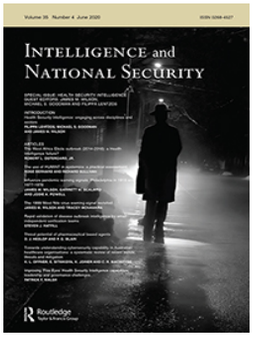

Routledge
Taylor & Francis Group

Intelligence and National Security

ISSN: 0268-4527 (Print) 1743-9019 (Online) Journal homepage: https://www.tandfonline.com/loi/fint20

Towards understanding cybersecurity capability in Australian healthcare organisations: a systematic review of recent trends, threats and mitigation

K. L. Offner, E. Sitnikova, K. Joiner & C. R. MacIntyre

To cite this article: K. L. Offner, E. Sitnikova, K. Joiner & C. R. MacIntyre (2020) Towards understanding cybersecurity capability in Australian healthcare organisations: a systematic review of recent trends, threats and mitigation, Intelligence and National Security, 35:4, 556-585, DOI: 10.1080/02684527.2020.1752459

To link to this article: https://doi.org/10.1080/02684527.2020.1752459

Published online: 22 Apr 2020.

INTELLIGENCE AND NATIONAL SECURITY
2020, VOL. 35, NO. 4, 556–585
https://doi.org/10.1080/02684527.2020.1752459

Routledge
Taylor & Francis Group

ARTICLE

Towards understanding cybersecurity capability in Australian healthcare organisations: a systematic review of recent trends, threats and mitigation

K. L. Offner, E. Sitnikova, K. Joiner and C. R. MacIntyre

ABSTRACT

Cybersecurity threats in the Health sector are increasing globally due to the rising value of sensitive health information and availability of digitalised personal health records. This systematic review compares international and Australian health system cybersecurity landscapes in relation to the introduction of universal electronic health records. It examines recent trends in healthcare cybersecurity breaches that can disrupt essential services if patient safety and privacy are compromised. Often health systems and health mangers are ill-equipped to mitigate such threats. Recommendations are provided to proactively mature the cybersecurity culture within healthcare organisations, thus increasing their resilience to cyber threat.

Introduction

Healthcare is a ubiquitous need and affects every person in society. The healthcare sector is responsible for collecting and storing highly sensitive and confidential data whilst simultaneously being required to share it amongst medical staff, patients and other organisations. HealthCare Systems (HCS) are compelled to evolve with advances in technology. The transition of healthcare from hospital centred, specialist focused approaches to distributed, patient centred care has been facilitated through health record digitalisation[1] and is widely recognised as both inevitable and essential.[2] Breaches of HCS cybersecurity that expose personal information or data will negatively impact both patients and the healthcare institution, with potentially life-threatening consequences.[3] The cybersecurity risk to healthcare, including ransomware attacks, hacking of personal medical devices and theft of personal medical data, is continuously rising.[4] Stolen health records are worth more than records from any other industry,[5] due to the high value of personal information.[6] Sold on the darkweb, they can fund criminal activity and enable identity theft, blackmail, extortion and even murder.[7] In 2015, the US Office of Personnel Management (OPM) and Anthem Health, which provides healthcare for Federal employees, were both hacked within months of each other, apparently by the same perpetrator.[8] This means the hackers can link personnel records with sensitive health data for federal employees and enable targeted harm to high-value individuals.[9] Despite a global increase in cyberattacks on health entities the healthcare sector has significantly trailed other sectors in the ability to secure its critical data.[10] Cybersecurity in healthcare is identified as an emerging health security challenge, but there is low awareness in the health sector of the risk.[11] A healthcare cybersecurity capability approach is required to address increasing cyberthreats. The recent introduction of a universal electronic medical record My Health Record (MHR) in Australia provides an opportunity to examine healthcare cybersecurity capability.

CONTACT K. L. Offner Kim.offner@uts.edu.au

Health cybersecurity capability is the capacity of the organisation or sector to produce an outcome, such as proactive cyber-awareness and defence.[12] Healthcare institutions have traditionally been focussed on patient care and not cybersecurity and pursued the electronic health record as a holy grail of optimal patient care. Yet healthcare lags behind other sectors in both securing data and developing comprehensive employee cybersecurity training programs.[13] As patient information grows in both volume and value, health managers are required to develop cybersecurity capability across organisations. Cybersecurity capability development includes updating existing information technology but also recognising the need for, and proactively acquiring, new technology, cybersecurity talent and comprehensive organisation training.[14]

The paradigm shift to digitalised healthcare requires information technologies to store vast amounts of electronic patient information across diverse operating systems.[15] The integration of new technologies with outdated, legacy or unsupported operating systems compromises interoperability and increases cybersecurity vulnerability.[16] The 2017 global WannaCry ransomware attack[17] provides a stark example of this. Widespread use of obsolete Windows XP software[18] in combination with ignored cybersecurity warnings to undertake system upgrades enabled the malware to spread across the National Health Service (NHS) in the UK. WannaCry severely affected NHS" ability to provide patient care for a week between 12–17 May 2017, spread to 200,000 computers in over 100 countries, and is the largest malware cyberattack to date.[19] WannaCry had not specifically targeted the healthcare sector,[20] but was able to spread to 80 out of 236 NHS trusts and 603 primary care organisations across England[21] due to poor cyber-hygiene and a lack of appreciation amongst healthcare executive management of the business risk impact of cyber breaches.[22] Ambulances had to be diverted, diagnostic equipment was infected, pathology and radiology unable to function, patient records were inaccessible and nearly 7000 medical appointments were cancelled.[23]

Healthcare has the reputation of 'low security maturity',[24] and lacks sophisticated data security tools compared to other industries.[25] This is due to budgetary constraints,[26] lack of cybersecurity training and awareness among health managers, the heterogenous healthcare information infrastructure, and innumerable wireless connected devices.[27] Current healthcare cyber-defence is often reactive and undertaken after malicious attack.[28] The retrospective nature of healthcare cybersecurity,[29] along with sector reliance upon perimeter defence (antivirus, firewalls) for protection[30] compounds cyber risk. Such measures are unlikely to protect against sophisticated and persistent attacks[31] or mitigate insider threats.[32] Other significant barriers to healthcare cybersecurity are lack of appropriate cybersecurity professionals working in health,[33] constantly emerging and evolving malware threats,[34] and complex network infrastructure.[35]

Aims

- To compare the international and Australian health system cybersecurity landscape in relation to introduction of the universal MHR in Australia.
- To examine recent trends in healthcare cybersecurity breaches in Australia and worldwide.

Methods

A systematic review of the relevant literature and background information regarding global cybersecurity in health systems and digital medical records was conducted using the PRISMA criteria. Ten databases in total were searched: Medline/PubMed; Embase; Emcare; CINAHL; Psycinfo; Web of Science; Scopus; Compendex; IEEE; and Google Scholar Advanced Search to obtain grey literature. The key concepts utilised were e-health records AND cybersecurity. The keywords used in the search are listed below:

- Electronic health records/OR medical record, computerised/OR digital health record* OR electronic medical record*

- Cyber security/OR data security/OR medical identity theft/OR terrorism/OR Malware/OR Ransomware OR Cyber adj4 (crime OR attack OR security OR threat OR terror)

The Google Scholar Advanced Search utilised 'healthcare AND cybersecurity' to obtain grey literature such as conference proceeding books, conference papers and thesis dissertations. Due to the emergent nature of electronic health records, the current social and political debate around privacy and security and the recent changes to MHR implementation, the decision was made to include media reports. The Factiva database was utilised to search relevant media articles. Key concepts were health data breach AND MHR. The search process is illustrated below in Figure 1.

Study eligibility

Articles were considered for inclusion if they were:

- English language publications,
- Published between 2014–2019 in a peer reviewed or scholarly journal,
- Full-text version of the manuscript, conference paper or prospective thesis/paper,
- Strategy, Guideline, Report or Policy review documents which provide relevant subject insight or recommendation

Study selection

Studies were selected if they discussed an issue related to cybersecurity in healthcare either in the title or the abstract. Studies were excluded if their content was not specific to cybersecurity within healthcare, or if they were focused solely on presenting a technical algorithmic solution without discussion of the general cybersecurity landscape. Two independent reviewers checked titles and abstracts as collated on a shared EndNote library.

Information synthesis

The findings of the included studies were synthesised narratively into themes which included:

(1) Theme 1 – emerging trends in cybersecurity risk,
(2) Theme 2 – cybersecurity capability countermeasures and mitigation strategies,
(3) Theme 3 – current cybersecurity issues within Australia.

An analysis of Australian healthcare cybersecurity capability is presented in the discussion session.

We also reviewed the accreditation requirements of the two peak bodies in health management in Australia, the Australian College of Health Systems Management Australia and the Royal Australasian College of Medical Educators, for health cybersecurity as a curriculum requirement.

Results

We identified 316 relevant records. Of the 316 records, 100 outlined cyberattacks on HCS. The common cyberattack types identified in the review are defined and categorised in Table 1 below. Mitigation strategies were presented in 131 of the records. An additional 29 records outlined cyber risk or cyberattack type, but also presented a specific countermeasure to potentially mitigate the threat discussed. A total of 27 records presented findings relevant to the Australian context. A summary of findings is presented in tables 2 and 3.

Ten systematic reviews were identified as part of the search, 5 of which were published since 2018. There were 32 Reports included as relevant to this review. These included official

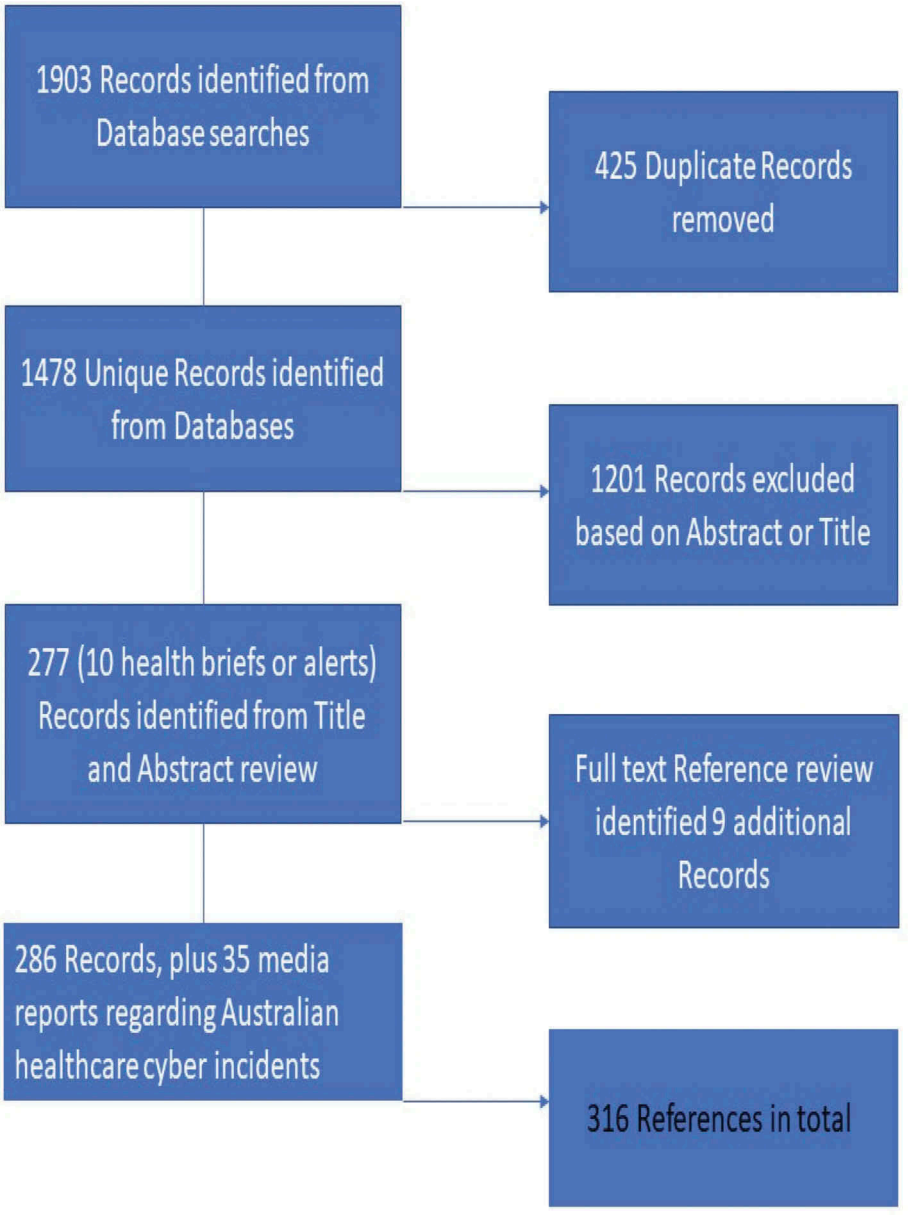

Figure 1. Flow chart of literature search screening process.

Government responses to data breaches (n = 3), Australian Government publications (n = 9), cybersecurity industry benchmark reports (n = 9), the Royal Australian College of General Practitioners cybersecurity position paper (n = 1), and finally a joint academic and consumer group report. Grey literature was identified and included to address publication bias. A total of 15 Conference Proceeding papers and 4 dissertation thesis papers were identified. The results are summarised in Table 1–4. Table 1 shows HCS Cybersecurity Attack and Threat Categories, Table 2 shows a summary of findings under Theme 1 (Cybersecurity Threat and Risk Landscape), Table 3b shows a summary of findings under Theme 2 (Cybersecurity Capability, Countermeasures and

Table 1. HCS cybersecurity attack and threat categories.

Attack Type	Definition and Examples	Threat Category
Hacking	The use of a computer to gain unauthorized access to data in a system to enable theft or destruction.[a] Mimikatz steals credentials from accessed server domains to enable network compromise. Used with other tools in NotPetya[b]	*Accessibility & Integrity* via system and network infiltration and *Confidentiality* of credentials.
Distributed Denial of Service (DDoS)/Denial of Service (DoS)	DDoS/DoS attacks are main threats to the availability of physical and network systems. Creates traffic jamming that disrupts communication through interference or collision, overflowing the buffer memory of network cards, and broadcasting spoofed network packets.[c] Network flooding with useless data traffic exhausts network resources making it unavailable to the authentic users.[d] Able to be spread by mobile applications and can be refined to also exfiltrate information.	System *Accessibility*
Malware	Computer code created with malicious intent, often spread through phishing. Can disrupt entire organisation or lie dormant until initiated. Masqueraded as legitimate upgrades and used in the 2015 Anthem Health Insurance attack.[e]	*Accessibility* through DoS, or attack to vendor supply chains; *Integrity* of data through encryption; *Confidentiality* via data breach/theft
Ransomware	Encrypts files on compromised computers for cryptocurrency ransom.[f] Potentially life threatening as decryption key may not be provided after payment.[g] Able to avoid detection and only encrypt specific information[h] or can spread across entire network.[i] New ransomware code is developed at a rate of 100,000 a day.[j] In 2019 it compiled over 70% of malware incidents.[k] Spread via inadvertent download of code through infected websites or most commonly in healthcare, in phishing emails.[l]	*Integrity, Accessibility and Confidentiality* of physical and network systems and data
Phishing	Indiscriminate scam emails that contain malware allowing attackers entry into the system by installing a virus, or to trick users to reveal credentials.[m] Can create a 'beachhead' to launch other attacks – often to install malware.[n] Increasingly sophisticated and role targeted, often employing follow up messages or calls to encourage opening infected links.[o] Used to deploy Remote Access Tools such as JBiFrost.[p]	*Accessibility* & *Integrity* via email compromise & computer intrusion to enable administrative control. Due poor cyber-hygiene practices of end users
Spear phishing	Carefully targeted emails to small groups or individuals using personalised information to 'verify' the message & link.[q]	*Confidentiality* of targeted credentials
Command and Control Obfuscators	Can both disguise the actor's communication within an infected network to evade detection and re-direct network traffic to alternate hosts/ports. Has been used to exploit Windows vulnerabilities.[r]	Network and web server compromise affecting *Accessibility, Integrity and Condentiality*
Lateral Movement Frameworks	Continued penetration tools that escalates privileges, collects credentials and enables information download. Able to move across a network and operate from memory making detection difficult. Can be used to initiate inter-organisation phishing exercises.	As Above
Sinkhole	Internet of Things (IoT) and/or medical device compromise at network level that diverts all network traffic to a compromised sensor node. As it is an active attack can escalate to DoS.[s]	*Confidentiality, Accessibility and Integrity*
Wormhole	Uses packet or relay connections to form a tunnel between two attackers to route data. Can potentially affect any device with connection to a wireless sensor network.[t]	As Above
Sybil	Sensor nodes are provided with multiple identities creating redundant or false information from medical or monitoring devices.[u]	Integrity of vital patient information

(*Continued*)

Table 1. (Continued).

Attack Type	Definition and Examples	Threat Category
Hello Flood	Attackers with high powered transmitters can create a signal that appears to be in proximity to the device to mimic a parent node for eavesdropping or to broadcast data to the entire network.[v]	Confidentiality
Cryptojacking or Crypto Mining Malware (CMM)	Malware introduced to draw huge organisational computing power and network resources to covertly mine digital currency.[w] CMM detections increased 459% between 2017 to 2018.[x]	
Orange Worm malware	Installs backdoor software that lies dormant within systems to target healthcare supply chains such as pharmaceuticals, IT companies and medical device vendors, potentially to enable economic espionage by nation-states.[y]	Accessibility of supply

Key: Orange = System Threat; Blue = User-based Threat; Green = Mobile or medical connected device Threat
[a]Carter, "Considerations for Genomic Data Privacy and Security when Working in the Cloud."
[b]Australian Cyber Security Centre (ACSC), Joint report on publicly available hacking tools.
[c]Almohri et al., On Threat Modeling and Mitigation of Medical Cyber-Physical Systems.
[d]Ahanger & Aljumah, "Internet of things: A comprehensive study of security issues and defense mechanisms."
[e]Institute for Critical Infrastructure Technology (ICIT), Industry Brief: Hacking Healthcare.
[f]Wirth, "Cyberinsights. The Times They Are a-Changin': Part One."
[g]Boddy et al., "An investigation into healthcare-data patterns."
[h]Lee, Moon & Park. CloudRPS: a cloud analysis based enhanced ransomware prevention system.
[i]Sittig & Singh. "A Socio-technical Approach to Preventing, Mitigating, and Recovering from Ransomware Attacks."
[j]Spence et al., "Ransomware in Healthcare Facilities: A Harbinger of the future?"
[k]Verizon, 2019 Data Breach Investigations Report.
[l]Lee, Moon & Park. CloudRPS: a cloud analysis based enhanced ransomware prevention system.
[m]Institute for Critical Infrastructure Technology (ICIT), Industry Brief: Hacking Healthcare.
n Wright, Aaron & Bates. "The Big Phish: Cyberattacks Against U.S. Healthcare Systems."
o Wirth, "Cyberinsights. The Times They Are a-Changin': Part One."
p Australian Cyber Security Centre (ACSC), Joint report on publicly available hacking tools.
q Wright, Aaron & Bates. "The Big Phish: Cyberattacks Against U.S. Healthcare Systems."
r Australian Cyber Security Centre (ACSC), Joint report on publicly available hacking tools.
s Ahanger & Aljumah, "Internet of things: A comprehensive study of security issues and defense mechanisms."
t Ibid.
u Ibid.
v Ibid.
w BDO USA Healthcare, Brace for the Breach - Cyberthreat Insights 2019.
x Verizon, 2019 Data Breach Investigations Report.
y BDO USA Healthcare, Brace for the Breach - Cyberthreat Insights 2019.

Table 2. Summary of findings – Theme 1 Cybersecurity Threat and Risk Landscape.

Population: Digitalised/electronic health records, personal health information and data
Setting: Healthcare Systems (HCS)
Intervention: International cybersecurity risks and threats (n = 100)
Comparison: Australian cybersecurity risks and threats (n = 19)

Outcomes (sub-themes)	International Records	Australian Records	Comments
Medical Cyber Physical Streams (MCPS) and/or Medical Internet of Things (MIoT)	40 24	5 8	Lack of interoperability combined with the vulnerability caused by MCPS intrinsic attributes are recognised as the most significant emerging cybersecurity threat in international records
Breaches of privacy, confidentiality and/or consent for data use	11 10	1 1	Australia (TGA) and US (FDA) greater MCPS regulation than UK/Europe Australian records remain predominantly concerned with threats to data protection, privacy and confidentiality.
Cloud Computing	8	3	Issues of consent are discussed concurrently with data protection in Australian records.
Malware	7	1	Recognised in international records as a potential attack vector to data in storage and transit
Health Apps			Lack of Australian records outlining malware specific threats. Australian malware information accessed through Australian Government publications (Office of Australian Information Commissioner or Australian Cyber Security Centre).
Insider threat			Information security issues and lack of regulation of health apps are addressed in recent records, especially when endorsed for use in mental health and dementia Paucity of records discussing this despite cybersecurity industry recognition it is the leading cause of data breach worldwide.

Table 3. Summary of findings Theme 2 – Cybersecurity Capability, Countermeasures and Mitigation strategies.

Population: Digitalised/electronic health records, personal health information and data
Setting: Healthcare Systems (HCS)
Intervention: International cybersecurity capability, protective countermeasures or mitigation (n = 131)
Comparison: Australian cybersecurity capability, protective countermeasures or mitigation (n = 15)

Outcomes (sub-themes)	International Records	Australian Records	Comments
Cryptographic architecture or technological solutions	**51** 22	11 1	International and Australian focus on technological solutions rather than holistic capability building approaches, education, or recognition of insider threat.
Risk assessment and governance	16	1	A comparison of risk assessment frameworks is presented in Table 4.
Regulation and/or legislation	16	0	A comparison of regulatory and legislative protection is presented in Table 4.
Holistic approach/Proactive cybersecurity culture	12 9	0 1	The importance of developing a proactive culture that engages all employees is presented in recent international records The need for practical, scenario-based education and simulation is emphasised, especially to address inadvertent insider threat
Education and/or simulation	5	0	
Capability and cyber maturity			System and organisational maturity to detect, identify, plan and manage data and infrastructure protection.
Cyber-hygiene			Digital security practices such as strong passwords, 2 factor authentication, encryption of shared patient information and data etc.

Table 4. International regulatory frameworks for data privacy and security.

Country	Framework/Regulation	Remit
European Union	General Data Protection Regulation (GDPR) 2018 is designed to harmonise data **privacy** laws across Europe to protect against privacy and data breaches.	Applies to all personal data held by an organisation. Breaches reported to the Information Commissioner's Office with fines for non-compliance up to €20 m.
United Kingdom	Data Protection Bill 2017	
United States	Health Insurance Accountability and Portability Act (HIPAA) 1996 and Omnibus 2013	Privacy and security rules. Mandatory end-to-end encryption of data that is in motion and at rest. Mandatory education of staff,[a] risk assessment[b] and breach notification. Non-compliance can lead to substantial fines of millions of dollars.
United States	The National Institute of Standards and Technology (NIST Framework)	Guidelines on security and privacy in public and cloud computing. Framework for Improving Critical Infrastructure Cybersecurity, 2018 includes five capability categories: identify, protect, detect, respond, and recover. Not specific to healthcare.[c]
United States	Food and Drug Administration (FDA).	Oversight of medical devices process, regulatory decision making, post-market surveillance, and product development life cycle.[d]
Canada	Canadian Personal Health Information Protection Act (PHIPA) 2005 update. Personal Information Protection and Electronic Documents Act (PIPEDA) of 2005.	Includes health technology and allows data deidentification for health systems planning, delivery, and design. Audits undertaken by Privacy Commissioner. Outlines the role of health records and technology: organisations can conduct data linkages if patient privacy is protected during re-identification. Consent required.[e]
Australia	My Health Records Act and Privacy Act (the My Health Records Rules and Regulation), Australian Privacy Act 1988, and the Data Privacy Amendment, Notifiable Data Breaches Act 2017	Covers the collection, use and disclosure of the personal health information, as well as penalties. Expanded upon in the next section. No clear distinction made between those who control or own personal information and those who process personal information.[f]
Global	International Organization for Standardization (ISO)	Used by Australian Digital Health Agency (ADHA). Comprehensive but complex and expensive to implement.[g]

[a]Upendra et al., "Operationalizing Medical Device Cybersecurity at a Tertiary Care Medical Center."
[b]Abouzakhar and Angelopoulou, Internet of Things Security: A Review of Risks and Threats to Healthcare Sector.
[c]Akinsanya, Papadaki & Sun. Current Cybersecurity Maturity Models: How Effective in Healthcare Cloud?
[d]Schwartz et al., "The evolving state of medical device cybersecurity."
[e]Thakkar & Gordon, "Privacy and Policy Implications for Big Data and Health Information Technology for Patients: A Historical and Legal Analysis".
[f]Flaumenhaft & Ben-Assuli. "Personal health records, global policy and regulation review."
[g]Akinsanya, Papadaki & Sun. Current Cybersecurity Maturity Models: How Effective in Healthcare Cloud?

Mitigation Strategies) and Table 4 shows the identified international regulatory and legislative frameworks for data privacy and security.

Theme 1 – Emerging trends in cybersecurity risk

Cyber-attacks can occur at any connection of the network and at any endpoint. Interoperability of software, operating platforms, medical device interfaces and information exchange networks is an essential requirement of a digitalised health system and is crucial to cybersecurity risk management.[36] The emergence of medical cyber physical streams, wireless connectivity and the advent of medical applications in healthcare have exponentially increased attack surfaces and vectors.[37] Protecting every entry point to the health system is now impossible.[38]

Medical cyber physical systems

This term encapsulates Medical Internet of Things (MIoT) and medical devices, both implantable and wearable. Medical Cyber-Physical Systems (MCPS) are increasingly used in hospitals to provide high-quality healthcare and have emerged as promising platforms for monitoring and controlling multiple aspects of patient health.[39] It is estimated there will be 20 billion connected devices by 2020, and 50 billion by 2028.[40] The intrinsic features of MCPS increase their inherent security risks.[41] These features make MCPS myriad, mobile, heterogenous and increasingly ubiquitous.[42] They are often left unattended (as in implantable devices) to record intimate physiological data and are constrained in size, power and memory function which provides them only basic security capability.[43] MCPS features make them vulnerable to compromise[44] meaning their connection to and reliance upon the healthcare network significantly increases the cybersecurity risk to the entire healthcare system.[45] MCPS have become considerable potential attack vectors[46] to enable intrusion by malicious actors, installation of malware and alteration of treatment delivery.[47] Cybersecurity measures such as vulnerability scans or patch management are often not available[48] or only possible by manufacturers.[49] There exists an international lack of clarity on post-sale ownership, software update and security regulation of MCPS.[50] Manufacturers may be reluctant to provide documentation detailing device cybersecurity vulnerabilities[51] or patching and upgrade policies[52] as this is viewed as proprietary information. The absence of healthcare standards[53] to promote MCPS interoperability[54] increases incompatibility[55] between different healthcare systems and medical devices[56] and creates a healthcare vendor market that pushes patient devices to market before cybersecurity issues are addressed.[57] The cybersecurity vulnerability of medical devices and the lack of vendor and regulatory oversight has been recognised as a strategic priority by the Australian Therapeutic Goods Administration.[58]

Data confidentiality, privacy and consent

Privacy of confidential patient data and issues concerning the use of personal information was the next sub-theme identified. Risk to personal information can be categorised as cybersecurity threats to healthcare confidentiality, accessibility and integrity.[59] Confidentiality is compromised through loss of personal health records or data, as well loss of consumer confidence.[60] Accessibility to health records, software platforms, operating systems and hardware is affected through denial of service (DoS) malware or ransomware attacks.[61] Integrity of health data is exposed if it is corrupted, deleted or altered; or if wireless communication to essential devices or monitors are compromised.[62]

Healthcare is both a vulnerable and attractive target for cyberattack due to its economic size[63] and broad attack surface.[64] An increased focus by the health sector on cybersecurity is warranted considering the criticality of the health sector and the type of user information stored within health information systems.[65] Health information and medical data are highly valuable assets to patients, healthcare providers and identity thieves alike.[66] Estimates place health data as between ten[67] and

twenty times[68] more lucrative than credit card or banking details. Credit card or banking details can be changed if stolen. Uniquely identifiable health history or data cannot.[69]

Cloud computing

Cloud computing was identified as a cybersecurity risk to data and information both during transfer and storage. The huge volume of health information produced has made centralised storage, encryption, deployment and maintenance of data prohibitive at the individual organisation level.[70] The advent of cloud computing allowed storage, processing and analysis of data to be outsourced to a remote server.[71] Cloud models share the cost of data accessibility and management, as well as sharing the cybersecurity risks – the scalability and efficiency of cloud computing means any potential breach exposes data to a far wider audience.[72] There are two attack vectors possible with cloud storage – attacks to data at rest which modifies or replaces information; and attacks to data in motion occurring during transfer to or from geographically distributed cloud servers. Encryption technology is essential to ensure the security of patient health information and data stored on cloud platforms.[73] A compromised host operating system could enable attackers to access hypervisor processes and services (such as a virtual machine monitor, a computer software, firmware or hardware that creates and runs virtual machines) and, potentially, any client application.

Malware

Records under this sub-theme discussed malware generally or applied examples such as the WannaCry attacks in the UK. Malware attack types and threat categorisation is outlined in detail in Table 1.

Health application ('app') security

The combined ubiquity of use and paucity of security provisions of Health apps are recognised as an increasing cybersecurity risk to the confidentiality of personal data and to the integrity of interconnected HCS infrastructure. Health apps can generate, store, and process huge volumes of identifiable health data.[74] The ubiquity, simplicity, low cost and improved encryption of WhatsApp, makes it attractive for telemedicine services[75] in resource constrained settings[76] and to facilitate professional networks and team communication.[77] Use of WhatsApp is now so commonplace amongst clinicians that urgent guidelines are required to ensure that clinicians do not inadvertently breach patient privacy or confidentiality.[78]

Mental health apps are promoted by health services as a discreet, accessible and affordable alternative to face-to-face therapy.[79] However, little research exists examining the safety and security of apps in medical practice, or of the proliferation of apps endorsed for mental health and dementia. A recent Australian study found that over half of government endorsed apps did not have a privacy policy to inform users how personal information would be collected, retained or shared with others.[80] Patient confidentiality and safety[81] or the security of communications,[82] are often not considered by app developers who are largely unregulated in terms of content, authorship or trustworthiness.[83] The author of a cross-sectional survey investigating the privacy and information security of health apps in wearable devices[84] identified a lack of awareness among respondents (n = 106) regarding the confidentiality or security of the data collected from their wearable device apps, including what was obtained and how it was transmitted or stored. The author postulates that these results reflect a wider lack of knowledge about potential data security and privacy risks throughout the general population. That these apps have received government endorsement for use in those with dementia and mental illness is of concern. Without adequate security provisions in place, health applications can be vulnerable to both active and passive attacks, resulting in data modification or theft.[85]

Insider threat

That cybersecurity mechanisms within health do not appropriately address the issue of insider threat as the 'entry point'[86] for ransomware was the final sub-theme identified (n = 7). Most data breaches involve some level of insider cooperation, either intentional or not.[87] Not recognising or responding to phishing emails remains a substantial problem[88] with email the most common vector through which healthcare organizations are attacked.[89] Most insider issues are due to ignorance rather than malice, but accidental error is equally damaging, making the lack of health information technology and cyber-hygiene knowledge an important threat. Studies indicate that respondents use weak or insecure passwords and are unaware of data security violation procedure.[90] Malicious intent as it relates to cyber-attacks is poorly understood and requires the integration of human factors into cybersecurity risk assessment to fully understand and characterise its impact upon mitigation strategies.[91] Inadvertent information leakages will remain inevitable due to the innumerable risks associated with collaborative sharing in complex healthcare network systems.[92]

Theme 2 – cybersecurity capability, countermeasures and mitigation strategies

The mitigation of risk to and protection of sensitive health information is now a global concern. The concept of a Cybersecurity Centre for Threat Control (based on the US Centers for Disease Control or a Cyber World Health Organisation)[93] is suggested to enable global recognition of the need for international collaboration to combat cybercrime. The incorporation of data breach response into organisational disaster plans, along with proactive partnerships between governments, industry and providers to enhance and develop collective security across healthcare sectors is advocated.[94]

Cryptographic architecture or technological solutions

There is strong emphasis, both in the international and Australian records, upon technological solutions and advanced cryptology to promulgate cybersecurity solutions. The greatest number of records identified (n = 63) concerned technological cybersecurity protective architecture, often developed by the authors of the records. It is beyond the scope of this paper to compare and discuss the different cryptographic security available to address data sharing and storage of patient information across network systems, cloud environments or through remote patient monitoring systems.[95] However, two cryptographies will be briefly mentioned due to their broad applicability and potential benefit for health specific challenges. The first, homomorphic encryption (HE) ensures strong security and privacy guarantees whilst enabling analysis on encrypted data and sensitive medical information.[96] Fully homomorphic encryption is versatile but has substantial computational requirements that at present slows processing significantly.[97] HE can also be used in mobile devices to transfer and store medical data without decrypting it, preserving privacy if a node is compromised.[98]

The second is Blockchain. Blockchain is a peer-to-peer distributed ledger technology that was initially used in the financial industry.[99] Its characteristics of decentralization, verifiability and immutability enable blockchain to securely store personal medical data.[100] Immutability ensures that any data, once stored in blockchain, cannot be altered or deleted.[101] Applications in health include integration of health information,[102] aggregation of data for research.[103] In blockchain all the data, including the keywords and the patients' identity are public key encrypted with keyword search. Challenges to blockchain include scalability, security and cost.[104] Whilst blockchain itself is secure, it can be accessed through stolen credentials and root privilege exploits.[105] Blockchain technology will require more research before large-scale production implementations.

Risk assessment and governance

Healthcare data breaches continue to rise[106] with at least one data breach per day in the health industry globally.[107] The average total cost of a healthcare data breach in 2019 was 6 USD.45 million

compared to the 2017–18 average of 4 USD.08 million. This is 65% higher than the average total cost of a data breach in any other industry.[108] On average, it takes the healthcare industry longer than any other to identify (mean 236 days) and rectify (93 days) a data breach.[109] The longer a breach goes unnoticed, the greater the estimated cost. The importance of comprehensive cybersecurity risk assessment therefore cannot be underestimated in order to proactively identify vulnerabilities and detect threats or system breaches.[110] This must include detailed assessment and analysis of the cybersecurity risk and vulnerability of all information technology hardware, software, MCPS and vendor or third-party partner cybersecurity agreements.[111] Healthcare cybersecurity risk assessments and strategy frameworks should be standardised across jurisdictions and should include stipulations that demand vendor cybersecurity compliance and accountability.[112] The National eHealth Security and Access Framework v4.0 (NESAF) is the Australian cybersecurity risk assessment framework developed to guide health sector data protection and eHealth security.[113] The applicability, practicality and adoption of NESAF in practice is difficult to determine. The National Institute of Standards and Technology (NIST) Framework, which was developed in the US as a healthcare specific cybersecurity assessment model, could be adopted to the Australian healthcare context,[114] and is used in HCS across the US.

'Whitehat' or 'Ethical' hackers[115] should also be utilised to regularly test and assess cyber vulnerabilities. 'Whitehats' are professional hackers who undertake penetration and infiltration exercises and attempt to breach cybersecurity defences.[116]

Regulation and/or legislation

Securing the privacy of collected information and data is a major concern of patients[117] and the reason why many withhold consent for the use of their data in research.[118] Patient privacy specifically refers to 'the right of patients to determine when, how, and to what extent their health information is shared with others.'.[119] Regulatory and policy oversight can decrease data and privacy breaches, as indicated by the HIPAA Omnibus Rules 2013[120] which restricted healthcare vendor access to patient information.[121] However comprehensive policy will not guarantee cybersecurity if not reflective of actual healthcare practice, culture or infrastructure limitations, as evinced in the NHS with WannaCry. Nor will it entirely protect against insider agents.[122]

A comparison of international privacy and security frameworks and regulations is presented in Table 2.

Holistic approach toward proactive cybersecurity culture

There is recognition within the international literature that healthcare cybersecurity is a complex socio-technical challenge[123] requiring a holistic integrated approach[124] to improve staff awareness,[125] competence,[126] and mitigation of threats across the industry. The international records also highlight the importance of developing a proactive cybersecurity culture,[127] in which compliance to protecting information is embedded.[128] Significantly, this theme is not discussed within the Australian records.

There is also recognition that merely enforcing security policies and procedures will not drive cultural change or learning.[129] Healthcare leadership must embrace cybersecurity and develop strong cultures of cyber-vigilance[130] throughout organisations and amongst all staff[131] to develop a robust, proactive incident response. Building a culture that systematically and continuously analyses the cyber context of an organisation will enable vulnerabilities and threats to be identified.[132]

Education and simulated environments

That staff cybersecurity education is the most important strategy[133] against data breaches is not addressed in the identified Australian records. The essential need for comprehensive employee training and education[134] to enable the identification and assessment of risk[135] is discussed throughout the international records. Cybersecurity simulation models[136] indicate that experienced managers make

less effective cybersecurity decisions than novices, as they are more likely to seek an optimal decision utilising past experiences. The unpredictable 'zero-day' cyber-attacks and ever evolving nature of cyber threats often means optimal reactive decisions are not possible. Rather, the capability to make proactive preventative decisions is key. As employees are often the inadvertent facilitators of security breaches,[137] behavioural skills training and education to raise privacy-protection awareness and change habitual information technology habits into conscious cybersecurity decisions is required.[138] Staff will engage with cybersecurity if interventions are not costly (i.e. time consuming or onerous) and if self-efficacy is enhanced through active involvement in the training.[139] Simulation based training[140] to practice and develop cybersecurity capabilities can facilitate this.[141] The magnitude of cybersecurity organisational capability and individual employee skills required to mitigate the risk of vulnerabilities and breaches cannot be underestimated.[142]

Capability and cyber maturity

Cybersecurity capability is identified as a strategic asset that every health organization must adopt,[143] along with the concepts of building organisational resilience and the capacity to learn from mistakes.[144] Cybersecurity capability includes the skills, knowledge and competence[145] of the workforce, organisation, sector and nation to detect, mitigate and protect against threat. The Australian HCS is recognised as having low cybersecurity capability maturity.[146] The lack of an Australian healthcare cybersecurity capability model is recognised as a significant security risk in a country that has adopted an opt-out digitalised health record with MHR.[147]

Cyber-hygiene practices

Organisational cyber-hygiene practices are recognised as mandatory safeguards that include email data encryption of patient information, antivirus software, software updates, and at least two-factor authentication patient data stored or shared on cloud platforms.[148] Cyber-hygiene can be practised at employee level, such as in recognition and escalation of suspicious emails, or through enforcement of organisational policy regarding information sharing and protection.[149]

Theme 3 – current cybersecurity issues within Australia

> "In Australian cybersecurity, there are only two types of healthcare organisations – those that know they've been hacked and those that don't know they've been hacked".[150]

The average cost of a data breach in Australia in 2018 was estimated to be 2 USD.5 million.[151] It takes Australia a mean of 200 days (compared to 185 in 2017) to identify a data breach and 81 days to contain the breach incidents.[152] A cross-sector survey of 1894 senior executives and senior IT managers found that almost 70% of data breaches reported in Australia during 2018 were directly attributed to human error.[153] The number of documented data breaches involving the My Health Record (MHR) system in 2017–18 was 42, an increase from 35 the preceding year.[154]

At present the Office of the Australian Information Commissioner (OAIC) Notifiable Data Breaches only cover private providers and not public institutions or healthcare systems. This makes it extremely difficult to gauge an accurate picture of the cybersecurity landscape within Australia. An independent cybersecurity report of 4067 cyber incidents, many of which were not included in the quarterly Notifiable Data Breach reports, was undertaken during 2018.[155] The report analysis estimated that there were 445 healthcare cyber incidents in Australia in 2018 which equated to almost 24% of the Australian cyber breach total. Crucially, the report found that the healthcare industry had the lowest cybersecurity capability maturity of any Australian industry to identify and manage risks and to protect against or contain attacks. Specifically, the health sector lacks the capability to anticipate and respond to vulnerabilities and has a very high risk of experiencing a cyber incident within 12 months.[156] In 2018, no community healthcare providers had a dedicated budget for cybersecurity, and only 16% of public hospitals allocate funds specifically to cybersecurity.[157] Over

40% of clinical, specialist non-clinical, and administrative health staff believe they have no responsibility for cybersecurity, and 6.2% of Australian health organisations are unable to undertake operating system updates or patches due to legacy and end of life systems.[158]

MHR is the Australian digital health record that supports clinical care and is accessible to authorised health care providers wherever and whenever health services are initiated. The accuracy and relevance of the MHR is a joint responsibility of the individual and health care provider/s.[159] MHR is intended as an integrated eHealth Record 'to provide a consolidated record of an individual's health information for consumers to access and as a mechanism for improving care co-ordination between care provider teams'.[160] However, this probably remains an ambitious ideal given the unique challenges and complexities of the Australian federated funding model combined with the ambiguous responsibilities of the commonwealth and states in relation to different aspects of healthcare delivery.[161] As of 28 July 2019, MHR has a 90.1% participation rate across Australia, with 16,400 healthcare providers registered to the system.[162] The legislative framework underpinning the My Health Record system include My Health Records Act 2012,[163] My Health Records Rule 2016 and My Health Records Regulation 2012.

The Australian Digital Health Agency (ADHA) is the System Operator of MHR. Healthcare organisations and providers are required to report potential or confirmed data 'breaches' involving MHR to the System Operator (the ADHA). MHR data breaches must also be reported to the OAIC, except where the healthcare provider organisation is a state or territory authority.[164] The Digital Health Cyber Security Centre (DHCSC) provides operational security support for the MHR on behalf of the ADHA. During a national healthcare sector cyber crisis, the DHCSC is responsible for coordinating responses across the health sector in liaison with other Government organisations such as the Australian Cyber Security Centre and CERT (Computer Emergency Response Team) Australia.[165] In other words, the ADHA coordinates the cybersecurity response for major for cybersecurity breaches potentially caused by its own system vulnerabilities.

There is a paucity of research within Australia to measure or gauge Government, public-private sector or users' cybersecurity capacity to adopt or engage with an electronic health system such as MHR,[166] or to measure public understanding or perceptions of the potential use of their data in research.[167] A 2016 study[168] of the Personally Controlled Electronic Health Record (PCEHR) which essentially incarnated into MHR in July 2018, identified a multitude of security weaknesses. PCEHR consisted of a distributed network of interconnected systems with multiple interfaces required to enable a variety of providers, services and applications have access. The potential security weaknesses included system misconfiguration and implementation flaws, inconsistent authorisation policies and authorisation errors, and insecure transfer of privileges between healthcare providers in the PCEHR system.

An analysis of the timeline of Australian electronic health record development and an examination of the failed 'HealthConnect' project which preceded it (and which subsequently has been removed from Department of Health websites)[169] concludes that enduring tensions exist between those seeking to enhance the widespread availability of individual health information reform, and those who view it as a threat to privacy. There appears to be an inability to seek compromise or learn from divergent viewpoints and values. This has been particularly evident since the transition of MHR to an opt out system[170] which commenced on 16 July 2018 and was extended to 31 January 2019.

An important note of interest and consideration in the Australian cybersecurity context is that the healthcare industry is not included as critical infrastructure in the Australian Security of Critical Infrastructure Act 2018. In contrast, healthcare is recognised as critical infrastructure internationally.[171] The cybersecurity challenges created by digital health transformation requires universal cross-sectoral governance and coordination that emphasises 'healthcare as Critical National Infrastructure'.[172] This concept must be identified and protected. Creating cybersecurity silos in which healthcare is separate from other critical infrastructure could potentially weaken healthcare cybersecurity defence and capability.

Health security breaches in Australia

The following section draws on current open access media reports to ascertain the extent of health related 'breaches' or 'incidents' occurring within Australia. It is not intended to be exhaustive, but rather indicative of public awareness around the issues of cybersecurity as it relates to health generally and MHR specifically. As this is an emerging topic there are limited scholarly studies published.

Medicare has been plagued with security and privacy issues. Medicare details have been found available for sale on the dark web,[173] though any 'breach' of MHR was denied by ADHA: '*there has not been a cyber security breach of our systems as such, but rather it is more likely to have been a traditional criminal activity*' (involving a likely insider).[174] In 2016 the Australian government published a deidentified data set comprising the health details of 10% of the Australian population with information collected since 1984.[175] A week later a group of University of Melbourne academics privately informed the government that it had been able to re-identify the entire data set. The government immediately withdrew the data set from the website, however access logs indicated the data set had been downloaded 1,500 times but could not indicate who had accessed it.

The Australian Bureau of Statistics (ABS) was 'attacked' by Macquarie University academics to illustrate weaknesses in the TableBuilder tool used by ABS to enable low dataset counts to be retrieved. TableBuilder creates tables, graphs and maps of Australian census data. As the tool could be manipulated through unlimited query counts to include cell counts of 1, it was theoretically possible to re-identify individuals from census data.[176] The ABS were made aware of the vulnerability and have consequently changed the ToolBuilder interface.

HealthEngine was the government endorsed health appointment and scheduling app recommended by the ADHA. HealthEngine was exposed for editing negative reviews of GP practices, revealing the identifying details of 75 users via a website flaw and sharing hundreds of patient's data to personal injury legal firms.[177] HealthEngine provided access to MHR information such as Medicare records, test results, scans and prescriptions, for their app users to view on mobile phones.[178]

The difficulty of estimating the extent of cybersecurity breaches at state level is also raised. The state of NSW does not currently have a mandatory notifiable data breach reporting requirement, with the NSW Privacy Commissioner recommending a voluntary reporting scheme only.[179] As the National Data Breach scheme covers only federal government agencies and private sector organisations regulated by the Australian Privacy Principles, it virtually impossible to determine at a national level how many data breaches have occurred in the patient record systems of state-based health services.[180]

In a politically interesting and provocative act, the Victorian Auditor General hacked into his own health databases to expose sensitive patient information.[181] 'Patient data in Victoria's public health system could be easily hacked in a system riddled with weaknesses. The sector is highly vulnerable to cyber-attacks but staff awareness of data security is low, with issues around physical security, password management and other access controls'.[182] The official Auditor General report of Victorian security vulnerabilities states: 'There are key weaknesses in health services' physical and logical security covering password management and other user access controls. Staff awareness of data security is low, which increases the likelihood of success of social engineering techniques such as phishing or tailgating into corporate areas where ICT infrastructure and servers may be located'.[183] Also in Victoria, Cabrini Hospital based Melbourne Heart Group was unable to access approximately 15,000 files in February 2019 due to a server ransomware attack which corrupted and encrypted data. The ransom was reportedly paid: 'The My Health Record database will be an enormously tempting target for cybercriminals, not just now but for years, if not decades, to come.'[184]

These cybersecurity breaches whether notifiable or not, highlight the need for expertly trained cybersecurity professionals within the healthcare system. At present however, across NSW and Australia, there is a significant shortfall in sufficiently skilled and experienced cybersecurity experts required to develop products and services to meet ever evolving cybersecurity threats.[185] A new Certificate IV in cyber security was accredited nationally and is being implemented in NSW. One of

the key aspects of the NSW Cybersecurity Strategy is the alignment of streamlined cybersecurity training with industry. The report does not specifically mention the healthcare sector as an area of need.

The idea of informed consent is contentious within MHR, in that implied consent is taken to have been granted if there has been no active opt-out of the MHR system. Several authors question the notion of ongoing consent inherent within systems such as MHR.[186] 'The MHR Act does not specify the types of applicants that may access MHR system data for secondary use'.[187] Ongoing consent for secondary use of health information and data through MHR is condoned by the ADHA. Section 66(2) of the Framework[188] specifically enables 'secondary use of identified MHR data, noting that the System Operator (ADHA) is authorised to collect, use and disclose an individual's health care information (i.e. identifiable information) with the consent of the individual'.[189] How and when this consent is obtained, and by whom is not elucidated. The concept of ongoing consent as a breach of trust was raised when the Department of Human Services (DHS) acted on behalf of a third-party research organisation to access Medicare prescription data and contact (via letter) 50, 000 Australians who had been prescribed Lithium.[190] DHS claims that researchers had no access to private patient information disregards the point that an open access letter did contain private and potentially damaging information, as well as avoiding the issue that consent to share private prescription data had not been sought from any of the people contacted. How was consent obtained for secondary use in this case?

Health management training in Australia

Health management courses in Australia (such as Masters in Health Management) are a prerequisite for health manager jobs, yet these do not usually cover cybersecurity in their curricula. We did not identify any Masters level degree in health or hospital management which teaches cybersecurity. The Australasian College of Health Service Management (ACHSM) Guideline for Universities (2017) lists the five core competencies required of health service managers including the requisite knowledge, skills and behaviours expected of graduates. Cybersecurity (risk awareness, assessment, mitigation or management) is not listed. Nor is it mentioned by RACMA, the other peak body for health management.

Discussion

The healthcare sector is a complex system of interconnected organisations, providers, staff and patients, of which MHR is an important component. As highlighted throughout, human factors play a crucial role in cybersecurity with employees often the weakest link in organizational cybersecurity.[191] However, lack of mandatory reporting of breaches, lack of health management training in cybersecurity, lack of investment in cybersecurity infrastructure in health systems and use of old, legacy computing systems by hospitals, leaves Australia vulnerable to cyber-attacks. The potential advantages of a centralised and accessible patient health record are clear, but the cybersecurity issues inherent in collating, transferring and storing electronic patient records and health information must be comprehensively addressed. The Privacy Act 1988 protects the personal information of Australians in federal agencies or private organisations but does not cover state and territory public hospitals or health services. The OAIC Notifiable Data Breach Scheme (NDBS) has the legislative power under the Privacy Act IIIC to enforce penalties for data breaches. As of February 2018, no fines have been issued despite 967 reported breaches that have affected tens of thousands of Australians. This is in stark contrast to HIPAA in the US which accredits health care organisations to enforce cybersecurity and data protection compliance, and which issues penalties of between 50,000 USD to 1.5 USD million US for noncompliance. HIPAA was amended in 2005 to protect the electronic protected health information stored, collected or transferred by any healthcare provider. Even with the protections of HIPAA, the US has suffered ransomware attacks on hospitals and other health data

breaches. Without any such protection, Australia would be even more vulnerable, and should consider adopting a data protection scheme and framework that includes a critical analysis of the capability of multiple health providers and organisations with disparate operating systems to ensure health data security, confidentiality and integrity. Mandatory reporting of breaches should also be adopted. Cybersecurity capability must integrate all aspects of information security measures to protect health information from malicious access or breach.[192] Currently this provision does not exist within Australia. Health budgets should include resources to upgrade computer systems and hire cybersecurity personnel.

Data breaches adversely affect patient and community faith in healthcare to protect privacy and can lead to health information being withheld from healthcare providers due to confidentiality concerns.[193] Non-disclosure of information could lead to inaccurate or delayed diagnoses and compromised patient safety. However, it is essential that allaying security and privacy concerns and protecting provider reputation not become motivation to withhold cybersecurity breach reporting. Mandatory reporting and open discussion of cybersecurity incidents and breaches can facilitate real world learning and become the basis for education and training programmes. Cybersecurity capability is the capacity to manage previously unknown and seen situations and is best developed through multiple experiences of dealing with new situations.[194]

There are significant concerns regarding the ethics and consent in MHR. The rights of the patient regarding information collected about them, especially when considering 'ongoing consent' for secondary research sharing and use are paramount.[195] It could be argued that the least influential and most vulnerable people are being co-opted into MHR by an opt-out system, without their informed consent, further cementing health inequity and disparity. The Government has not fully addressed access and consent issues relating to many vulnerable communities including adolescents, abuse victims, sex workers, people with HIV and those with mental illnesses.[196] MHR raises the concept of a social licence not only for the open disclosure of potential cybersecurity risks, but also regarding the secondary use of health record data for research.[197] Consumers are entitled to control how their data are used, but this must be balanced to ensure that informed consent can be obtained to enable high quality primary and public health research.

It is impossible to completely mitigate cyber threats: 'Today it has become a question of "when", and "at what level"'[198] systems such as MHR will be breached. This does not invalidate the need for comprehensive, integrated and accessible electronic health records such as MHR. Instead it indicates the need for open disclosure of and proactive dialogue about cyber-attacks, innovate and holistic strategies and policies to reduce cyber threat, and cyber education and training for all health staff in order to develop cybersecurity awareness and capability. A healthcare culture that shares risk and threat information[199] is as essential as infrastructure management such as replacing legacy software and hardware, patching and updates and undertaking comprehensive risk assessments of connected devices.[200]

The overall cybersecurity maturity of healthcare organisations should be assessed to ensure a secure healthcare environment of interconnected systems.[201] The multiple health providers, organisations and agencies combining information into a comprehensive electronic health record provide innumerable potential attack interfaces. Cybersecurity threats are emerging from new vectors. Healthcare is also vulnerable from rapidly evolving technologies including wireless sensor networked medical devices, healthcare applications, and implantable medical devices. 'Enhancing the security and privacy in MCPS remains a serious challenge demanding careful considerations and joint efforts by the industry, the health systems, and the research community'.[202]

Limitations

There are three main limitations to this systematic review. The first is that the cybersecurity landscape is evolving at such an exponential rate, that new information is emerging regularly. The second is that as

this is such an emerging field, the number of scholarly research articles published on this topic is sparse. Third, the scope of this review was broad and some themes were not able to be considered in detail.

Conclusion

This review investigates the body of literature on global cyberattacks against the healthcare sector, in order to categorise the cyber threats to health, and present mitigating countermeasures or protective strategies in relation to a universal electronic health record in Australia. Cyberattacks against healthcare are rising due to the lucrative patient data available in digitalised health systems, and because healthcare has poor cybersecurity defences and awareness. Australia lacks some of the protections that other countries such as the US has, such as the HIPAA law and mandatory reporting of breaches. Outdated health computing systems and lack of investment by the hospital sector in cybersecurity is an additional problem. Health management training lacks cybersecurity content, and until this is addressed, the health system will remain vulnerable. If healthcare mangers are not taught essential cybersecurity skills, it is unlikely they will lead change in the development of healthcare cybersecurity capability and resilience in the workplace. There is no way to completely mitigate the risk of a cybersecurity incident or breach within the healthcare system, globally or within Australia. However, building a proactive healthcare culture of cybersecurity maturity can help to reduce cybersecurity risk.

Notes

1. Abd-alrazaqa et al., "Factors that affect the use of electronic personal health records among patients: A systematic review."
2. Zeb et al., U-prove based security framework for mobile device authentication in eHealth networks.
3. Abouzakhar and Angelopoulou. Internet of Things Security: A Review of Risks and Threats to Healthcare Sector.
4. Global Digital Health Partnership, Securing Digital Health 2018.
5. BDO USA Healthcare, Brace for the Breach – Cyberthreat Insights 2019.
6. Institute for Critical Infrastructure Technology (ICIT). Industry Brief: Hacking Healthcare.
7. MacIntyre et al., "Converging and emerging threats to health security."
8. Ibid.
9. IT News, "Hack linked to attack on US insurer Anthem".
10. Forcepoint Whitepaper. Life Support: Eliminating Data Breaches in the Healthcare Sector.
11. Gordon, Fairhall and Landman, "Threats to Information Security – Public Health Implications."
12. Jalali & Kaiser, "Cybersecurity in Hospitals: A Systematic, Organizational Perspective."
13. Argaw et al., "The state of research on cyberattacks against hospitals and available best practice recommendations: a scoping review."
14. See note 12 above.
15. Sittig & Singh. "A Socio-technical Approach to Preventing, Mitigating, and Recovering from Ransomware Attacks."; Small et al., "Patient Perceptions About Data Sharing & Privacy: Insights from Action."
16. Kruse et al., "Cybersecurity in healthcare: A systematic review of modern threats and trends."
17. National Audit Office Report, Investigation: WannaCry Cyber Attack and the NHS.
18. Wirth A., "Cyberinsights. Hardly Ever a Dull Moment: The Ongoing Cyberthreats of 2017."
19. See note 17 above.
20. Walker-Roberts et al., A Systematic Review of the Availability and Efficacy of Countermeasures to Internal Threats in Healthcare Critical Infrastructure.
21. O"Sullivan
22. Schwartz et al., "The evolving state of medical device cybersecurity."
23. See note 17 above.
24. Pratt, "How cyberattacks can impact physicians."; Connory, 2019 Annual Report. State of cyber security.
25. See note 20 above.
26. Farringer, "Cybersecurity Report Identifies Unique Challenges to Tackling Cybersecurity in Health Care."; Sedlack, Understanding Cyber Security Perceptions Related to Information Risk in a Healthcare Setting.
27. Boddy et al., A Study into Data Analysis and Visualisation to increase the CyberResilience of Healthcare Infrastructures.
28. Akinsanya, Papadaki & Sun. Current Cybersecurity Maturity Models: How Effective in Healthcare Cloud?.
29. See note 27 above.

30. Sittig & Singh. "A Socio-technical Approach to Preventing, Mitigating, and Recovering from Ransomware Attacks."
31. Reagin & Gentry. "Enterprise Cybersecurity: Building a Successful Defense Program."
32. Safavi et al., Cyber Vulnerabilities on Smart Healthcare, Review and Solutions.
33. Carlton, Development of a Cybersecurity Skills Index: A Scenarios-Based Hands on Measure of Non-IT Professionals Cybersecurity Skills 2016.; NSW Dept of Industry. NSW-cyber-security-industry-development-strategy 2018.
34. Chen et al., "Blockchain-Based Medical Records Secure Storage and Medical Service Framework."
35. Wilson & Khansa. "Migrating to electronic health record systems: A comparative study between the United States and the United Kingdom."
36. Zaidan et al., "A Security Framework for Nationwide Health Information Exchange based on Telehealth Strategy."
37. Nippon Telegraph and Telephone (NTT) Security. Global Threat Intelligence Report 2019.
38. Dogaru & Dumitrache, Cyber Security in Healthcare Networks. Conference Proceedings of the 6th IEEE International Conference on E-Health and Bioengineering – EHB 2017.
39. Chaudhry et al., POStCODE Middleware for Post-market Surveillance of Medical Devices for Cyber Security in Medical and Healthcare Sector in Australia.
40. See note 5 above.
41. Zhou et al., "The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved."
42. Raber, McCarthy & Yeh. "Health Insurance and Mobile Health Devices: Opportunities and Concerns. JAMA."
43. Almohri et al., On Threat Modeling and Mitigation of Medical Cyber-Physical Systems.
44. See note 27 above.
45. Zheng et al., From WannaCry to WannaDie: Security trade-offs and design for implantable medical devices.
46. Camara, Peris-Lopez & Tapiador, "Security and privacy issues in implantable medical devices: A comprehensive survey."
47. Stern, "A life cycle approach to medical device cybersecurity."
48. Rubenfire, "The nightmare scenario: dialing devices to deadly."
49. See note 22 above.
50. See note 39 above.
51. See note 47 above.
52. Smigielski, "Hardening Infusion Pump Communication Software for Medical Device Cybersecurity."
53. See note 39 above.
54. O"Dowd, "NHS patient data security is to be tightened after cyberattack."
55. Jayaratne et al., "A data integration platform for patient-centered e-healthcare and clinical decision support."
56. See note 35 above.
57. See note 43 above.
58. Holdsworth, Glisson & Choo. "Medical device vulnerability mitigation effort gap analysis taxonomy."
59. Siddique et al., A survey of big data security solutions in healthcare.
60. Shenoy & Appel, "Safeguarding Confidentiality in Electronic Health Records."
61. Wirth, "Cyberinsights. The Times They Are a-Changin": Part One."
62. Baranchuk et al., "Cybersecurity for Cardiac Implantable Electronic Devices: What Should You Know?".
63. Blanke & McGrady. "When it comes to securing patient health information from breaches, your best medicine is a dose of prevention: A cybersecurity risk assessment checklist."
64. Coventry & Branley. "Cybersecurity in healthcare: A narrative review of trends, threats and ways forward."
65. Martin et al., "Cybersecurity and healthcare: How safe are we?".
66. See note 16 above.
67. Beeksow, "Reducing Security Risk using data loss prevention technology."
68. Kruse, Smith & Vanderlinden and A. Nealand. Security Techniques for the Electronic Health Records.
69. See note 11 above.
70. Lee, Moon & Park. CloudRPS: a cloud analysis based enhanced ransomware prevention system.; Abrar et al., "Risk Analysis of Cloud Sourcing in Healthcare and Public Health Industry."
71. Sahi, Lai & Li. "Security and privacy preserving approaches in the eHealth clouds with disaster recovery plan."
72. Sajid & Abbas. "Data Privacy in Cloud-assisted Healthcare Systems: State of the Art and Future Challenges."
73. See note 71 above.
74. Rosenfeld, Torous & Vahia. "Data Security and Privacy in Apps for Dementia: An Analysis of Existing Privacy Policies."
75. Kamel Boulos, Giustini & Wheeler. "Instagram and WhatsApp in Health and Healthcare: An Overview."
76. Scott, "WhatsApp in Clinical Practice: A Literature Review."
77. Chan & Leung. "Use of Social Network Sites for Communication Among Health Professionals: Systematic Review."
78. Morris, Scott & Mars. "Security and Other Ethical Concerns of Instant Messaging in Healthcare."

79. Parker et al., "How private is your mental health app data? An empirical study of mental health app privacy policies and practices."
80. Ibid.
81. Huckvale et al., "Unaddressed privacy risks in accredited health and wellness apps: a cross-sectional systematic assessment."; Mense et al., "Analyzing Privacy Risks of mHealth Applications."
82. Thamilarasu & Lakin. "A Security Framework for Mobile Health Applications. Proceedings –5th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)".
83. Grundy et al., Finding Peace of Mind: Navigating the Marketplace of Mental Health Apps, Australian Communications Consumer Action Network, Sydney.
84. Cilliers, "Wearable devices in healthcare: Privacy and information security issues."
85. Al-Muhtadi et al., "Cybersecurity and privacy issues for socially integrated mobile healthcare applications operating in a multi-cloud environment."
86. Spence et al., "Ransomware in Healthcare Facilities: A Harbinger of the future?".
87. Yasnoff, Breach Risk Magnitude: A Quantitative Measure of Database Security.
88. Gordon et al., "Evaluation of a mandatory phishing training program for high-risk employees at a US healthcare system."
89. Klas-CHIME, Whitepaper: How Aligned Are Provider Organizations with the Health Industry Cybersecurity Practices (HICP) Guidelines?.
90. Fernandez-Aleman
91. King et al., "Characterizing and Measuring Maliciousness for Cybersecurity Risk Assessment."
92. See note 88 above.
93. Smith, "Malware and Disease: Lessons from Cyber Intelligence for Public Health Surveillance."
94. Magnus, Public Report of the Committee of Inquiry (COI) into the Cyber Attack on SingHealth 10 January 2019.
95. Coventry & Branley. "Cybersecurity in healthcare: A narrative review of trends, threats and ways forward."; Wang, Gao & Zhang. Searchable and revocable multi-data owner attribute-based encryption scheme with hidden policy in cloud storage.; Zhang, Xue & Liu. "Searchable Encryption for Healthcare Clouds: A Survey."; Gardiyawasam Pussewalage & Oleshchuk. "Privacy preserving mechanisms for enforcing security and privacy requirements in E-health solutions."
96. Raisaro et al., "Are privacy-enhancing technologies for genomic data ready for the clinic? A survey of medical experts of the Swiss HIV Cohort Study."
97. Saleem et al., Survey on cybersecurity issues in wireless mesh networks based eHealthcare.
98. Wang & Zhang. Data Division Scheme Based on Homomorphic Encryption in WSNs for Health Care Wireless sensor networks.
99. Dubovitskaya et al., Secure and Trustable Electronic Medical Records Sharing using Blockchain.
100. Akinsanya, Papadaki & Sun. Current Cybersecurity Maturity Models: How Effective in Healthcare Cloud?; Carlton, Development of a Cybersecurity Skills Index: A Scenarios-Based Hands on Measure of Non-IT Professionals Cybersecurity Skills 2016.
101. Esposito et al., "Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy?".
102. Park et al., "Is Blockchain Technology Suitable for Managing Personal Health Records? Mixed-Methods Study to Test Feasibility."
103. See note 99 above.
104. Alonso et al., "Proposing New Blockchain Challenges in eHealth."; Angraal, Krumholz & Schulz. "Blockchain Technology: Applications in Health Care."
105. Firdaus et al., "Root Exploit Detection and Features Optimization: Mobile Device and Blockchain Based Medical Data Management."
106. See note 35 above.
107. See note 10 above.
108. Ponemon Institute, Cost of a Data Breach Report 2019.
109. Verizon, 2019 Data Breach Investigations Report.
110. Connory, 2019 Annual Report. State of cyber security.; Ponemon Institute. Cost of a Data Breach Report 2019.
111. Holdsworth, Glisson & Choo. "Medical device vulnerability mitigation effort gap analysis taxonomy."; Upendra et al., "Operationalizing Medical Device Cybersecurity at a Tertiary Care Medical Center."
112. Terry, "HIPAA BREACH. Secure data & prevent fines."
113. Australian Digital Health Agency, National health security and access framework – NESAF.
114. Akinsanya et al., Current Cybersecurity Maturity Models: How Effective in Healthcare Cloud? Online Proceedings of the 5th Collaborative European Research Conference.
115. Taylor, "An SOS on Cybersecurity: To protect patient data, hospitals beef up risk management programs. Hello, chief security officers and "white hat hackers".
116. Perakslis & Califf. "Employ Cybersecurity Techniques Against the Threat of Medical Misinformation."
117. Papoutsi et al., "Patient and public views about the security and privacy of Electronic Health Records (EHRs) in the UK: results from a mixed methods study."

118. Carter, "Considerations for Genomic Data Privacy and Security when Working in the Cloud."
119. Andriole, "Security of electronic medical information and patient privacy: what you need to know."
120. HIPAA Omnibus Rule 2013 Summary.
121. Yaraghi & Gopal, "The Role of HIPAA Omnibus Rules in Reducing the Frequency of Medical Data Breaches: Insights from an Empirical Study."
122. See note 20 above.
123. See note 30 above.
124. Natsiavas et al., "Comprehensive user requirements engineering methodology for secure and interoperable health data exchange."
125. Pullin, "Cybersecurity: Positive Changes Through Processes and Team Culture."
126. Rajamäki et al. Cybersecurity education and training in hospitals: Proactive resilience educational framework (Prosilience EF).
127. Coventry & Branley. "Cybersecurity in healthcare: A narrative review of trends, threats and ways forward."; Verizon, 2019 Data Breach Investigations Report.; Nippon Telegraph and Telephone (NTT) Security. Global Threat Intelligence Report 2019.
128. Raths, "What to Do If a Breach Happens to You."
129. Ropp & Quammen. "Protecting health data in a troubling time. Understand who and what you're up against."
130. Dameff et al., "Clinical Cybersecurity Training Through Novel High-Fidelity Simulations."
131. See note 5 above.
132. Wickham, M. H. Exploring Data Breaches and Means to Mitigate Future Occurrences in Healthcare Institutions: A Content Analysis.
133. See note 16 above.
134. Gordon, Fairhall and Landman, "Threats to Information Security – Public Health Implications."; Dameff et al., "Clinical Cybersecurity Training Through Novel High-Fidelity Simulations."
135. Sedlack, Understanding Cyber Security Perceptions Related to Information Risk in a Healthcare Setting.
136. See note 12 above.
137. See note 11 above.
138. Zafar, Cybersecurity: Role of behavioral training in healthcare.; Sher et al., "Compliance with Electronic Medical Records Privacy Policy: An Empirical Investigation of Hospital Information Technology Staff."
139. Blythe & Coventry. "Costly but effective: Comparing the factors that influence employee anti-malware behaviours."
140. Gaynor, Omer & Turner. "Teaching EHRs security with simulation for non-technical healthcare managers."
141. Zafar, Cybersecurity: Role of behavioral training in healthcare.
142. Carlton, Development of a Cybersecurity Skills Index: A Scenarios-Based Hands on Measure of Non-IT Professionals Cybersecurity Skills 2016.
143. See note 31 above.
144. See note 30 above.
145. Carlton, Development of a Cybersecurity Skills Index: A Scenarios-Based Hands on Measure of Non-IT Professionals Cybersecurity Skills 2016.
146. Connory, 2019 Annual Report. State of cyber security.
147. Burke et al., Cybersecurity Indexes for eHealth.
148. Pratt, "How cyberattacks can impact physicians."
149. McSweeney, Motivating cybersecurity compliance in critical infrastructure industries: A grounded theory study.
150. Pinskier, Royal Australian College of General Practitioners.
151. Ponemon Institute. Cost of a Data Breach Report 2019.
152. Ibid.
153. See note 146 above.
154. Australian Digital Health Agency (ADHA). Annual Report 2017–18.
155. See note 146 above.
156. Ibid.
157. Health Informatics Society Australia, Healthcare-Cybersecurity-Report_June-2018.
158. Ibid.
159. Department of Health, Framework to guide the secondary use of My Health Record system data.
160. See note 154 above.
161. Garetty et al., "National electronic health record systems as wicked projects the Australian experience."
162. My Health Record Statistics (28 July 2019).
163. My Health Records Act 2012.
164. Office of the Australian Information Commissioner, My Health Record Privacy.
165. Global Digital Health Partnership, Securing Digital Health 2018.; ADHA. About the DH Cyber Security Centre, ADHA.
166. See note 147 above.
167. Canaway et al., "Gathering data for decisions: best practice use of primary care electronic records for research."

168. Zhou, Varadharajan & Gopinath. "A Secure Role-Based Cloud Storage System for Encrypted Patient-Centric Health Records."
169. See note 161 above.
170. Australian Government. 14 November 2018. My Health Records (National Application) Amendment (Extension of Opt-out Period No. 2) Rules 2018.
171. Ogunlana, Countering expansion and organization of terrorism in cyberspace.; Shah, Protecting Australian critical national infrastructure in an era of IT and OT convergence.; Walker-Roberts et al., A Systematic Review of the Availability and Efficacy of Countermeasures to Internal Threats in Healthcare Critical Infrastructure.; Boddy et al., A Study into Data Analysis and Visualisation to increase the CyberResilience of Healthcare Infrastructures.; Rajamäki et al. Cybersecurity education and training in hospitals: Proactive resilience educational framework (Prosilience EF).
172. Global Digital Health Partnership, Securing Digital Health 2018.
173. Farrell, "Medicare Machine – patient details of any Australian for sale on Darknet".
174. Minion, "Leaked ADHA document gives inside look at My Health Record challenges".
175. Phillips, Dove & Knoppers. "Criminal Prohibition of Wrongful Re-Identification: Legal Solution or Minefield for Big-Data?".
176. Asghar & Dali. Averaging Attacks on Bounded Perturbation Algorithms.
177. See note 174 above.
178. ABC News (24 July 2018).
179. Information and Privacy Commission NSW.
180. Information and Privacy Commission NSW, Voluntary Breach Notification.
181. ABC News (30 May 2019).
182. The Victorian Auditor General.
183. Ibid.
184. ABC News (22 February 2019); Houston & Colangelo. "Crime syndicate hacks 15,000 medical files at Cabrini Hospital demands ransom".
185. NSW Dept of Industry.
186. Garetty et al., "National electronic health record systems as wicked projects the Australian experience."; Mendelson, "The European Union General Data Protection Regulation (Eu 2016/679) and the Australian My Health Record Scheme – A Comparative Study of Consent to Data Processing Provisions."; Rumbold & Pierscionek. "The Effect of the General Data Protection Regulation on Medical Research."; Rocher et al., "Estimating the success of re-identifications in incomplete datasets using generative models."
187. See note 159 above.
188. Ibid.
189. Ibid.
190. Arnold & Bonython. "No, its not OK for the government to use your prescription details to recruit you for a study".
191. See note 12 above.
192. See note 119 above.
193. Khan & Latiful Hoque. "Digital Health Data: A Comprehensive Review of Privacy and Security Risks and Some Recommendations."
194. Baillie, Bowden & Meyer. "Threshold capabilities: threshold concepts and knowledge capability linked through variation theory."
195. Stahl et al., "Critical theory as an approach to the ethics of information security."
196. Woodruff, "Fixing My Health Record will take more than Hunt"s promises".
197. See note 159 above.
198. See note 12 above.
199. See note 13 above.
200. Nippon Telegraph and Telephone (NTT) Security, Global Threat Intelligence Report 2019.
201. See note 28 above.
202. See note 43 above.

Disclosure statement

No potential conflict of interest was reported by the authors.

Notes on contributors

K. L. Offner is a clinical nurse educator, currently studying a Master of Public Health and Health Management.

Dr, E. Sitnikova, PhD, BE (Hon), CSSLP, SFHEA is is an award-winning academic and researcher at UNSW Canberra and Adjunct Professor at University of Alabama in Huntsville. She is a global leader in cutting-edge research in Critical Infrastructure protection, focusing on intrusion detection for Supervisory Control and Data Acquisition (SCADA) systems cyber security, cyber-physical systems and Industrial Internet of Things (IIoT). Given the increasing number of cyber-attacks globally, Elena's research explores systems resilience and the use of artificial intelligence in the analytics of abnormal data that may affect critical systems. Her contribution in the field is demonstrated through the recent Spitfire Memorial Defence Fellowship Award. She is one of the first Australians to be certified in CSSLP - Certified Secure Software Lifecycle Professional

Dr, K. Joiner is Group Captain (Ret'd), PhD, MMgmt, MSc, BEng(Aero), CPEng, CPPD, MAIPM, MIEAust and Senior Lecturer Test, Evaluation & Aircraft Systems. He is an Educationally Focussed Academic at The UNSW Canberra Cyber at the Australian Defence Force Academy (ADFA)

Professor **C. R. MacIntyre** ***MBBS (Hons 1), M App Epid, PhD, FRACP, FAFPHM*** is Professor of Global Biosecurity and NHMRC Principal Research Fellow at the Kirby Institute, UNSW Australia, and an adjunct professor at Arizona State University. She is a specialist physician with a masters and PhD in epidemiology. She leads a research program in control and prevention of infectious diseases, spanning epidemiology, risk analysis, vaccinology, bioterrorism, mathematical modelling, public health and clinical trials. She is best known for research in the detailed understanding of the transmission dynamics and prevention of infectious diseases, particularly respiratory pathogens such as influenza, tuberculosis, bioterrorism agents and vaccine-preventable infections. She has led the largest body of research internationally on face masks and respirators in health care workers. She won many career awards including the Sir Henry Wellcome Medal and Prize, from the Association of Military Surgeons of the United States for her work on a risk-priority scoring system for category A bioterrorism agents; and the highest national award in infectious diseases, the Frank Fenner Award for Research in Infectious Diseases. She has also won the CAPHIA Research Team Prize, The Public Health Association of Australia National Immunisation Achievement Award, the Peter Baume Public Health Impact Prize and a Harkness Fellowship. She has over 370 peer reviewed publications and sits on several expert committees and editorial boards including Vaccine, BMJ Open, Global Biosecurity and Epidemiology & Infection. She is currently on the Global Accreditation Board for TEPHINET, the network of global field epidemiology programs. She also has an interest in the ethics of medicine, and specifically in dual-use research of concern and has been on the World Organisation for Animal Health (OIE) committee for developing Guidelines For Responsible Conduct in Veterinary Research Identifying, Assessing and Managing Dual Use Research.

ORCID

E. Sitnikova http://orcid.org/0000-0001-7392-0383
C. R. MacIntyre http://orcid.org/0000-0002-3060-0555

Bibliography

ABC News. (February 22, 2019). Accessed July 26, 2019. https://www.abc.net.au/news/2019-02-22/melbourne-heart-hack-cyber-criminals-my-health-record-risks/10834482/

ABC News. (July 24, 2018) https://www.abc.net.au/news/2018-07-24/digital-health-agency-changes-my-health-record-app-contracts/10026644/

ABC News. (May 30, 2019) https://www.abc.net.au/news/2019-05-30/victorian-hospitals-vulnerable-attack-auditor-general-hack-finds/11162352

Abd-alrazaqa, A., B. M. Bewicka, T. Farraghera, and P. Gardner. "Factors that Affect the Use of Electronic Personal Health Records among Patients: A Systematic Review." *International Journal of Medical Informatics* 126 (2019): 164–175. doi:10.1016/j.ijmedinf.2019.03.014.

Abouzakhar, N. S., A. Jones, and O. Angelopoulou. "Internet of Things Security: A Review of Risks and Threats to Healthcare Sector. Joint 10th IEEE International Conference on Internet of Things, iThings 2017, 13th IEEE International Conference on Green Computing and Communications, GreenCom 2017." *10th IEEE International Conference on Cyber, Physical and Social Computing, CPSCom 2017 and the 3rd IEEE International Conference on Smart Data, Smart Data*. June 21, 2017 - June 23, 2017, Exeter UK.

Abrar, H., S. J. Hussain, J. Chaudhry, K. Saleem, M. A. Orgun, J. Al-Muhtadi, and C. Valli. "Risk Analysis of Cloud Sourcing in Healthcare and Public Health Industry." *IEEE Access* 6 (2018): 9140–9150.

ACHSM university course accreditation guidelines. 2017. https://www.achsm.org.au/Portals/15/documents/education/university-accreditation/ACHSM-university-accreditation-guidelines.pdf

ADHA. "About the DH Cyber Security Centre, ADHA." https://www.digitalhealth.gov.au/about-the-agency/digital-health-cyber-security-centre/about

Ahanger, T. A., and A. Aljumah. "Internet of Things: A Comprehensive Study of Security Issues and Defense Mechanisms." *IEEE Access* 7 (2019): 11020–11028. doi:10.1109/ACCESS.2018.2876939.

Akinsanya, O., M. Papadaki, and L. Sun. "Current Cybersecurity Maturity Models: How Effective in Healthcare Cloud?" *Online Proceedings of the 5th Collaborative European Research Conference (CERC)* March 29-30, 2019. http://ceur-ws.org/Vol-2348/

Almohri, H., L. Cheng, D. Yao, and H. Alemzadeh. "On Threat Modeling and Mitigation of Medical Cyber-Physical Systems." *2017 IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE)*. DOI 10.1109/CHASE.2017.84

Al-Muhtadi, J., B. Shahzad, K. Saleem, W. Jameel, and M. A. Orgun. "Cybersecurity and Privacy Issues for Socially Integrated Mobile Healthcare Applications Operating in a Multi-cloud Environment." *Health Informatics Journal* 25, no. 2 (2019): 315–329. doi:10.1177/1460458217706184.

Alonso, S. G., J. Arambarri, M. Lopez-Coronado, and I. de la Torre Diez. "Proposing New Blockchain Challenges in eHealth." *Journal of Medical Systems* 43, no. 64 (2019). doi:10.1007/s10916-019-1195-7.

Andriole, K. P. "Security of Electronic Medical Information and Patient Privacy: What You Need to Know." *Journal American College of Radiology* 11, no. 12 (2014): 1212–1216. doi:10.1016/j.jacr.2014.09.011.

Angraal, S., H. M. Krumholz, and W. L. Schulz. "Blockchain Technology: Applications in Health Care." *Circulatory & Cardiovasc Qual Outcomes* 10 (2017): e003800. doi:10.1161/CIRCOUTCOMES.117.003800.

Argaw, S. T., N. E. Bempong, B. Eshaya-Chauvin, and A. Flahault. *The State of Research on Cyberattacks against Hospitals and Available Best Practice Recommendations: A Scoping Review*. BMC Medical Informatics and Decision Making 19, 10 (2019). https://doi.org/10.1186/s12911-018-0724-5.

Arnold, B. B., and W. Bonython. 2019. "No, It's Not OK for the Government to Use Your Prescription Details to Recruit You for a Study". *The Conversation*, July 31

Asghar, H. J., and K. Dali. *Averaging Attacks on Bounded Perturbation Algorithms*. Australia: Macquarie University, 2019. February.

Australian Cyber Security Centre (ACSC). 2018. "Joint Report on Publicly Available Hacking Tools. Australian Government Signals Directorate." https://www.cyber.gov.au/sites/default/files/2019-03/u5-joint-product-acsc-release-final.pdf

Australian Digital Health Agency. "National Health Security and Access Framework – NESAF V.4." *Australian Government*. Accessed August 18, 2019. https://www.digitalhealth.gov.au/implementation-resources/ehealth-foundations/EP-1544-2014.

Australian Digital Health Agency (ADHA). "Annual Report 2017–18." *Australian Government*.

Australian Government. 2018. "My Health Records (National Application) Amendment (Extension of Opt-out Period No. 2) Rules 2018." *Federal Register of Legislation*, November 14.

Australian Privacy Act. 1988. https://www.legislation.gov.au/Details/C2019C00241

Baillie, C., J. A. Bowden, and J. H. Meyer. "Threshold Capabilities: Threshold Concepts and Knowledge Capability Linked through Variation Theory." *Higher Education* 65, no. 2 (2012): 227–246. doi:10.1007/s10734-012-9540-5.

Baranchuk, A., M. M. Refaat, K. K. Patton, M. K. Chung, K. Krishnan, V. Kutyifa, G. Upadhyay, J. D. Fisher, and D. R. Lakkireddy. "Cybersecurity for Cardiac Implantable Electronic Devices: What Should You Know?" *Journal of the American College of Cardiology (JACC)* 71, no. 11 (2018): 1284–1288. doi:10.1016/j.jacc.2018.01.023.

BDO USA Healthcare. 2019. "Brace for the Breach - Cyberthreat Insights." https://www.bdo.com/getattachment/630056fa-52ef-48e8-a25c-8e9fcff168a6/attachment.aspx?HC_Cyber-Threats_Insight_2-19_WEB.pdf

Beeksow, J. 2015. "Reducing Security Risk Using Data Loss Prevention Technology." *Healthcare Financial Management*, November, p.108–111.

Blanke, S. J., and E. McGrady. "When It Comes to Securing Patient Health Information from Breaches, Your Best Medicine Is A Dose of Prevention: A Cybersecurity Risk Assessment Checklist." *Journal of Healthcare Risk Management* 36, no. 1 (2016): 14–24. doi:10.1002/jhrm.21230.

Blythe, J. M., and L. Coventry. "Costly but Effective: Comparing the Factors that Influence Employee Anti-malware Behaviours." *Computers in Human Behavior* 87 (2018): 87–97. doi:10.1016/j.chb.2018.05.023.

Boddy, A., W. Hurst, M. Mackay, and A. El Rhalibi. "A Study into Data Analysis and Visualisation to Increase the CyberResilience of Healthcare Infrastructures." *Online Proceedings of the Institute of Managers and Leaders (IML) Conference 'International Conference on Internet of Things and Machine Learning'* October 17-18, 2017. http://iml-conference.org

Boddy, A., W. Hurst, M. Mackay, A. El Rhalibi, T. R. Baker, and C. A. C. Montañez. "An Investigation into Healthcare-data Patterns." *Future Internet* 11, no. 2 (2019): p1–23. doi:10.3390/fi11020030.

Burke, W., T. Oseni, A. Jolfaei, and I. Gondal. "Cybersecurity Indexes for eHealth." *Proceedings - Australasian Computer Science Week Multiconference, ACSW* January 29-31, 2019: 2019. doi:10.1145/3290688.3290721.

Camara, C., P. Peris-Lopez, and J. E. Tapiador. "Security and Privacy Issues in Implantable Medical Devices: A Comprehensive Survey." *Journal of Biomedical Informatics* 55 (2015): 272–289. doi:10.1016/j.jbi.2015.04.007.

Canaway, R., D. I. R. Boyle, J. E. Manski-Nankervis, J. Bell, J. S. Hocking, K. Clarke, M. Clark, J. Gunn, and J. Emery. "Gathering Data for Decisions: Best Practice Use of Primary Care Electronic Records for Research." *Medical Journal of Australia* 210 (2019): S12–S16. doi:10.5694/mja2.50026.

Carlton, M. 2016. *Development of A Cybersecurity Skills Index: A Scenarios-Based Hands on Measure of Non-IT Professionals Cybersecurity Skills*. Doctoral dissertation. Nova Southeastern University. NSU Works, College of Engineering and Computing. (979). https://nsuworks.nova.edu/gscis_etd/979

Carter, A. B. "Considerations for Genomic Data Privacy and Security When Working in the Cloud." *The Journal of Molecular Diagnostics* 21, no. 4 (2019): 542–552. doi:10.1016/j.jmoldx.2018.07.009.

Chan, W. S. Y., and A. Y. M. Leung. "Use of Social Network Sites for Communication among Health Professionals: Systematic Review." *Journal Medical Internet Research* 20, no. 3 (2018): e117. doi:10.2196/jmir.8382.

Chaudhry, J., M. Crowley, P. Roberts, C. Valli, and J. Haass. "POStCODE Middleware for Post-market Surveillance of Medical Devices for Cyber Security in Medical and Healthcare Sector in Australia." *Conference: 2018 12th International Symposium on Medical Information and Communication Technology (ISMICT)*. Sydney, NSW, Australia.

Chen, Y., S. Ding, Z. Xu, H. Zheng, and S. Yang. "Blockchain-Based Medical Records Secure Storage and Medical Service Framework." *Journal Medical Systems* 43, no. 5 (2019). doi:10.1007/s10916-018-1121-4.

Cilliers, L. "Wearable Devices in Healthcare: Privacy and Information Security Issues." *Health Information Management Journal* (Online Access 2019): 1–7. https://doi.org/10.1177/1833358319851684.

Connory, M. 2019 "Annual Report." State of Cyber Security. Security in Depth. https://securityindepth.com.au/

Coventry, L., and D. Branley. "Cybersecurity in Healthcare: A Narrative Review of Trends, Threats and Ways Forward." *Maturitas* 113 (2018): 48–52. doi:10.1016/j.maturitas.2018.04.008.

Dameff, C. J., J. A. Selzer, J. Fisher, J. P. Killeen, and J. L. Tully. "Clinical Cybersecurity Training Through Novel High-Fidelity Simulations." *Journal of Emergency Medicine* 56, no.2 (0736-4679 2019): 233–238. doi:10.1016/j.jemermed.2018.10.029.

Department of Health. Framework to guide the secondary use of My Health Record system data. 2018. "Australian Government." May. https://www1.health.gov.au/internet/main/publishing.nsf/Content/F98C37D22E65A79BCA2582820006F1CF/$File/MHR_2nd_Use_Framework_2018_ACC_AW3.pdf

Department of Industry. "NSW Cyber Security Industry Development Strategy 2018." NSW Government.

Dogaru, D. I., and I. Dumitrache. "Cyber Security in Healthcare Networks." *Conference Proceedings of the 6th IEEE International Conference on E-Health and Bioengineering - EHB* 2017, June 22-24. 978-1-5386-0358-1/17/

Dubovitskaya, A., Z. Xu, S. Ryu, M. Schumacher, and F. Wang. "Secure and Trustable Electronic Medical Records Sharing Using Blockchain." *Proceedings - Annual Symposium proceedings. AMIA Symposium*. 2017, p.650–659. New York, United States.

Esposito, C., A. De Santis, G. Tortora, H. Chang, and -K.-K. R. Choo. "Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy?" *IEEE Cloud Computing* 5, Jan/Feb (2018): 31–37. doi:10.1109/MCC.2018.011791712.

Farrell, P. 2017. "Medicare Machine – Patient Details of Any Australian for Sale on Darknet". *The Guardian*, July 04. https://www.theguardian.com/australia-news/2017/jul/04/the-medicare-machine-patient-details-of-any-australian-for-sale-on-darknet/

Farringer, D. "Cybersecurity Report Identifies Unique Challenges to Tackling Cybersecurity in Health Care." *J. Health & Life Sci. L* 11, no. 1 (2017): 117.

Fernandez-Aleman, J. L., A. Sanchez-Henarejos, A. Toval, A. B. Sanchez-Garcia, I. Hernandez-Hernandez, and L. Fernandez-Luque. Analysis of health professional security behaviors in a real clinical setting: An empirical study. *International Journal of Medical Informatics*. 84 (2015): 454–467.

Firdaus, A., N. B. Anuar, M. F. A. Razak, I. A. B. Hashem, S. Bachok, and A. K. Sangaiah. "Root Exploit Detection and Features Optimization: Mobile Device and Blockchain Based Medical Data Management." *Journal of Medical Systems* 42 (2018): 112. doi:10.1007/s10916-018-0966-x.

Flaumenhaft, Y., and O. Ben-Assuli. "Personal Health Records, Global Policy and Regulation Review." *Health Policy* 122, no. 8 (2018): 815–826. doi:10.1016/j.healthpol.2018.05.002.

Food and Drug Administration (FDA). https://www.fda.gov/medical-devices

Forcepoint Whitepaper. 2018. "Life Support: Eliminating Data Breaches in the Healthcare Sector." https://www.forcepoint.com//whitepapers/

Gardiyawasam Pussewalage, H. S., and V. A. Oleshchuk. "Privacy Preserving Mechanisms for Enforcing Security and Privacy Requirements in E-health Solutions." *International Journal of Information Management* 36 (2016): 1161–1173. doi:10.1016/j.ijinfomgt.2016.07.006.

Garetty, K., I. McLoughlin, A. Dalley, R. Wilson, and P. Yue. "National Electronic Health Record Systems as Wicked Projects the Australian Experience." *Information Polity* 21 (2016): 367–381. doi:10.3233/IP-160389.

Gaynor, M., G. Omer, and J. S. Turner. "Teaching EHRs Security with Simulation for Non-technical Healthcare Managers." *Journal of Healthcare Protection Management* 32, no. 1 (2016): 84–97.

General Data Protection Rule. 2018. https://gdpr-info.eu/

Global Digital Health Partnership. 2018. "Securing Digital Health." https://www.gdhp.org/media-hub/news_feed/gdhp-reports

Gordon, W. J., A. Fairhall, and A. Landman. "Threats to Information Security — Public Health Implications." *The New England Journal of Medicine* 377, no. 8 (2017): 707–709. doi:10.1056/NEJMp1707212.

Gordon, W. J., A. Wright, R. J. Glynn, J. Kadakia, C. Mazzone, E. Leinbach, and A. Landman. "Evaluation of a Mandatory Phishing Training Program for High-risk Employees at a US Healthcare System." *Journal of the American Medical Informatics Association* 26, no. 6 (2019): 547–552. doi:10.1093/jamia/ocz005.

Grundy, Q., L. Parker, M. Raven, D. Gillies, B. Mintzes, J. Jureidini, and L. Bero. *Finding Peace of Mind: Navigating the Marketplace of Mental Health Apps*. Sydney: Australian Communications Consumer Action Network, 2017.

"Health Informatics Society Australia." *Healthcare-Cybersecurity-Report*, June-2018.

HIPAA Omnibus Rule. 2013. "Summary." http://www.hipaasurvivalguide.com/hipaa-omnibus-rule.php

HIPAA Privacy Rule 1996.

Holdsworth, J., W. B. Glisson, and K. K. Choo. "Medical Device Vulnerability Mitigation Effort Gap Analysis Taxonomy." *Smart Health* 12 (2017): 82–98. doi:10.1016/j.smhl.2017.12.001.

Houston, C., and A. Colangelo. 2019. "Crime Syndicate Hacks 15,000 Medical Files at Cabrini Hospital Demands Ransom". *The Age*, February 22. Accessed July 30, 2019. https://www.theage.com.au/national/victoria/crime-syndicate-hacks-15-000-medical-files-at-cabrini-hospital-demands-ransom-20190220-p50z3c.html

Huckvale, K., J. T. Prieto, M. Tilney, P.-J. Benghozi, and J. Car. "Unaddressed Privacy Risks in Accredited Health and Wellness Apps: A Cross-sectional Systematic Assessment." *BMC Medicine* (2015) 13:214. doi:10.1186/s12916-015-0444-y.

Information and Privacy Commission NSW. https://www.ipc.nsw.gov.au/data-breach-guidance

Information and Privacy Commission NSW. Accessed July 27, 2019. https://www.ipc.nsw.gov.au/privacy/voluntary-data-breach-notification/

Institute for Critical Infrastructure Technology (ICIT). 2016. Industry Brief: Hacking Healthcare. https://icitech.org/wp-content/uploads/2016/01/ICIT-Brief-Hacking-Healthcare-IT-in-2016.pdf

IT News. 2015. "Hack linked to attack on US insurer Anthem." June 22. https://www.itnews.com.au/news/opm-hack-linked-to-attack-on-us-insurer-anthem-405514

Jalali, M. S., and J. P. Kaiser. "Cybersecurity in Hospitals: A Systematic, Organizational Perspective." *J Med Internet Res* 20, no. 5, May (2018): e10059. doi:10.2196/10059.

Jalali, M. S., M. Siegel, and S. Madnick. "Decision-making and Biases in Cybersecurity Capability Development: Evidence from a Simulation Game Experiment." *Journal of Strategic Information Systems* 28 (2019): 66–82. doi:10.1016/j.jsis.2018.09.003.

Jayaratne, M., D. Nallaperuma, D. De Silva, D. Alahakoon, B. Devitt, K. E. Webster, and N. Chilamkurti. "A Data Integration Platform for Patient-centered E-healthcare and Clinical Decision Support." *Future Generation Computer Systems* 92 (2019): 996–1008. doi:10.1016/j.future.2018.07.061.

Kamel Boulos, M., D. Giustini, and S. Wheeler. "Instagram and WhatsApp in Health and Healthcare: An Overview." *Future Internet* 8, no. 37 (2016): 37. doi:10.3390/fi8030037.

Khan, S. I., and A. S. L. Hoque. "Digital Health Data: A Comprehensive Review of Privacy and Security Risks and Some Recommendations." *Computer Science Journal of Moldova* 24, no. 71 (2016): 2.

King, Z. M., D. S. Henshel, L. Flora, M. G. Cains, B. Hoffman, Blaine, and C. Sample. "Characterizing and Measuring Maliciousness for Cybersecurity Risk Assessment." *Frontiers in Psychology* 9, no. 39 (2018): p1–19.

Klas-CHIME. 2019. "Whitepaper: How Aligned are Provider Organizations with the Health Industry Cybersecurity Practices (HICP) Guidelines?" *KLAS Research and College of Healthcare Information Management Executives (CHIME)*. www.klasresearch.com/reports

Kruse, C. S., B. Frederick, T. Jacobson, and D. K. Monticone. "Cybersecurity in Healthcare: A Systematic Review of Modern Threats and Trends." *Technology and Health Care* 25 (2017): 1–10. doi:10.3233/THC-161263.

Kruse, C. S., B. Smith, H. Vanderlinden, and A. Nealand. "Security Techniques for the Electronic Health Records." *J Med Syst* 41 (2017): 127. doi:10.1007/s10916-017-0778-4.

Lee, J. K., S. Y. Moon, and J. H. Park. "CloudRPS: A Cloud Analysis Based Enhanced Ransomware Prevention System." *The Journal of Supercomputing* 73, no. 7 (2016): 3065–3084. doi:10.1007/s11227-016-1825-5.

MacIntyre, C. R., T. E. Engells, M. Scotch, D. J. Heslop, A. B. Gumel, G. Poste, X. Chen, et al. "Converging and Emerging Threats to Health Security." *Environment and System Decisions* 38, no. 2 (2018): 198–207. doi:10.1007/s10669-017-9667-0.

Magnus, R. 2019. "Public Report of the Committee of Inquiry (COI) into the Cyber Attack on SingHealth." January 10. https://www.mci.gov.sg/coireport

Martin, G., P. Martin, C. Hankin, A. Darzi, and J. Kinross. "Cybersecurity and Healthcare: How Safe are We?" *BMJ (Online)* 358 (2017): j3179. doi:10.1136/bmj.3179.

McSweeney, K. "Motivating Cybersecurity Compliance in Critical Infrastructure Industries: A Grounded Theory Study." Dissertation Abstracts International Section A: Humanities and Social Sciences, 79. Dissertation Thesis. Capella University, January 2018

Mendelson, D. "The European Union General Data Protection Regulation (Eu 2016/679) and the Australian My Health Record Scheme – A Comparative Study of Consent to Data Processing Provisions." *Journal of Law and Medicine* 26 (2018): 23–38.

Mense, A., A. Steger, M. Sulek, D. Jukic-Sunaric, and A. Meszaros. "Analyzing Privacy Risks of mHealth Applications." *Studies in Health Technology & Informatics* 221 (2016): 41–45.

Minion, L. "MHR Security Concerns Persist - ADHA Issues Amended Contracts for Third Party Apps". Healthcare IT News. Accessed July 26 2019. https://www.healthcareit.com.au/article/my-health-record-security-concerns-persist-adha-issues-amended-contracts-third-party-apps
Minion, L. 2018. "Leaked ADHA Document Gives inside Look at My Health Record Challenges". *Healthcare IT News*, August. https://www.healthcareit.com.au/article/exclusive-leaked-adha-document-gives-inside-look-my-health-record-challenges
Morris, C., R. E. Scott, and M. Mars. "Security and Other Ethical Concerns of Instant Messaging in Healthcare." *Studies in Health Technology & Informatics* 254 (2018): 77–85. doi:10.3233/978-1-61499-914-0-77.
My Health Record Statistics. 2019, July 28. Accessed August 12, 2019. www.myhealthrecord.gov.au
My Health Records Act 2012, No. 63. https://www.legislation.gov.au/Details/C2017C00313
National Audit Office Report. *Investigation: WannaCry Cyber Attack and the NHS*. https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf (2017).
National Institute of Standards and Technology (NIST) Framework. https://www.nist.gov/cyberframework
Natsiavas, P., J. Rasmussen, M. Voss-Knude, K. Votis, L. Coppolino, P. Campegiani, I. Cano, et al. "Comprehensive User Requirements Engineering Methodology for Secure and Interoperable Health Data Exchange." *BMC Medical Informatics & Decision Making* 18, no. 85 (2018). doi:10.1186/s12911-018-0664-0.
Nippon Telegraph and Telephone (NTT) Security. 2019. "Global Threat Intelligence Report." https://www.nttsecurity.com/landing-pages/2019-gtir
NSW Dept of Industry. 2018. "NSW-cyber-security-industry-development-strategy."
O'Dowd, and A. O'Dowd. "NHS Patient Data Security Is to Be Tightened after Cyberattack." *BMJ* 358 (2017): j3412. doi:10.1136/bmj.j3412.
O'Sullivan, D. M., E. O'Sullivan, M. O'Connor, D. Lyons, and J. McManus. "WhatsApp Doc?" *BMJ Innovations* 3 (2017): 238–239. doi:10.1136/bmjinnov-2017-000239.
Office of the Australian Information Commissioner. My Health Record Privacy. (July 19, 2019). https://www.oaic.gov.au/privacy/other-legislation/my-health-record/
Ogunlana, S. O. "Countering Expansion and Organization of Terrorism in Cyberspace." *Dissertation Abstracts International: Section B: The Sciences and Engineering* 80 (2019): 3-B(E).
Papoutsi, C., J. E. Reed, C. Marston, R. Lewis, A. Majeed, and D. Bell. "Patient and Public Views about the Security and Privacy of Electronic Health Records (Ehrs) in the UK: Results from a Mixed Methods Study." *BMC Medical Informatics & Decision Making* 15, no. 86 (2015). doi:10.1186/s12911-015-0202-2.
Park, Y. R., E. Lee, W. Na, S. Park, Y. Lee, and J.-H. Lee. "Is Blockchain Technology Suitable for Managing Personal Health Records? Mixed-Methods Study to Test Feasibility." *Journal Med Internet Research* 21, no. 2 (2019): e12533. doi:10.2196/12533.
Parker, L., V. Halter, T. Karliychuk, and Q. Grundy. "How Private Is Your Mental Health App Data? an Empirical Study of Mental Health App Privacy Policies and Practices." *International Journal of Law & Psychiatry* 64 (2019): 198–204. doi:10.1016/j.ijlp.2019.04.002.
Perakslis, E., and R. M. Califf. "Employ Cybersecurity Techniques against the Threat of Medical Misinformation." *JAMA*. 322: 207. Published online June 14, 2019. https://jamanetwork.com/
Phillips, M., E. S. Dove, and B. M. Knoppers. "Criminal Prohibition of Wrongful Re-Identification: Legal Solution or Minefield for Big-Data?" *Bioethical Inquiry* 14 (2017): 527–539. doi:10.1007/s11673-017-9806-9.
PHIPA http://www.health.gov.on.ca/english/providers/project/priv_legislation/phipa_pipeda_qa.html
Pinskier, N. "Royal Australian College of General Practitioners; Cited by Whigham, N." https://www.news.com.au/technology/online/hacking/health-sector-tops-the-list-as-australians-hit-by-300-data-breaches-since-february/news-story/5e95c47694418ad072bf34d872e22124
PIPEDA http://www.health.gov.on.ca/english/providers/project/priv_legislation/phipa_pipeda_qa.html
Ponemon Institute. Cost of a Data Breach Report. 2019. *IBM Security*. https://www.ibm.com/security/data-breach/2019
Pratt, M. "How Cyberattacks Can Impact Physicians." *Medical Economics* 93, no. 12 (June, 2016): 43–47.
Privacy Amendment (Notifiable Data Breaches) Act 2017, No. 12. https://www.legislation.gov.au/Details/C2017A00012
Pullin, D. W. "Cybersecurity: Positive Changes through Processes and Team Culture." *Frontiers of Health Services Management* 35, no. 1 (2018): 3–12. doi:10.1097/HAP.0000000000000038.
Raber, I., C. P. McCarthy, and R. W. Yeh. "Health Insurance and Mobile Health Devices: Opportunities and Concerns." *Journal of the American Medical Association* 321, no. 18 (2019): 1767–1768. doi:10.1001/jama.2019.3353.
Raisaro, J. L., P. J. McLaren, J. Fellay, M. Cavassini, C. Klersy, and J.-P. Hubaux. "Are Privacy-enhancing Technologies for Genomic Data Ready for the Clinic? A Survey of Medical Experts of the Swiss HIV Cohort Study." *Journal of Biomedical Informatics* 79 (2018): 1–6. doi:10.1016/j.jbi.2017.12.013.
Rajamäki, J., J. Nevmerzhitskaya, and C. Virág. "Cybersecurity Education and Training in Hospitals: Proactive Resilience Educational Framework (Prosilience EF)." *Proceedings - IEEE Global Engineering Education Conference (EDUCON)*, 17-20 April 2018, p.2042–2046. doi:10.1109/EDUCON.2018.8363488
Raths, D. "What to Do if a Breach Happens to You." *Behavioral Healthcare* V0l.36, no. 2 (2016): 45–46.
Reagin, M. J., and M. V. Gentry. "Enterprise Cybersecurity: Building a Successful Defense Program." *American College of Healthcare Executives Journal* 35, no. 1 (2018): 13–22.

Rocher, L., . L., J. M. Hendrickx, and Y. de Montjoye. "Estimating the Success of Re-identifications in Incomplete Datasets Using Generative Models." *Nature Communications* 10, no. 1 (2019). doi:10.1038/s41467-019-10933-3.

Ropp, R., and B. Quammen. "Protecting Health Data in a Troubling Time. Understand Who and What You're up Against." *Health Management Technology* 36, no. 7 (2015): 14–15.

Rosenfeld, L., J. Torous, and I. V. Vahia. "Data Security and Privacy in Apps for Dementia: An Analysis of Existing Privacy Policies." *American Journal Geriatric Psychiatry* 25, no. 8 (2017): 873–877. doi:10.1016/j.jagp.2017.04.009.

Rubenfire, A. "The Nightmare Scenario: Dialing Devices to Deadly." *Modern Healthcare* 47 (2017): 4.

Rumbold, J. M. M., and B. Pierscionek. "The Effect of the General Data Protection Regulation on Medical Research." *Journal of Medical Internet Research* 19, no. 2 (2017): e47. doi:10.2196/jmir.7108.

Safavi, S., A. M. Meer, E. K. J. Melanie, and Z. Shakur. "Cyber Vulnerabilities on Smart Healthcare, Review and Solutions." *Online Proceedings Cyber Resilience Conference (CRC)*. 2018 November 15- 18. doi:10.1109/CR.2018.8626826

Sahi, A., D. Lai, and Y. Li. "Security and Privacy Preserving Approaches in the eHealth Clouds with Disaster Recovery Plan." *Computers in Biology and Medicine* 78 (2016): 1–8. doi:10.1016/j.compbiomed.2016.09.003.

Sajid, A., and H. Abbas. "Data Privacy in Cloud-assisted Healthcare Systems: State of the Art and Future Challenges." *Journal of Medical Systems* 40, no. 155 (2016). doi:10.1007/s10916-016-0509-2.

Saleem, K., K. Zeb, A. Derhab, H. Abbas, J. Al-Muhtadi, M. A. Orgun, and Gawanmeh. "Survey on Cybersecurity Issues in Wireless Mesh Networks Based eHealthcare." *Proceedings - 18th IEEE International Conference on e-Health Networking, Applications and Services, Healthcom*, September 14-16, 2016. DOI: 10.1109/HealthCom.2016.7749423

Schwartz, S., A. Ross, S. Carmody, P. Chase, S. C. Coley, J. Connolly, C. Petrozzino, and M. Zuk. "The Evolving State of Medical Device Cybersecurity." *Biomedical Instrumentation and Technology* 52, no. 2 (2018): 103–110. doi:10.2345/0899-8205-52.2.103.

Scott, R. E. "WhatsApp in Clinical Practice: A Literature Review." *Studies in Health Technology and Informatics* 231 (2016): p 82–90. http://ovidsp.ovid.com/ovidweb.cgi?T=JS&CSC=Y&NEWS=N&PAGE=fulltext&D=emexa&AN=621263287.

Sedlack, D. J. "Understanding Cyber Security Perceptions Related to Information Risk in a Healthcare Setting." *Conference Proceedings: Cyber Security Strategy in Healthcare*. Twenty-second Americas Conference on Information Systems, San Diego, California, USA, 2016.

Shah, R. "Protecting Australian Critical National Infrastructure in an Era of IT and OT Convergence." Policy Brief Report No. 18/2019.

Shenoy, A., and J. M. Appel. "Safeguarding Confidentiality in Electronic Health Records." *Cambridge Quarterly of Healthcare Ethics* 26, no. 2 (2017): 337–341. doi:10.1017/S0963180116000931.

Sher, M. L., P. C. Talley, C.-W. Yang, and K.-M. Kuo. "Compliance with Electronic Medical Records Privacy Policy: An Empirical Investigation of Hospital Information Technology Staff." *INQUIRY: The Journal of Health Care Organization, Provision, and Financing* 54 (2017): 1–12.

Siddique, M., M. A. Mirza, M. Ahmad, J. Chaudhry, and R. Islam. "A Survey of Big Data Security Solutions in Healthcare." *14th International EAI Conference on Security and Privacy in Communication Networks, (SecureComm)* August 8-10, 2018. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST, 255, p.391–406. Doi: 10.1007/978-3-030-01704-0_21

Sittig, D. F., and H. Singh. "A Socio-technical Approach to Preventing, Mitigating, and Recovering from Ransomware Attacks." *Appl Clin Inform* 7 (2016): 624–632. doi:10.4338/ACI-2016-04-SOA-0064.

Small, S., D. Peddie, C. Ackerley, C. M. Hohl, and E. Balka. "Patient Perceptions about Data Sharing & Privacy: Insights from Action." In *Context Sensitive Health Informatics: Redesigning Healthcare Work*, C. Nøhr, C.E. Kuziemsky, Z.S.-Y. Wong edited by. 2017, p.109–116. IOS Press: Amsterdam, Netherlands.

Smigielski, R. "Hardening Infusion Pump Communication Software for Medical Device Cybersecurity." *Biomedical Instrumentation & Technology* (2017): 46–50. https://search.proquest.com/docview/1967813395?accountid=12763.

Smith, F. L. "Malware and Disease: Lessons from Cyber Intelligence for Public Health Surveillance." *Health Security* 14, no. 5 (2016): 305–314. doi:10.1089/hs.2015.0077.

Spence, N., N. Niharika Bhardwaj, D. P. Paul III, and A. Coustasse. "Ransomware in Healthcare Facilities: A Harbinger of the Future?" *Perspectives in Health Information Management, Summer* (2018): 1–22.

Stahl, B. C., N. F. Doherty, M. Shaw, and H. Janicke. "Critical Theory as an Approach to the Ethics of Information Security." *Science and Engineering Ethics* 20, no. 3 (2014): 675–699. doi:10.1007/s11948-013-9496-6.

Stern, G. "A Life Cycle Approach to Medical Device Cybersecurity." *Biomedical Instrumentation and Technology* 52, no. 6 (2018): 464–466. doi:10.2345/0899-8205-52.6.464.

Taylor, M. "An SOS on Cybersecurity: To Protect Patient Data, Hospitals Beef up Risk Management Programs. Hello, Chief Security Officers and 'White Hat Hackers'." *Hospitals & Health Networks* 89, no. 2 (2015): 36–38.

Terry, K. "HIPAA BREACH. Secure Data & Prevent Fines." *Medical Economics* 92, no. 14 (2015): 26–32.

Thakkar, V., and K. Gordon. "Privacy and Policy Implications for Big Data and Health Information Technology for Patients: A Historical and Legal Analysis." *Studies in Health Technology & Informatics* 257 (2019): 413–417. doi:10.3233/978-1-61499-951-5-413.

Thamilarasu, G., and C. Lakin. "A Security Framework for Mobile Health Applications. *Proceedings –5th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)*". 2017, p.221–226. DOI 10.1109/W-FiCloud.2017.35

UK Data Protection Act 2018 ico.org.uk. 2018-07-20
Upendra, P., P. Prasad, G. Jones, and H. Fortune. "Operationalizing Medical Device Cybersecurity at a Tertiary Care Medical Center." *Biomedical Instrumentation & Technology* 49, no. 4 (2019): 251–258. doi:10.2345/0899-8205-49.4.251.
"Verizon 2019 Data Breach Investigations Report." Verizon Enterprise Solutions. https://enterprise.verizon.com/resources/reports/dbir/
The Victorian Auditor General, Andrew Greaves. https://www.theguardian.com/australia-news/2019/may/29/victorias-patient-data-vulnerable-to-cyber-attacks-says-audit/.
Victorian Auditor General's Office. 2019. "Independent Assurance Report to Parliament 2018–19." May 23.
Walker-Roberts, S., M. Hammoudeh, and A. Dehghantanha. "A Systematic Review of the Availability and Efficacy of Countermeasures to Internal Threats in Healthcare Critical Infrastructure, 2018." *IEEE Access*. doi:10.1109/ACCESS.2018.2817560i.
Wang, S., R. Gao, and Y. Zhang. "Searchable and Revocable Multi-data Owner Attribute-based Encryption Scheme with Hidden Policy in Cloud Storage." *PLoS ONE [Electronic Resource]* 13, no.11 (pone 2018): 0206126. doi:10.1371/journal.
Wang, X., and Z. Zhang. "Data Division Scheme Based on Homomorphic Encryption in WSNs for Health Care Wireless Sensor Networks." *Journal of Medical Systems* 39, no. 12 (2015): 1–7. doi:10.1007/s10916-015-0340-1.
Wickham, M. H. "Exploring Data Breaches and Means to Mitigate Future Occurrences in Healthcare Institutions: A Content Analysis." *Dissertation Northcentral University, San Diego*, School of Business and Technology Management, April 2019.
Wilson, K., and L. Khansa. "Migrating to Electronic Health Record Systems: A Comparative Study between the United States and the United Kingdom." *Health Policy* 122, no. 11 (2018): 1232–1239. doi:10.1016/j.healthpol.2018.08.013.
Wirth, A. "Cyberinsights. Hardly Ever a Dull Moment: The Ongoing Cyberthreats of 2017." *Biomedical Instrumentation & Technology* 51, no. 5 (2017): 431–443. doi:10.2345/0899-8205-51.5.431.
Wirth, A. "Cyberinsights. The Times They are a-Changin': Part One." *Biomedical Instrumentation & Technology* 52, no. 2 (2018): 148–152.
Woodruff, T. 2018. "Fixing My Health Record Will Take More than Hunt's Promises". Crikey INQ, August 02. https://www.crikey.com.au/2018/08/02/fixing-my-health-record-will-take-more-than-hunts-promises/
Wright, A., S. Aaron, and D. W. Bates. "The Big Phish: Cyberattacks Against U.S. Healthcare Systems." *Journal of General Internal Medicine* 31, no. 10 (2016): 1115–1118. doi:10.1007/s11606-016-3741-z.
Yaraghi, N. I., and R. A. Gopal. "The Role of HIPAA Omnibus Rules in Reducing the Frequency of Medical Data Breaches: Insights from an Empirical Study." *Milbank Quarterly* 96 (2018): 144–166. doi:10.1111/1468-0009.12314.
Yasnoff, W. A. "Breach Risk Magnitude: A Quantitative Measure of Database Security." *AMIA 2016 Annual Symposium Proceedings/AMIA Symposium*, 2017, (2016): p. 1258–1263.
Zafar, H. "Cybersecurity: Role of Behavioral Training in Healthcare." *Proceedings - 22nd Americas Conference on Information Systems: Surfing the IT Innovation Wave*, AMCIS 2016, August 11-14. San Diego, California, USA.
Zaidan, B. B., A. Haiqi, A. A. Zaidan, M. Abdulnabi, M. L. Kiah, and H. Muzamel. "A Security Framework for Nationwide Health Information Exchange Based on Telehealth Strategy." *Journal of Medical Systems* 39 (2015): 5. doi:10.1007/s10916-015-0235-1.
Zeb, K., K. Saleem, J. Al Muhtadi, and C. Theummeler. "U-prove Based Security Framework for Mobile Device Authentication in eHealth Networks." *2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom)*. DOI: 10.1109/HealthCom.2016.7749518
Zhang, R., R. Xue, and L. Liu. "Searchable Encryption for Healthcare Clouds: A Survey." *IEEE Transactions on Services Computing* 11, no. 6 (2018): 978–996. doi:10.1109/TSC.2017.2762296.
Zheng, G., G. Zhang, W. Yang, C. Valli, R. Shankaran, and M. A. OrguA. "From WannaCry to WannaDie: Security Trade-offs and Design for Implantable Medical Devices." *Proceedings - 17th International Symposium on Communications and Information Technologies (ISCIT)*, September 25-27, 2017. DOI: 10.1109/ISCIT.2017.8261228
Zhou, L., V. Varadharajan, and K. Gopinath. "A Secure Role-Based Cloud Storage System for Encrypted Patient-Centric Health Records." *Computer Society Journal* 59, no. 11 (2016): 1159–1611.
Zhou, W., Y. Jia, A. Peng, Y. Zhang, and P. Liu. "The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges yet to Be Solved." *IEEE Internet of Things Journal* 6, no. 2 (2019): 1606–1616. doi:10.1109/JIOT.2018.2847733.