://www.bcbsm.com/health-care-fraud/fraud-statistics.html (accessed November 13, 2018).

[2] G.S. Brost and M. Hoffmann, Identifying Security Requirements and Privacy Concerns in Digital Health Applications, in: *Requirements Engineering for Digital Health,* S.A. Fricker, C. Thümmler, and A. Gavras, eds., Springer International Publishing, Cham, 2015, pp. 133-154.

[3] N. Carroll, C. Kuziemsky, and I. Richardson, Software engineering for connected health (journal first session), in: *Proceedings of the 2017 International Conference on Software and System Process*, ACM, Paris, France, 2017, pp. 3-4.

[4] M. Househ, Sharing sensitive personal health information through Facebook: the unintended consequences, *Stud Health Technol Inform* **169** (2011), 616-620.

[5] C.E. Kuziemsky, S.B. Gogia, M. Househ, C. Petersen, and A. Basu, Balancing Health Information Exchange and Privacy Governance from a Patient-Centred Connected Health and Telehealth Perspective, *Yearb Med Inform* **27** (2018), 48-54.

[6] F. Rezaeibagha, K.T. Win, and W. Susilo, A Systematic Literature Review on Security and Privacy of Electronic Health Record Systems: Technical Perspectives, *Health Information Management Journal* **44** (2015), 23-38.