


REVIEW

Open Access



# Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks

Salem T. Argaw<sup>1</sup>, Juan R. Troncoso-Pastoriza<sup>2</sup>, Darren Lacey<sup>3</sup>, Marie-Valentine Florin<sup>4</sup>, Franck Calcavecchia<sup>5</sup>, Denise Anderson<sup>6</sup>, Wayne Burluson<sup>7</sup>, Jan-Michael Vogel<sup>8</sup>, Chana O'Leary<sup>9</sup>, Bruce Eshaya-Chauvin<sup>1</sup> and Antoine Flahault<sup>1\*</sup> 

## Executive summary

The increasing incorporation of technology into the health field is leading to greater precision in healthcare; however, advancements in cybersecurity measures are still required. According to a 2016 report by IBM and the Ponemon Institute, the frequency of data breaches in the healthcare industry has been rising since 2010 [1], and it is now among the sectors most targeted by cyberattacks globally [2]. Due to its immutability, the information accessed through health data breaches is of particular interest to criminals [3]. Blood type, past surgeries and diagnoses, and other personal health information are contained in an individual's medical file. As these records include private data such as name, date of birth, insurance and health provider information, as well as health and genetic information, it is not possible to restore privacy or to reverse psychosocial harm when private data are compromised.

These sorts of attacks are not only a threat to patients' identity and finances, but they can also impede hospital operations and place the health and well-being of patients at risk. The United Kingdom's National Health System hospitals, which suffered from the WannaCry ransomware attacks in May 2017, were forced to delay treatment plans and even to reroute incoming ambulances because they lost access to hospital information systems [4]. Among these operational delays and the financial consequences of data breaches and ransomware

attacks, cyberattacks have long-term detrimental effects on the reputation and revenue of hospitals and health facilities.

In response to these global attacks, the *M8 Alliance* undertook a project that began with a scoping review on cyberattacks against hospitals [5]. The review was a basis for several teleconferences conducted by a multidisciplinary team of experts. A workshop ensued in April 2018 at the bi-annual *Geneva Health Forum* (GHF). The purpose of these meetings was to exchange perceived threats, to promote interdisciplinary discussion, and to propose practical recommendations for hospitals across the globe. The onsite meeting at the GHF was organized as a *World Health Summit Expert Meeting* on the cybersecurity of hospitals [6].

Here, we describe the most prominent discussions and recommendations from this working group for other security officers, hospital decision makers, vendors, manufacturers, industry representatives, and academics in the field. We begin with some case examples that serve to illustrate what these attacks look like and how health organizations have responded in the past. We then discuss the need to address cybersecurity through the product lifecycle in a preventative and proactive way as well as an approach to cybersecurity that values quality IT at the foundation with a stable application base and strong IT infrastructure. A risk-based approach is recommended, beginning with the identification of at-risk IT assets, followed by management of tradeoffs between risks and benefits, as well as different types of risks. The training of end-users is emphasized, alongside strategies such as vulnerability management and patch management, the

\* Correspondence: [antoine.flahault@unige.ch](mailto:antoine.flahault@unige.ch)

<sup>1</sup>Institute of Global Health, Faculty of Medicine, University of Geneva, Campus Biotech, Chemin des Mines 9, 1202 Geneva, Switzerland  
Full list of author information is available at the end of the article



© The Author(s). 2020 **Open Access** This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>. The Creative Commons Public Domain Dedication waiver (<http://creativecommons.org/publicdomain/zero/1.0/>) applies to the data made available in this article, unless otherwise stated in a credit line to the data.

controlled and restrictive granting of administrative privileges, and the development of incident response and business continuity plans. Information sharing between stakeholders is also recommended in order to build resilience. We conclude with a discussion on privacy-conscious data sharing and the unique challenges medical devices pose to security.

## Introduction

*Personally identifiable information* (PII) and *protected health information* (PHI) are handled by almost every department in a hospital, in one or more health information system. All healthcare providers (e.g., physicians, physician assistants, nurses, pharmacists, technicians, dietitians, physical therapists) use electronic health records (EHR), e-Prescribing software, remote patient monitoring, and/or laboratory information systems; the billing office works with insurance and financial information through medical billing software; scheduling and administration departments work with clinical data on scheduling software, and the list continues. While PII in organizations within most other fields (e.g., academic institutions or businesses) are typically contained within limited departments where cybersecurity measures can be centralized, in a hospital setting, the data are highly sensitive and valuable, yet almost all departments handle it at least in some manner. Cybersecurity measures aim to protect PII and PHI by securing devices, electronic systems, networks, and data from attacks.

In other fields, such as the financial sector the issue of cybersecurity has been confronted for decades, hence they have established policies and dedicated resources to invest in security, whereas the health field struggles to give sufficient attention and resources to the problem, as it is relatively new to this field. As healthcare is extremely cost constrained, very limited resources are allocated to IT security. Despite these constraints, cybersecurity in hospitals must take into account the thousands of interconnected medical devices and the often-inconsistent business processes. Connected medical devices introduce numerous vulnerabilities in a hospital's cybersecurity; nevertheless, these devices are used throughout the hospital and can even be used off-site. The business process in hospitals can vary significantly from patient to patient, and is difficult to computationally model, this often requires openness (for data interoperability and access to health records in case of emergency), and hence, insecure codes.

Cybersecurity in the health field is unique due to the type of information at risk and the consequences for patient safety. When a credit card number is stolen, the bank cancels the card, issues a new one, and reimburses the client. However, when a patient's PHI is stolen, the patient cannot change, for example, their birthdate,

blood type, and health and genetic information. Once stolen, health information is widely applicable and valuable for a range of crimes, from identity theft to medical fraud. An individual's health information is valued significantly more on the dark web than their social security number or credit card number; it can sell for 10 to 20 times more than this type of data [7, 8].

The regulatory framework around PHI has been evolving over the past two decades. In the United States (US), the Health Insurance Portability & Accountability Act (HIPAA) was passed in 1996; it enforced the protection of health information usage, disclosure, storage, and transmission [9]. This was followed by the Health Information Technology for Economic and Clinical Health (HITECH) Act in 2009, which increased penalties for HIPAA violations, strengthened breach notification, and encouraged the meaningful use of electronic health records [10]. In 2016, the General Data Protection Regulation (GDPR) was adopted by the European Union (EU) to replace existing regulations, and it entered into force in May 2018. GDPR implements provisions and requirements pertaining to the PII of all EU citizens, including provisions for breach notification and penalty implementation [11]. Although the increasingly strict regulations pose technological and organizational challenges for health institutions, they are for the protection of data and the cybersecurity of hospitals, as well as the sake of patient safety.

Cyberattacks risk delay and disruption of sensitive hospital operations and place patients' lives at risk. When the British National Health Service hospitals were attacked in the global WannaCry attack of May 2017 or in the Hollywood Presbyterian Medical Center attack of February 2016, surgeries had to be delayed and patients diverted to nearby hospitals [4]. Cyberattacks can threaten a wide variety of services within a hospital, from surgeries to drug delivery, by targeting advanced equipment such as blood-product refrigerators, imaging equipment, automated drug dispensers and electronic health records, as well as by targeting supporting critical systems such as heating, ventilation, and air conditioning (HVAC). When EHR integrity is compromised, or they are suddenly encrypted in an attack, such as ransomware, providers lose access to critical information (e.g., patient allergies, current medications, and comorbidities). Hospitals are especially at risk in extreme or conflict situations, where stealth malware can stay hidden in the system until conveniently activated, thus leading to severe consequences when healthcare is most urgent (e.g., following a natural or human-instigated disaster). Cyberattacks can also compromise the trust in a doctor-patient relationship, e.g., if data are breached [12].

Moreover, when PHI is stolen, or patients' lives are put at risk in a cyberattack, it is often nearly impossible

to pinpoint the guilty party. Digital forensics is a challenging task in a hospital setting. Data are already used by many services and, when medical devices are involved, few services are equipped to collect necessary traces, run intrusion detection, or forensic analyses. It is difficult to track down the attacker(s), even when a ransom is paid, especially when anonymous cryptocurrencies such as Bitcoin, Dash, Verge, Monero, or ZCash are used. The question of liability is also complex, as there are uncertainties in liability attribution (e.g. in software liability), hence problematic for those who run operations. Assigning responsibility can lead to an oppositional relationship between hospitals and manufacturers. Instead of working together to ensure the highest security practices, they can become competitors by trying to avoid responsibility. However, without assigning responsibility and liability, it is difficult to maintain accountability and effectively deter future attacks.

In 2016, IBM X-Force reported that the healthcare industry faced more cyberattacks than other industries, even surpassing the financial sector [13]. That same year, the Ponemon Institute announced that the frequency of data breaches and their annual economic impact had been rising since 2010 [1]. A 2017 report also averaged the global cost per stolen record to be the highest in the healthcare sector [14]. The case examples in the following section (II) provide concrete details of recent attacks on healthcare organizations.

### Case examples

The following cases of cybersecurity breaches exemplify the variety of attacks the healthcare field has faced in different parts of the world, consequences of these attacks, and steps organizations took in response.

#### Lukaskrankenhaus Neuss (Germany)

Lukaskrankenhaus Neuss is a public hospital founded in 1911 in Neuss, Germany with 537 beds and 1400 employees. In February 2016, employees encountered various error messages from a ransomware attack initiated through a social-engineering tactic. In response, the hospital took servers and computer systems offline to assess and cleanse infected systems. In the meantime, staff resorted to using pen, paper, and fax machines to continue their work but needed to postpone high-risk procedures [15].

While the hospital did not receive a direct demand for money, they were given an email address to contact for further instructions. No attempt was made to contact the attackers as recommended by local authorities [15]. The hospital reported that its backup system was kept up-to-date and only a few hours of data were lost, but a backlog of handwritten records from when the computer systems were offline need to be integrated with the

remainder of the EHR eventually [15]. The hospital's spokesperson predicted it would take a few months before their workflow was back to the status quo [16]. There was no evidence that patient data were breached.

#### South-eastern Norway regional health authority (Norway)

The South-Eastern Norway Regional Health Authority (South-East RHF) is a state-run region-specific organization of specialist hospitals and healthcare services created in 2002 alongside three other regional authorities. In January 2018, South-East RHF announced that the PHI and records of nearly 2.9 million people (more than half of the population of Norway) had been compromised [17]. It is suspected that a sophisticated criminal group from a foreign spy or state agency led the attack targeting both patient health data and the health service's interaction with Norway's armed forces [18]. The vulnerability is thought to have come from the legacy system, Windows XP [18]. While the organization had begun security measures to reduce the risks brought on by Windows XP along with a plan to phase it out, the attack took place before they could implement the security measures [19].

While this attack did not seem to pose risks to patient safety or delays in hospital operations, the event raised concerns about future attacks on health data for the purpose of political gain and served as a wake-up call for GDPR. Under GDPR, the organization would have had to notify those affected within 72 h, which it did not do [20].

#### Hancock regional hospital (United States)

The Hancock Regional Hospital is a small (71 beds) non-profit hospital in Greenfield, Indiana founded in 1951. On January 11, 2018, Hancock Regional faced a ransomware attack by the malware SamSam [21]. The attack targeted a server in their emergency IT backup-system and spread through the electronic connection between the backup site, located miles from the main campus, and the server farm at the hospital [22]. It was later discovered that the hackers had permanently corrupted components of the backup files from many systems, except the electronic medical record backup files. Investigators found that the attack was conducted using Microsoft's Remote Desktop Protocol as an entry point into the server and that the hackers had compromised a hardware vendor's administrative account to initiate the attack [23].

Following the attack, the hospital's IT team shut down all network and desktop systems. Nevertheless, hospital operations continued within the confines of their downtime procedures. Patients were not diverted, and the hospital did not shut down. The hackers demanded four Bitcoins (55,000 USD) for the ransom, and the hospital

paid. IT staff then spent the next three-and-a-half days decrypting files and trying to get the system to run normally [22]. They found no evidence that patient data had been compromised. The CEO, Steve Long, stated that the attack was found to be a premeditated targeted attack on the healthcare facility, by a sophisticated criminal group, and published an article explaining their decision to pay the ransom [22].

## Recommended approach to Cybersecurity in healthcare

### Quality IT at the foundation

For a health facility to have a strong information security posture, it requires quality IT: at least a stable application base and IT infrastructure. This is especially difficult to achieve in healthcare settings due to a lack in human resources, restraints in the budget, a history of underinvestment, and the complex application space; nevertheless, it is crucial.

Although there are no established models or tools for a health facility to use in evaluating the quality of its IT, there are a few markers that can shed some light. For example, a health facility with a stable application base does not have helpdesk call-logs that are overwhelmed with break/fix requests and its IT staff is not preoccupied primarily with repairing malfunctioning or broken applications.

Equally important to IT quality is the state of the IT infrastructure. The infrastructure can include any related resources and services used to deliver and support IT services (e.g., hardware platforms, software applications, operating systems, and networking and telecommunication tools) [24]. Information security requires that the IT infrastructure has configuration management, change management, and logging and monitoring in place. At its core, configuration management aims to maintain an updated inventory of IT assets and the relationship between different components. According to the Information Technology Infrastructure Library (ITIL), this involves identifying and reporting each assets' version and its associated components [25]. Although it is a daunting task, well-maintained configuration management boosts vulnerability management and patch management. The SANS Institute states that "configuration management underlies the management of all other management functions: security, performance, accounting and fault" [26]. In line with configuration management is change management that ITIL describes as a systematic approach to handling all changes in a standardized method [27]. Change management not only avoids unnecessary service downtime, but it is also useful during a cyberattack. An incident response plan can be a version of change management. Similarly, strict audit logs and monitoring of logging records are IT

functions which are critical to quickly recognizing attacks and obtaining details on an attack [28].

### Preventative and proactive stance

In the past, hospitals experienced difficulties with devices that refuse operating system patches or that became functionally compromised when, for example, Microsoft Windows was updated multiple times [29]. Consequently, hospitals had to delay or refrain from closing various security gaps in the operating system. There has been a recent push to promote cybersecurity as a value proposition among medical device and equipment manufacturers, shifting the approach to cybersecurity by motivating them to value it and sell it as an asset [30, 31]. Cybersecurity is not simply plugged in as an afterthought but has become one of the prerequisites of the design [32]. This has also been reinforced by the US Food and Drug Administration (FDA), that expects manufacturers to implement on-going lifecycle processes and to monitor continued safety post-market [33].

In 2017, the FDA began mandating that medical device manufacturers show that their devices are able to have updates and security patches applied throughout their lifespan. Additionally, they must show that they have addressed any undesirable issues that would affect the patients if the device was to be compromised. As part of this same regulation, the FDA requires that a "bill of materials" be shared with buyers of a medical device. The bill of materials provides transparency to the device buyer as to the source of each component (hardware and software) contained in the medical device. These new rules will apply to manufacturers, who must submit a 510(k)-pre-market submission package to the FDA [34].

These measures puts the onus on manufacturers, however, the call to approach cybersecurity with a more engaged and proactive stance should not be limited to manufacturers but should challenge health facilities as well. Hospitals ought to invest in prevention by designating resources and budgeting early, rather than depending on reactive approaches following attacks; this might be difficult in light of historic underinvestment in human resources and funding in hospital information security [35–37].

### Risk-based approach

Cybersecurity requires the highest level of security measures. However, as infallible cybersecurity is nonexistent, a risk-based approach through enterprise risk management is necessary. Even with quality IT infrastructure and practices, along with a proactive stance and information security measures, the risk of an attack will always persist. Therefore, the framework for managing cybersecurity recommended by the US National Institute

of Standards and Technology (NIST) and the recommendations of the European Union Agency for Network and Information Security (ENISA) are rooted in a risk-based approach.

Risk assessment depends on the identification of at risk IT assets, stressed as the first step by the NIST Cybersecurity Framework (CSF) for critical infrastructure, and the identification of potential threats through methods such as vulnerability management [38]. An asset's value to the organization and its exposure to risk should determine its priority in the protection processes. Quality IT is important here, as configuration management will be integral to this identification step. Risk analysis of these findings should consider tradeoffs between risks and benefits, as well as between different risks [39]. It should also evaluate the potential consequences for patient safety and maintenance of operations [38]. This requires the assessment of an incident's impact on data and privacy protection (confidentiality), availability of information, and integrity of information. The latter is especially important as the integrity of health data can have severe consequences for the patient's safety.

Health facilities can manage risks through various methods, from mitigating, avoiding, or transferring to accepting the risks [40]. The NIST CSF follows this identification of risks step with Protect, Detect Incidents, Respond, and Recover [40].

### Training and awareness

As humans are the weakest link in cybersecurity, health facilities' approaches to cybersecurity should take into account the need for raising awareness among all users [41, 42]. This, of course, does not guarantee security, but it is a step in the right direction. End users, from clinicians to billing and scheduling staff, as well as patients and caregivers who connect their personal devices with the hospital network, can unintentionally—or intentionally—threaten the cybersecurity of the health facility. Human error also poses risks as in the incident at Geneva University Hospital (HUG) in October 2019 [43]. In an effort to mitigate risk, the ENISA's Security and Resilience in eHealth publication among others recommend providing cybersecurity training [38, 44].

To offer relevant and effective trainings, health facilities should frequently assess and identify gaps in knowledge [28]. It is important for end users to realize the risks they cause through inadvertent actions. For example, they should be aware that storing data on their mobile devices can pose privacy and data-integrity risks [45], whereas the use of connected devices or removable storage devices can increase the risk of malware execution. Similarly, end users should have a concrete understanding of the threats (e.g., What is a ransomware attack, what are the effects, and how is the attack

initiated?). End users are potential targets for social engineering methods, hence training programs should explore how to handle unrecognized e-mails and avoid phishing tactics, while encouraging basic digital-hygiene practices (e.g., strong passwords, not clicking on unknown links).

Cyberattacks, such as the May 2017 worldwide WannaCry attack, serve as a wakeup call, but it is in the best interest of organizations to keep up vigilance even when threats are not in the headlines [46]. One way to do this is by enacting mock exercises and simulating cybersecurity drills. Health facilities can approach this in different ways: from having the information security team send users simulated phishing e-mails, to setting up drills for IT officers such as locating and neutralizing unauthorized devices on the network [47, 48]. These exercises can even evaluate the effectiveness of the organization's current training programs [49].

### Recommended Cybersecurity measures

#### Vulnerability management, patch management

Exposure and vulnerability management involves the identification, evaluation, and mitigation of IT vulnerabilities. It relies heavily on threat-monitoring processes but also entails all the identification steps: risk assessment, remediation or mitigation steps, and reevaluation [50]. In handling and investigating attacks and post-infection remediation, Endpoint Detection and Response (EDR) solutions should be used. In most cases, this risk assessment is highly complex. Among the steps towards remediation or mitigation, there is also patch management that can become complicated by a health facility's need to operate 24/7/365. Risk analysis is at the core of patch processes: weighing the sensitivity of data on the server and an enterprise's critical functions or assets vulnerable to an attack [26].

Organizations should actively search out vulnerabilities in their systems and maintain ongoing vulnerability management with penetration testing [28]. Early detection can help reduce exposure to a security risk. The identification of vulnerabilities should also be followed with configuration hardening or patch processes without an overemphasis on zero-day vulnerabilities. Gartner analysts recently found that 99% of exploits are based on vulnerabilities that were known to security and IT professionals for over six months [51]. In prioritizing the remediation of different vulnerabilities, organizations should consider such findings.

As for the importance of maintaining quality IT infrastructure, configuration management has the benefit of increasing ease in assessing vulnerabilities because of a broader understanding of the facilities' IT infrastructure and in running risk assessments, as well as analyses required for patch processes. Patching should be applied

to all systems in the configuration (this includes the operating system and third-party applications) and changes should be noted by change management [50].

#### **Administrative privileges and administrative multifactorial authentication**

The risks associated with granting administrative privileges to users in health facilities are immense. According to CyberSheath's APT Privileged Account Exploitation report, the vast majority of large-scale attacks that caused significant damage and expenses were initiated through the compromise of a privileged account such as that of a third-party provider [52]. This was the case for the attack that took place at Hancock Regional Hospital in January 2018, when the login credentials to a vendor's account were compromised [23].

Health entities should grant administrative privileges in a controlled and restrictive manner, in order to minimize the number of such accounts to an enterprise-dependent manageable sum [28, 53]. These accounts should be inventoried, monitored for abnormal use, and evaluated for log entries. To avoid malicious insider threats, the health entity should also enforce local password policy and revisit their criteria for privileged access in addition to the vetting of users. A study revealed that disgruntled employees account for 70% of computer-related criminal activity [54]. Organizations should address the risk of such threats by closely monitoring the lifecycle of user accounts and revoking client and user certificates when no longer in use. Additionally, end users requiring administrative privileges should have two accounts: one that has privileges limited to local machines and another with no administrative privileges to be used for routine tasks such as browsing the internet or checking emails [28, 47, 55]. When necessary, direct web-access on critical devices should be denied or the use of encapsulated browsers should be enforced.

It is important to provide users who are granted administrative or privileged accounts with additional training on the risks brought on by their privileges, as it is important to equip them with the proper security measures. Among the most important measures is the use of multifactorial authentication for all administrative and privileged users—preferably for all users. The Center for Internet Security's (CIS's) Critical Security Controls for Effective Cyber Defense lists the use of smart cards, One Time Passwords, or biometrics, among the techniques to implement this vital step [28].

#### **Incident response plan**

As cyberattacks have become increasingly frequent and consequential in recent years, health facilities should prepare an incident response and business continuity plan. These plans should be regularly tested, exercised,

and stored offline [55]. Plans should involve an agreed upon process with the appropriate stakeholders identified. It is important to have a designated team and a cybersecurity leader, or simply a designated person in cases where the organization does not have a CISO [56, 57]. The roles and responsibilities should be clearly divided within the team. The organizations should also have an agreement on what constitutes as a reportable incident and when to escalate [58, 59]. Ideally, plans should embed prevention training as well.

Incident response plans should also endorse post-incident steps. This can involve enforcing organization-wide password resets after an attack, factory resetting, and replacing compromised hardware and software as necessary. However, there needs to be an internal plan for regrouping and implementing changes [40]. The IT and cybersecurity system and its management should then be adapted to the new needs and requirements that were revealed by the incident (i.e., patching and beyond).

A notification system should be established between the health facility and the manufacturers [60]. A process can be built for those in the enterprise (e.g., clinicians, business administrators, and IT staff) to report incidents directly to the manufacturers. In fact, this type of sharing is also being mandated in the most recent FDA 510(k) pre-market submission guidelines [34].

#### **Information sharing**

The exchange of potential threats, indicators of compromise, best practices, vulnerabilities, lessons learned, and of mitigation strategies between stakeholders across public and private sectors is an essential step in building the cybersecurity of healthcare systems [61, 62]. Information sharing facilitates situational awareness and a solid understanding of threats and threat actors, their motivations, campaigns, tactics, and techniques. Consequently, it better equips decision makers to understand organizational exposure and to employ enterprise risk management policies. Information sharing should include all stakeholders: providers, manufacturers, suppliers, payers, and electronic record providers, as well as government(s) where applicable.

There are organizations that exist specifically to facilitate collaboration between institutions, for example, the National Health Information Sharing and Analysis Center (NH-ISAC), a global, member-driven non-profit providing a forum for trusted sharing amongst healthcare organizations. The EU adopted the Network and Information System (NIS) Directive in 2016—the first EU law specifically focused on cybersecurity—to be transposed by member states by 2018. The directive requires member states, most notably, to adopt national cybersecurity strategies, to designate national competent authorities, and to develop one or more computer security incident

response teams (CSIRTs). It also establishes security and incident notification requirements for “operators of essential services,” such as healthcare organizations, even requiring incidents of certain magnitudes to be reported to national authorities. To promote swift and effective operational cooperation regarding threats and incidents, the directive emphasizes coordination among member states, setting up a CSIRT network (also to include CERT-EU), and a strategic NIS “cooperation group” to support and facilitate cooperation and information exchange among member states [63].

#### Privacy-conscious data sharing and processing

The sharing of medical and genomic data, across departments and institutions, is necessary for both effective patient care and for meaningful research that advances the state-of-the-art in personalized medicine. In fact, the recent increasing trend towards P4 (Predictive, Preventive, Personalized and Participatory) medicine is called to revolutionize healthcare by providing better diagnoses and targeted preventive and therapeutic measures. However, clinical and research data on large numbers of individuals must be efficiently shared among all stakeholders. In this context, cybersecurity is as relevant as it is in regular hospital operations, but the privacy risks that stem from disclosing medical and genomic data play a prominent role and have become a barrier in the advancements of P4 medicine [64]. This is further reflected in the evolution of stricter regulations (e.g. HIPAA in US and GDPR in the EU [9, 11]).

The challenges of privacy-conscious data sharing and processing can be addressed through the use of advanced cryptographic mechanisms (such as homomorphic encryption [65, 66], trusted hardware [67], secure multiparty computation [68, 69]), and strong trust distribution techniques (such as distributed ledger technologies [70]). The use of these technologies provides security guarantees beyond those implemented by traditional approaches against cyberattacks [71], with the following four direct advantages: (a) achieving a more fine-grained control on access permissions, hence reducing or avoiding the need of privileged accounts to third parties, (b) implementing minimization principles on the released data for the agreed usage, in line with the latest and stricter data protection regulations and minimizing the risk of breaches and intentional or unintentional data misuse, (c) keeping individual and identifiable data within the confines of the security perimeter of the medical institution that governs them, and (d) enabling distributed logging and access control management, hence avoiding single points of failure and greatly reducing the effect of a breach and the risk of a successful attack, while allowing for more advanced implementations of auditability, accountability and incident recovery.

Consequently, privacy-conscious data sharing and processing approaches are aligned with the aforementioned risk-based cybersecurity strategies, provide guarantees that go beyond the latter, yet enables operations across medical institutions that would otherwise be impossible.

#### Recommendations for connected medical devices

The FDA defines medical devices as

An instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including a component part, or accessory [ ... ] intended for use in the diagnosis [ ... ] cure, mitigation, treatment, or prevention of disease [ ... ] [72].

This definition encompasses equipment such as beds, in-house treadmills, intravenous pumps, and monitors, as well as implantable and connected devices such as pacemakers and insulin pumps. Additionally, wearable devices (such as Fitbits) that monitor, and record health and lifestyle data can now be connected to clinicians’ devices. These devices can propagate flaws or incidents in cybersecurity and act as weak elements in the security chain by which malware can spread. The diversity in devices can also make it difficult to enact strict security policy, but the cybersecurity of these devices is critical. Medical devices are typically in direct contact with patients and can increase risks to hospital operations and patient safety.

Advancements such as the Internet of Things enables remote medical care and precision in healthcare delivery. However, clinical care utility and safety need to be balanced with security and privacy. Devices are highly interconnected in the hospital network and large sums of collect clinical data that need to be securely transferred, but these devices also have inherent limitations that expose them to vulnerabilities. They often do not have the proper security measures because they do not have the battery power or the built-in resources to efficiently employ security measures such as encryption and forensic processes, threat modeling activities, and malware detection [58, 60]. Devices designed to function in isolation often end up integrated into the network, whereas physical security of the wearable devices is nearly impossible as they do not typically have long life spans and their operating system or relevant platforms become outdated relatively quickly [56, 58].

Decision makers should evaluate the expected lifetime of devices (e.g., manufacturer/vendor-support or operating system-support) before purchase. In conjunction, equipment maintenance is critical to medical-device security. Hospitals and manufacturers, with support from certifying authorities, should develop a patching policy

that minimizes equipment downtime and enables timely updates through a collaboration with the external manufacturing community and internal stakeholders. Collaboration with manufacturers can allow facilities to better monitor new alerts in order to keep up with critical or urgent patches and updates. Facilities should also develop and budget for life-cycle management in order to retire devices that cannot be replaced right away.

It is also essential for IT to maintain a regularly updated inventory of all devices on the network (authorized and unauthorized). Hospital networks often have numerous personal devices that are integrated. Patients and physicians often connect external mobiles and wearables [73], thus increasing exposure and complicating bring your own device (BYOD) policies. The health organization should enact reasonable measures and policies to block connectivity of unapproved personal devices (mobiles, tablets ...) [55], even using mobile device management or software distribution systems. Besides this, health facilities should enforce local data encryption, when possible, in a preventative stance.

## Conclusion

A year and a half after this workshop, attacks on hospitals continue to take headlines. At the beginning of October 2019, three hospitals in Alabama (US) faced a ransomware attack that forced them to diverge new patients to nearby hospitals [74]. Around the same time, another ransomware infection on seven Australian hospitals was reported [74]. There continues to be an outbreak of these attacks, further stressing the urgency of the matter at hand.

Building the cyber resilience of a hospital is vital and it is a shared responsibility. Users (i.e., clinicians and administration staff) should undergo training and should practice digital hygiene, decision makers should enforce the proper policies and consider cybersecurity in purchasing decisions, and manufacturers should equip their products with the appropriate cybersecurity measures. The information security teams of hospitals should also enact and upkeep the proper tools to safeguard the hospital and patients.

Information security teams should equip users to counter social engineering methods by, for example, filtering e-mail content, auto-checking suspicious URLs in e-mails for linked malicious code, whitelisting trustworthy websites and applications, as well as blocking Flash, advertisements and untrusted JAVA code on the Internet, as necessary [55]. Other tactics for reducing exposure should be used, such as intentionally changing default passwords and regularly updating security configurations on laptops, servers, workstations, firewalls, etc. [47]. Antivirus software is also important, along with penetration tests, control of physical access, and the

maintenance of regularly updated backups (which should be stored offline). The organization's website and the industrial control systems, including HVAC, cameras, fire alarm panels, should be secure and locked down from attacks. EDR Software can also help detect malware breaches and react properly to recorded infections. Finally, there should be appropriate tools in place for protecting data shared across different departments or medical institutions in a privacy-conscious way, therefore reducing the risk of intentional or unintentional breaches through trust distribution [64].

Cybersecurity is also a matter of arbitrating tradeoffs [39]. As mentioned, utility and safety need to be balanced with security, privacy, and compliance with data protection regulations, especially in the highly distributed and collaborative environments required for precision medicine. Yet, convenience cannot be left out of the equation. Without considering the latter point, these recommendations will remain theoretical and inapplicable in actual practice. A physician who wants to store or access clinical data on their mobile phone is not doing so to increase exposure to cyber threats but for the sake of convenience and efficiency in the delivery of care, and the quality of care. Similarly, an information security officer who takes a system offline to apply updates or patches does not intend to inconvenience health providers but to decrease the risks against unexpected downtime from large-scale attacks. There should not be two sides working independently of each other towards their own goals, but a collective, multidisciplinary team working towards protecting and improving patient care and data.

## Additional resources

Cybersecurity of healthcare organizations is critical to patient safety, as well as to hospital operations. Many resources have become available in recent years. Here are some:

- ISO/IEC 27002 (2013)
- CIS Critical Security Controls for Effective Cyber Defense (2016)
- ENISA Security and Resilience in eHealth: Security Challenges and Risks (2015)
- Medical Device Innovation Safety and Security Consortium ([MDISS.org](http://MDISS.org))
- DTS Cybersecurity Standard for Connected Diabetes Devices ([www.dtsec.org](http://www.dtsec.org))

## Abbreviations

PII: Personally identifiable information; PHI: Protected health information; HIPAA: Health Insurance Portability & Accountability Act; US: United States; EU: European Union; GDPR: General Data Protection Regulation; EHR: Electronic health records; HVAC: Heating, ventilation, and air conditioning; CERT: Computer Emergency Response Team; CISO: Chief Information Security Officer; CIO: Chief Information Officers; ITIL: Information



Technology Infrastructure Library; IT: Information technology; FDA: Food and Drug Administration; NIS: Network & Information Systems; NIST: National Institute of Standards and Technology; ENISA: European Union Agency for Network and Information Security; CSF: Cybersecurity Framework; HUG: Geneva University Hospital; EDR: Endpoint Detection and Response; NH-ISAC: National Health Information Sharing and Analysis Center; P4: Predictive, Preventive, Personalized and Participatory; BYOB: Bring your own device

#### Acknowledgments

This product is the result of the collaboration of experts who represent various institutions and backgrounds. We would like to extend a special thank you to all those who were a part of the 7th edition of the Geneva Health Forum M8 Alliance Expert Meeting on Cybersecurity in Healthcare working group and those listed here for their contribution and support: Chang-Chuan Chan, Eric de Roodenbeke, Feipei Lai, Mahmood Tara, Jean-Pierre Hubaux, Ken Hoyme, Malika Ait-Mohamed Parent, and Scott Burleson.

#### Authors' contributions

A.F. conceived the project and directed it alongside B.E., B.E. and S.A. organized the teleconferences and workshop that led to this white paper. Members of the 7th edition of the Geneva Health Forum M8 Alliance Expert Meeting Group on Cybersecurity in Healthcare were integral to the general conception of the presented ideas—particularly J.T., D.L., M.F., D.A., W.B., F.C., C.O., and J.V. and they were additionally involved in on-going edits of the manuscript. D.L. conceived the ideas presented in Section 1 as well as Section 4.1 and 4.2 and J.T. conceived and drafted crucial sections such as Section 4.5. S.A. drafted rest of the manuscript with additional help from the other authors and all authors commented on initial and final edits. The author(s) read and approved the final manuscript.

#### Funding

The authors received no financial support for the research, authorship, and/or publication of this article.

#### Availability of data and materials

Data sharing is not applicable to this article as no datasets were generated or analyzed during the current study.

#### Ethics approval and consent to participate

Not applicable.

#### Consent for publication

Not applicable.

#### Competing interests

The authors declare that they have no competing interests.

#### Author details

<sup>1</sup>Institute of Global Health, Faculty of Medicine, University of Geneva, Campus Biotech, Chemin des Mines 9, 1202 Geneva, Switzerland. <sup>2</sup>School of Computer and Communication Sciences, EPFL (Ecole polytechnique fédérale de Lausanne), EPFL IC IINFCOM LDS, BC 266 (Bâtiment BC), Station 14, CH-1015 Lausanne, Switzerland. <sup>3</sup>Johns Hopkins University/Johns Hopkins Medicine, 5801 Smith Avenue, Davis Building, Suite 3110B, Baltimore, MD 21209, USA. <sup>4</sup>International Risk Governance Center (IRGC), EPFL (Ecole polytechnique fédérale de Lausanne), EPFL ENT-R IRGC, BAC 001.1 (Château de Bassenges), Station 5, CH-1015 Lausanne, Switzerland. <sup>5</sup>Hôpitaux Universitaires de Genève, Rue Gabrielle-Perret-Gentil 4, CH-1211 Genève 14, Switzerland. <sup>6</sup>National Health Information Sharing and Analysis Center (NH-ISAC), 226 North Nova Road, Suite 391, Ormond Beach, Florida 32174, USA. <sup>7</sup>Electrical and Computer Engineering, University of Massachusetts Amherst, 309B Knowles Engineering Bldg, University of Massachusetts, 151 Holdsworth Way, Amherst, MA 01003-9284, USA. <sup>8</sup>Department of Information Technology, Charité-Universitätsmedizin Berlin, Charitéplatz 1, 10117 Berlin, Germany. <sup>9</sup>Aspen University, 1660 S. Albion St., Suite 525, Denver, Colorado 80222, USA.

Received: 27 June 2018 Accepted: 24 June 2020

Published online: 03 July 2020

#### References

1. Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data. Traverse City: Ponemon Institute LLC; 2016. p. 1–50. <https://www.ponemon.org/local/upload/file/Sixth%20Annual%20Patient%20Privacy%20%26%20Data%20Security%20Report%20FINAL%206.pdf>.
2. Martin G, Martin P, Hankin C, Darzi A, Kinross J. Cybersecurity and healthcare: how safe are we? *BMJ*. 2017. <https://doi.org/10.1136/BMJJ3179>.
3. Alvarez M. Security trends in the healthcare industry. Somers: IBM; 2017. p. 2–18.
4. Millard WB. Where bits and bytes meet flesh and blood. *Ann Emerg Med*. 2017. <https://doi.org/10.1016/j.annemergmed.2017.07.008>.
5. Argaw ST, Bempong N, Eshaya-Chauvin B, Flahault A. The state of research on cyberattacks against hospitals and available best practice recommendations: a scoping review. *BMC Med Inform Decis Mak*. 2019;5:1–11.
6. Ganten D, Silva JG, Regateiro F, et al. Science Has to Take Responsibility . 10 Years World Health Summit — The Road to Better Health for All; 2018. p. 6. <https://doi.org/10.3389/fpubh.2018.00314>.
7. Humer C, Finkle J. Your medical record is worth more to hackers than your credit card. *Reuters*. 2014. <https://www.reuters.com/article/us-cybersecurity-hospitals-idUSKCN0HJ2120140924>. Accessed 27 Apr 2018.
8. Luna R, Rhine E, Myhra M, Sullivan R, Kruse CS. Cyber threats to health information systems: a systematic review. *Technol Health Care*. 2016;24:1–9.
9. Health Insurance Portability and Accountability Act of 1996. Office of the Assistant Secretary for Planning and Evaluation. <https://aspe.hhs.gov/report/health-insurance-portability-and-accountability-act-1996>. Accessed 29 May 2018.
10. The Impact of HIPAA and HITECH. Mountain View: Symantec corporation; 2010. p. 1–7.
11. Regulation 2016/679 of the European parliament and the Council of the European Union. Brussels: Off J Eur Communities; 2016. 1–88.
12. EPFL IRGC. Governance of trust in precision medicine. Lausanne: EPFL International Risk Governance Center; 2018. p. 1–24.
13. Bradley N, Alvarez M, McMillen D, Craig S. Reviewing a year of serious data breaches, major attacks and new vulnerabilities: Analysis of cyber attack and incident data from IBM's worldwide security services operations. Somers: IBM X-Force® Res 2016 Cyber Secur Intell Index. 2016. 1–19. 2017.
14. Cost of Data Breach Study, Global Overview. Traverse City: Ponemon Institute LLC; 2017. p. 1–34. <https://www.ponemon.org/library/2017-cost-of-data-breach-study-united-states>.
15. Steffen S. Hackers hold German hospital data hostage. *DW*. 2016. <http://www.dw.com/en/hackers-hold-german-hospital-data-hostage/a-19076030>. Accessed 20 Feb 2018.
16. Zorz Z. Crypto ransomware hits German hospitals. *Help Net Security* 2016. <https://www.helpnetsecurity.com/2016/02/26/crypto-ransomware-hits-german-hospitals/>. .
17. Khandelwal S. Nearly half of the Norway population exposed in HealthCare data breach. *The Hacker News* 2018. <https://thehackernews.com/2018/01/healthcare-data-breach.html>. Accessed 21 Feb 2018.
18. Hughes O. Norway healthcare cyber-attack could be biggest of its kind. *Digital Health*. 2018. <https://www.digitalhealth.net/2018/01/norway-healthcare-cyber-attack-could-be-biggest/>. Accessed 21 Feb 2018.
19. Irwin L. Breach at Norway's largest healthcare authority was a disaster waiting to happen. *IT Governance Blog* 2018. <https://www.itgovernance.eu/blog/en/breach-at-norways-largest-healthcare-authority-was-a-disaster-waiting-to-happen/>. Accessed 21 Feb 2018.
20. Warwick A. Norwegian healthcare breach alert failed GDPR requirements. *Computer Weekly* 2018. <http://www.computerweekly.com/news/252433538/Norwegian-healthcare-breach-alert-failed-GDPR-requirements>. Accessed 21 Feb 2018.
21. Secureworks Counter Threat Unit Threat Intelligence. *SamSam Ransomware campaigns*. Secureworks. 2018. <https://www.secureworks.com/research/samsam-ransomware-campaigns>. Accessed 29 May 2018.
22. Long S. The cyber attack - from the POV of the CEO - Hancock regional hospital. *Hancock Health* 2018. <https://www.hancockregionalhospital.org/2018/01/cyber-attack-pov-ceo/>. Accessed 21 Feb 2018.
23. Hughes O. Hancock regional hospital back online after paying hackers \$55,000. *Digital Health* 2018. <https://www.digitalhealth.net/2018/01/hancock-regional-hospital-back-online/>. Accessed 21 Feb 2018.

24. Laudon KC, Jane P. Laudon. IT Infrastructure and Emerging Technologies. In: Management Information Systems: Managing The Digital Firm. 10th edition. Prentice Hall; 2008. [https://paginas.fe.up.pt/~als/mis10e/ch5/chpt5-2\\_bulletext.htm](https://paginas.fe.up.pt/~als/mis10e/ch5/chpt5-2_bulletext.htm). Accessed 16 Apr 2018.
25. A guide to service asset and configuration management. Oxford: UCSIA ITIL; 2014. p. 1–9. [https://www.academia.edu/29873674/ITIL\\_guide\\_to\\_SA\\_and\\_CM\\_management\\_pdf](https://www.academia.edu/29873674/ITIL_guide_to_SA_and_CM_management_pdf).
26. Voldal D. A practical methodology for implementing a patch management process. Swansea: SANS Inst Inf Secur Read Room; 2003. p. 1–14.
27. A guide to change management. Oxford: UCSIA ITIL; 2017. p. 1–4. [https://docuri.com/download/itila-guide-to-change-management-pdf\\_59c1e978f581710b286d4333\\_pdf](https://docuri.com/download/itila-guide-to-change-management-pdf_59c1e978f581710b286d4333_pdf).
28. The CIS Critical security controls for effective cyber defense. 2016. <https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode>.
29. Centricity Down After Applying Windows Updates. Quattris health. 2016. <http://www.quattris.com/messagecenter/centricity-services-update-centricity-applying-windows-updates/>. Accessed 30 May 2018.
30. Tanev G, Apiafi R. A Value Blueprint Approach to Cybersecurity in Networked Medical Devices. *Technol Innov Manag Rev*. 2015;5(6):17–25. <https://doi.org/10.22215/timreview/903>.
31. Alvarenga A, Tanev G. Cybersecurity risk assessment framework that integrates value-sensitive design. *Technol Innov Manag Rev*. 2017;7:32–43. .
32. Moses V, Korah I. Lack of security of networked medical equipment in radiology. *Am J Roentgenol*. 2015;204:343–53.
33. Software as a Medical Device ( SAMD ): Clinical Evaluation Guidance for Industry and Food and Drug Administration Staff. 2017. <https://www.fda.gov/media/100714/download>. Accessed 7 Oct 2019.
34. Medical Device Safety Action Plan. Silver Spring: FDA; 2018. 1-18. 2017 HIMSS Cybersecurity survey. Chicago: HIMSS; 2017. p. 5–37.
35. Khan SI, Hoque ASML. Digital health data: a comprehensive review of privacy and security risks and some recommendations. *Comput Sci J Mold*. 2016;24:273–92.
36. Protecting Your Networks from Ransomware. Washington, DC: The United States Department of Justice; 2016. p. 2–8. <https://www.justice.gov/criminal-ccips/file/872771/download>.
37. Liveri D, Sarri A, Skouloudi C. Security and resilience in eHealth: security challenges and risks. ENISA. 2015. <https://doi.org/10.2824/217830>.
38. EPFL IRGC. Governing cybersecurity risks and benefits of the.
39. Internet of Things. Connected medical & health devices and connected vehicles. Workshop report. Lausanne: EPFL International Risk Governance Center; 2017. p. 6–29.
40. Framework for Improving Critical Infrastructure Cybersecurity Note to Readers on the Update. Gaithersburg: National Institute of Standards; 2018. p. 1–44. <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>.
41. Ondiege B, Clarke M, Mapp G. Exploring a new security framework for remote patient monitoring devices. *Computers*. 2017;6:11.
42. Pycroft L, Boccard SG, Owen SLF, Stein JF, Fitzgerald JJ, Green AL, et al. Brainjacking: implant security issues in invasive Neuromodulation. *Elsevier*; 2016. <https://doi.org/10.1016/j.wneu.2016.05.010>.
43. Wagner S. Les données médicales d'une centaine de patients des HUG accessibles sur internet. <https://www.ictjournal.ch/news/2019-10-04/les-donnees-medicales-dune-centaine-de-patients-des-hug-accessibles-sur-internet>. Accessed 7 Oct 2019.
44. Kruse CS, Frederick B, Jacobson T, Monticone DK. Cybersecurity in healthcare: a systematic review of modern threats and trends. *Technol Heal Care*. 2017;25:1–10.
45. Cybersecurity. The protection of data and systems in networks that connect to the Internet - 10 Best Practices for the Small Healthcare Environment. Washington: Department of Health and Human Service; 2010. p. 5–21.
46. Ehrenfeld JM. WannaCry, Cybersecurity and Health Information Technology: A Time to Act. *J Med Syst*. 2017;41:104.
47. Sittig DF, Singh H. A socio-technical approach to preventing, mitigating, and recovering from Ransomware attacks. *Appl Clin Inform*. 2016;7:624–32.
48. Langer SG. Cyber-security issues in healthcare information technology. *J Digit Imaging*. 2017;30:117–25.
49. Kim L. Cybersecurity awareness: Protecting data and patients. *Nursing* 2018. 2017;47:65–7.
50. Palmaers T. Implementing a vulnerability management process. Swansea: SANS Inst Inf Secur Read Room; 2013. p. 1–21.
51. Rochford O, Young G, Lawson C. Predicts 2017: Threat and vulnerability management. Stamford: Gartner; 2016. 1–6.
52. New Report Connects Privileged Account Exploitation to Advanced Cyber Attacks. CyberArk. 2013. <https://www.cyberark.com/press/new-report-connects-privileged-account-exploitation-advanced-cyber-attacks/>. Accessed 23 Apr 2018.
53. Wright A, Aaron S, Bates DW. The big phish: Cyberattacks against U.S. healthcare systems. *J Gen Intern Med*. 2016;31:1115–8.
54. Harries D, Yellowlees PM. Cyberterrorism: is the U.S. healthcare system safe? *Telemed J E Health*. 2013;19:61–6.
55. Strategies to Mitigate Cyber Security Incidents – Mitigation Details. ASD Australian Signals Directorate. 2017. <https://www.asd.gov.au/infosec/top-mitigations/mitigations-2017-details.htm>. Accessed 30 Jan 2018.
56. Health Care Industry Cybersecurity Task Force Report on Improving Cybersecurity in the Health Care Industry. Washington: Department of Health and Human Service; 2017. 1–87.
57. Le Bris A, El Asri W. State of Cybersecurity & Cyber Threats in healthcare organizations: applied Cybersecurity strategy for managers. *Cergy: ESSEC Bus Sch*; 2017. p. 1–13.
58. SMART Hospitals. ENISA; 2013. <https://doi.org/10.2824/28801>.
59. Cybersecurity and Hospitals. Four Questions Every Hospital Leader Should Ask in Order to Prepare for and Manage Cybersecurity Risks. Chicago: America Hospital Association; 2015. p. 1–15.
60. Williams P, Woodward A. Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem. *Med Devices Evid Res*. 2015. <https://doi.org/10.2147/MDER.S50048>.
61. Healthcare and Public Health Sector-Specific Plan. Washington: Department of Homeland Security; 2015. p. 1–53. <https://www.cisa.gov/sites/default/files/publications/nipp-ssp-healthcare-public-health-2015-508.pdf>.
62. Piggan R. Cybersecurity of medical devices - addressing patient safety and the security of patient health information. London: BS; 2017. p. 3–22.
63. The Directive on security of network and information systems (NIS Directive). European Commission. 2016. <https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive>. Accessed 20 Jun 2018.
64. DPPH18. <https://dpph18.epfl.ch/>. Accessed 30 May 2018.
65. Bost R, Popa R, Tu S, Goldwasser S. Machine Learning Classification over Encrypted Data. *NDSS*; 2015. <https://doi.org/10.14722/ndss.2015.23241>.
66. Dowlin N, Gilad-Bachrach R, Laine K, Lauter K, Naehrig M, Wernsing J. CryptoNets: Applying neural networks to Encrypted data with high throughput and accuracy. *Proc 33rd Int Conf Int Conf Mach Learn*. 2016;48:201–10.
67. Costan V, Devadas S. Intel SGX explained. *IACR Cryptol ePrint Arch*. 2016;2016:86.
68. Corrigan-Gibbs H, Boneh D. Prio: private, robust, and scalable computation of aggregate statistics. Boston: NSDI; 2017. p. 259–82.
69. Froelicher D, Egger P, Sousa JS, Raisaro JL, Huang Z, Mouchet C, et al. UnLynx: a decentralized system for privacy-conscious data sharing. *Proc Priv Enhancing Technol*. 2017. <https://doi.org/10.1515/popets-2017-0047>.
70. Kokoris-Kogias E, Jovanovic P, Gasser L, Gailly N, Syta E. OmniLedger: a secure, scale-out, decentralized ledger via Sharding. *IEEE Symp Secur Priv*. 2018. <https://doi.org/10.1109/SP.2018.000-5>.
71. Raisaro JL, Troncoso-Pastoriza JR, Misbach M, Sousa JS, Pradervand S, Missaglia E, et al. MedCo: Enabling Privacy-Conscious Exploration of Distributed Clinical and Genomic Data. Orlando: 4th Int Work Genome Priv Secur; 2017. p. 1–21.
72. Classify Your Medical Device - Is The Product A Medical Device? 2018. <https://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/Overview/ClassifyYourDevice/ucm051512.htm>. Accessed 25 Apr 2018.
73. Kotz D, Gunter CA, Kumar S, Weiner JP. Privacy and security in Mobile health: a research agenda. *Computer*. 2016;49:22–30.
74. US hospitals turn away patients as ransomware strike. 2019. <https://www.bbc.com/news/technology-49905226>. Accessed 5 Oct 2019.

## Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.