Contents lists available at ScienceDirect

Maturitas

journal homepage: www.elsevier.com/locate/maturitas

Cybersecurity in healthcare: A narrative review of trends, threats and ways forward

Lynne Coventry[*], Dawn Branley

Northumbria University, Newcastle upon Tyne, UK

ARTICLE INFO

Keywords:
Cybersecurity
Medical devices
Electronic health record

ABSTRACT

Electronic healthcare technology is prevalent around the world and creates huge potential to improve clinical outcomes and transform care delivery. However, there are increasing concerns relating to the security of healthcare data and devices. Increased connectivity to existing computer networks has exposed medical devices to new cybersecurity vulnerabilities. Healthcare is an attractive target for cybercrime for two fundamental reasons: it is a rich source of valuable data and its defences are weak. Cybersecurity breaches include stealing health information and ransomware attacks on hospitals, and could include attacks on implanted medical devices. Breaches can reduce patient trust, cripple health systems and threaten human life. Ultimately, cybersecurity is critical to patient safety, yet has historically been lax. New legislation and regulations are in place to facilitate change. This requires cybersecurity to become an integral part of patient safety. Changes are required to human behaviour, technology and processes as part of a holistic solution.

1. Introduction

Healthcare technologies have the potential to extend, save and enhance lives. Technologies range from those providing storage of electronic health records (EHRs); devices that monitor health and deliver medication (including general purpose devices and wearables, and technology embedded within the human body); to telemedicine technology delivering care remotely – even across countries. Patients increasingly use their own mobile applications, which can now be integrated with telemedicine/telehealth into the medical Internet of Things [1] for collaborative disease management and care coordination.

As healthcare devices continue to evolve, so does their interconnectivity. Whilst traditionally standalone, many are now integrated into the hospital network. There are currently 10–15 connected devices per bed in US hospitals [2]. Interconnection has many benefits—e.g., efficiency, error reduction, automation and remote monitoring. These benefits are transforming the treatment of both acute and chronic long-term conditions. Interconnected technology outside of the clinical environment allow health professionals to monitor and adjust implanted devices without the need for a hospital visit or invasive procedures. EHRs can improve patient care by making health information more broadly available [3]. Unfortunately, interconnection introduces new cybersecurity vulnerabilities. Cybersecurity is concerned with safeguarding computer networks and the information they contain from penetration and accidental or malicious disruption. There are growing concerns that cybersecurity within healthcare is not sufficient and this has already resulted in a lack of medical information confidentiality [4] and integrity of data [5,6].

Of course, privacy breaches were a concern prior to the emergence of digital health records. However, the interconnectivity of today's records provides multiple potential gateways to access; the ability to access remotely (whereas historically paper records would have been safeguarded within hospitals and only accessible via physical breaches); the ability for data theft to go unnoticed; and access to a more complete health record providing a more valuable resource for potential attacks (whereas previously health records may have been split between many different hospital(s)/departments). Historically, misplaced paper records or a stolen laptop may have exposed hundreds or thousands of patients to a potential date breach, now that this information is electronic and available on numerous networks, a privacy breach has the potential to affect millions of people [7]. To illustrate further, celebrity health records have always been a target for breaches [8]. However prior to the emergence of electronic records, these breaches were limited to hospital staff who could gain access to the physical paperwork. Now celebrity health records can be potentially remotely accessed—increasing the potential for breaches. That said, electronic records also have a key privacy benefit over paper records—the ability to track staff access (a recent report suggests that over half of healthcare breaches come from inside the organisation [8]). Whereas previously it

---

[*] Corresponding author at: 153 Northumberland Building, Northumbria University, Newcastle upon Tyne, NE1 8ST, UK.
E-mail address: Lynne.coventry@northumbria.ac.uk (L. Coventry).

https://doi.org/10.1016/j.maturitas.2018.04.008
Received 2 March 2018; Received in revised form 16 April 2018; Accepted 18 April 2018
0378-5122/

aceghijlmnoprstuvw./:

*

abcdefgilmnopqrstuvwyBHINTUW?

1adghnoprstuB

fiffiff