IBIMA Publishing
Journal of e-health Management
https://ibimapublishing.com/articles/JEHM/2020/557564/
Vol. 2020 (2020), Article ID 557564, 12 pages, ISSN: 2165-9478
DOI: 10.5171/2020.557564

Research Article

A Comparative Study of Security and Privacy in Electronic Health Records

Jayakrishna NAIR[1], Moneer ALSHAIKH[2] and Christopher CULNANE[3]

[1,3]University of Melbourne, Melbourne, Australia
[2]University of Jeddah, Jeddah, Saudi Arabia

Correspondence should be addressed to: Jayakrishna NAIR; jnair@student.unimelb.edu.au

Received date: 18 March 2020; Accepted date: 26 July 2020; published date: 15 September 2020

Academic Editor: Afra I. ALAQEEL

Abstract

Electronic health records (EHR) systems can provide doctors and other healthcare professionals with a greater access to the patient's information in a timely manner. Researchers will also have more complete and higher quality data to improve diagnosis and treatments. However, people have genuine privacy concerns that their data might be leaked and thus eroding their trust in the health system. Trust is at the core of privacy and therefore, this paper examines the security measures that are implemented in three countries, namely Denmark, England and Australia, to protect their EHR systems. To identify the countermeasures related to the technologies, policies and human factors that are implemented in the three countries, an in-depth analysis of literature (including an official documentation of EHR in the three countries) was performed. This paper finds that it is important to adopt a more holistic approach where strong policies and practices are implemented, and cyber security awareness and trainings are provided to the users of the system. Adopting this approach can reduce any human related incidents as well as mitigate the concerns surrounding security and privacy.

Keywords: Electronic Health Record, Information Security, Privacy, Information Security Management, Security awareness.

Introduction

Over the last decade, there has been a global push for the use of electronic health records (Kanwal, Lonie and Sinnot, 2018). There are many benefits of having an EHR. A study has found that EHRs can improve the quality of care, reduce medical errors as well as improve the financial and operational performance (Menachemi and Collum, 2011). From a research standpoint, EHRs can allow researchers to access more

____

Cite this Article as: Jayakrishna NAIR, Moneer ALSHAIKH and Christopher CULNANE (2020)," A Comparative Study of Security and Privacy in Electronic Health Records", Journal of e-health Management, Vol. 2020 (2020), Article ID 557564, DOI:10.5171/2020.557564

quality data and use data linkage to help them produce more accurate results for their research. For example, data linkage has enabled researchers to compare hospital caseloads with the outcomes of oesophagogastric cancer surgery (Smith, et al. 2014).

Although EHRs provide several benefits, it also raise several challenges in implementing such a system. Most of these challenges are in the area of privacy, confidentiality and data security. These challenges become of a significant concern when EHRs are shared across healthcare professionals, researchers and other interested parties. A leak in the identity of a patient can lead to discrimination or embarrassment. If these fears manifest in the public, people may feel reluctant to disclose their symptoms or even visit their doctors.

Many countries have implemented various forms of EHRs. However, this study will only be focusing on Denmark, England and Australia. Denmark had been selected because of its high adoption rates of its EHR system; sundhed.dk, with more than 2.4 million unique users each month (OECD, 2019). In contrast to Denmark, England was selected for this study because it had not been so successful in this matter. It uses Summary Care Records (SCR) to manage their patients' data and later implemented care.data which failed only few months after it was released to the public (Godlee, 2016). Australia has had a centralised electronic health record system, Personally Controlled Electronic Health Record (PCEHR), since 2012. PCEHR is now known as My Health Record (MHR), and since February 2019, 9 out 10 Australians have MHR accounts (Australian Digital Health Agency, 2019). Australia was selected because its MHR was not as widely used as sundhed.dk, but it also did not fail as care.data did. Thus, this research aims to provide a comparative study of the security measures across Denmark's sundhed.dk, England's SCR/care.data and Australia's MHR.

Methods

To best compare the security measures in place across the three countries, the McCumber cube will be used to evaluate the information security (McCumber, 2004). The cube has three dimensions: data states, security goals and security measures. This research will only be focusing on the security measures dimension.

One aspect of this dimension is the technological solutions. The underlying technology plays an important role as it helps in setting the foundations for the security measures to be built upon. The cube also highlights the importance to consider the human element that is involved in the security measures. Thus, the paper will also examine the policies and human factors that surround the use of EHRs.

The literature review was conducted in four steps. First, the University of Melbourne's digital library was utilized to collect and screen the academic journals based on filters detailed in Table 1. Second, articles that did not focus on electronic health records were omitted. Finally, the articles based on the three factors of security measures were grouped. This paper will apply these three areas of the countermeasures as a criterion to compare the security measures of the different EHR systems across Denmark, England and Australia.

Table 1: Research steps

Step	Actions performed	Results
1	Broad search in University of Melbourne's digital library. **Keywords:** *privacy in electronic health records, privacy in Sudhed.dk, privacy in Summary Care Records, privacy in My Health Records* **Year since:** 2009 **Language:** English	Articles found: **2,565**
2	Omit those that didn't focus on the technology, policy or the human factors element of cyber security	Articles selected: **45**
3	Select documents based on abstract relevance and years since published	Articles selected: **20**
4	Group the articles based on technology, policy and human factors	

Technology

The first security measure that is often proposed is information security technologies. These technologies are IT components, both hardware and software, that are used as security controls to enforce a particular security requirement (McCumber, 2004). Although it has been argued that information technology alone should not be relied upon, it is still an important element of security that must be maintained to improve an entity's security posture (Blakley, McDermott and Geer, 2001). In this section, the authors will identify the different technologies employed by each of the countries and examine their effectiveness.

Denmark

Sundhed.dk is an online public health portal that provides healthcare professionals and the citizens of Denmark with a single point of access to the electronic health records and other information surrounding the health services provided in Denmark. Citizens can log into this portal to view their own patients' summaries, book appointments electronically, request renewal of medications and view discharge summaries and laboratory results. Healthcare professionals can also use this portal to view their patients' health records and laboratory results.

A secure communication in this network of electronic health services is achieved through the Danish National Health Data Network that was established by MedCom, a publicly funded non-profit organisation. This network is a secure infrastructure that provides both public and private organisations with the means to securely transmit and exchange health data, images, as well communication with external systems such as Sundhed.dk.

To authenticate the access to the electronic health systems and secure the interactions between systems, the public-key infrastructure (PKI) is employed. From 2010, NemIDs were used to further improve the ease of access to the system. NemIDs is a six-digit security number that can be read from a paper or an electronic token which is also used for authentication in banks and other public Danish agencies. This essentially serves as a form of a multi-factor authentication to authenticate the user accessing the portal. In 2017, there were a total of 4.7 million Danish citizens that had NemIDs (Agency for Digitisation, 2017). Therefore, at that time, almost 5 million Danish citizens could have logged into the Sundhed.dk portal.

Patients can monitor the log files where all activities are recorded and report any discrepancies. A letter is sent to the patient if a healthcare professional, who does not have any direct treatment relationship with the patient, has accessed the patient's record. The patients also can prevent any healthcare professionals from accessing certain information such as medical conditions and current medications.

England

SCR is one of the services provided by NHS Digital. It is an EHR system that contains patients' information created from GP medical records. A patient's data can be viewed by health care professionals in other areas of the healthcare system who are directly involved in the patient's care. In contrast to Denmark and Australia, there is no portal for the patient to access this data in England. However, the patient can request to view or add information to the SCR by visiting their GP.

The SCR has three controls in place to control the access to its information. The first is through authentication and Role Based Access Control. This is achieved through smartcards that are used in combination with the user's passwords, hence providing a multi factor authentication. The second control is through Legitimate Relationships. This requires the healthcare professional to have a legitimate reason to view the patient's SCR. The third control requires patients' consent to be obtained before their SCR is viewed. Legitimate relationships and consent are recorded by a member of the staff. However, selecting an emergency access or self-claiming a legitimate relationship will produce an alert. These alerts will be audited by the organisation's privacy officer to ensure that the access to the SCR was valid.

Information on the SCR is recorded in a national database, The Spine. Although the Spine is a national database, it is not integrated into a single system and therefore is not linked to the EHRs obtained through the hospital systems. In 2013, the care.data programme was announced which would link patients' data from GPs with data obtained through hospitals and other healthcare organisations. This program had faced a lot of criticism since its launch and was eventually abandoned in 2016 (Saleem, 2009).

Australia

The PCEHR system is a distributed system that provides numerous repositories for essential services. A registered repository must inform an indexing service of the existence of patients' data available for retrieval upon request. This essentially interrogates the system to see if there are any atomic data, which is the tiniest level of details. This differs from other EHR systems where they act more like a central repository. Only the data sent to the repositories are used by the MHR system. EHRs are never queried directly. Users of MHR can create patients' health summaries and health notes. This includes both the healthcare providers and the patients.

For an organisation to use MHR, it needs a Healthcare Provider Identifier-Organisation (HPI-O) and a National Authentication Service for Health (NASH) PKI certificate. These certificates use a secure hash algorithm (SHA) technology to send secure messages online. The Multifactor Authentication can be enabled through the MyGov portal where a code as well as a password are received via a text message then used.

Once a patient is registered in MHR, healthcare providers will have default access to his record if they have had a relationship with this patient before. Documents can be restricted but can be revealed if the healthcare professional possess a limited document access code. Once a healthcare provider has accessed the patient's record, he will be placed on a list. Patients can access this list and remove providers to deny their access. The system logs all access to the patient's records, and it is available to review as an audit log. The audit logs do not provide information on an individual access, but patients can request to see which individuals have accessed their records, and be notified whenever this happens.

Policy and Practices

Information security policies are used to identify valuable information assets, providing governance and strengthening the controls over these assets (Flowerday and Tuyikeze, 2016). Policies in nature are more control oriented. Practices, however, are more individually constructed (Burdon Siganto and Coles-Kemp, 2016). A practice can be viewed as the procedure that helps ensure the policy is followed (McCumber, 2004). Effective policies and practices are required to maintain the security posture. This section will compare between the different policies and practices adopted by the three countries.

Denmark

In 2006, the Danish General Practice Database (DAMD) was established to record patients' prescriptions and clinical data based on their consultations with their GPs. By 2013, all 2,100 general practices were obliged to supply their data to the DAMD (Paulsen, et al. 2012). This database was initially designed to enable quality improvement in general practices, but the Danish Quality Unit of General Practice (DAK-E) later provided the Danish Health and Medicine Authority with a permission to conduct research using this data. Statistics Denmark, a government institution, would perform linkages with other data sources using a personal identification number that is assigned to all Danish citizens. In 2014, the National Board of e-Health (NSI) and the Danish data protection agency ruled that this collection of data was illegal and ordered all collection of data to DAMD to be stopped and the data on DAMD to be deleted (Christiansen and Rudkjøbing, 2015).

EHRs from hospitals are available to researchers through the Danish National Patient Registry. However, the use of this data is regulated by the Data Protection Act (DPA) which acts as an extension of the General Data Protection Regulation (GDPR) since Denmark is a part of the European Union. This act covers the legal basis for the use of personal data. Personal data can be considered as any data that identifies an individual (GDPR, 2018).

The use of health data for research also requires a permission to be obtained from the Danish Data Protection Agency. If the linkage between various data sources is required, then a permission from the Danish Health and Medicine Authority is required. This legislation also governs the way EHRs can be transferred amongst healthcare professionals. There is a provision which states that healthcare professionals involved in the patient's episode of care will by default have access to important information. Health data can be collected electronically without patients' consent, but the patient must be informed. Patients' consent is required when confidential information is shared with parties outside of their healthcare.

England

NHS England is responsible for providing health services to the citizens of England. The collection of personal data of its patients and other parties involved in the provision of the healthcare services is governed by England's DPA. When care.data was introduced in 2012, some legislations and policies became even less clear. During this time, the Health and Social Act (HSCA) was passed that included a provision from which the Information Centre would be created. This legislation gave the Information Centre the power to collect, collate and gain access to the medical records of all the patients that have received health services by NHS England, including both hospitals and general practices.

To address concerns on the confidentiality of patients' data, the amendments to the HSCA werre passed through the Care Act in 2014 (Sterckx, et al. 2016). This act contained a provision stating that patients' data can only be released for the provision of the healthcare services, adult social care or the promotion of health. However, the exact boundaries imposed by this act were not clear.

GPs were directed to the Information Commissioner's Office (ICO), for more information on the DPA and the legislation that surround patients' data. According to ICO, HSCA gives NHS England the power to direct the Information Centre to collect certain data from a patient's medical record. It also requires the disclosure of the data and therefore is exempt from the DPA. Since this law in the DPA is exempt, both the GPs and the patient are legally not allowed to prevent the transfer of information into the Information Centre. However, the Secretary of State for Health offered patients an option to not upload their information to this service.

The HSCA also contains a provision that allows all EHRs to be used for purposes other than patients' care, e.g. research. The DPA requires the healthcare professionals to notify the patients of the intended use of their data unless it is impractical to do so. However, it has been pointed out that the DPA can be overruled in this instance as the healthcare professional is obliged to transfer such information to the Information Centre, and the Information Centre is not obliged to notify the patient of the use of their data, once the data has been "anonymised" (Grace and Taylor, 2013).

Australia

The Australian Digital Health Agency (ADHA) acts in accordance with the Australian Privacy Principles which can be found in the Privacy Act (1988). My Health Record Rule and My Health Record Regulation were introduced as an extension of the Privacy Act. These legislations give patients the right to monitor and control the access to their data. However, these legislations are not comprehensive in protecting patients' privacy. The MHR's privacy policy mentions that the privacy controls used to manage the access to patients' information, cannot be applied to the Shared Health Summary if it has been uploaded by the GP. The privacy controls are also no longer effective when the documents have been downloaded from the portal.

Data obtained through the MHR portal can be used for secondary purposes such as research. Patients do have the option to opt out of the secondary use of their data. The data released for secondary use will not be sold and will only be provided to organisations which can prove that they will use the data for the public good. This means that insurance companies will not be able to access the data, and government entities cannot use it to assess the eligibility for benefits. MHR's Secondary Use of Data Governance Board will assess all the applications that request access to this data. The Secondary Use Framework states that this board will ensure that the patient's privacy is protected, and the data made available will be of adequate quality (Department of Health, 2018).

Under the Privacy Act, organisations are required to notify the affected individuals and the Office of the Australian Information Commissioner (OAIC) when a data breach is likely to result in serious threats to individuals whose personal information is involved in the breach. Organisations must also provide suggestions to mitigate the impact. For example, if your credit card details are leaked, the organisation can suggest cancelling your credit card to prevent further unauthorised use of the card. However, the suggestions of a similar nature cannot be provided to patients to reduce the impact if their personal details are leaked. A privacy breach victim cannot also claim for emotional distress or other damages.

Human Factors

Human factors are commonly overlooked when assessing cyber security measures, but they are just as important as they are often the last line of defence. Improving the human factors can enhance the security posture of the individuals and ultimately the organisation (Hadlington, 2018). These factors can include motivation, awareness, belief and behaviour (Shouran, Priyambodo and Ashari, 2019). This section will investigate the human factors that are present in each of the countries in terms of the use of electronic health records.

Denmark

Government and healthcare entities are required to have business continuity and disaster recovery plans in place. This involves identifying potential security threats, analysing the impact it will have on the organisation and the recovery of specific applications and functions. Healthcare providers train their users who operate the Danish Health Data Network and other services. However, there is no cybersecurity training provided to the healthcare professionals or other end users. A report has found that healthcare organisations require their staff to frequently update their passwords which has led to clinicians sharing passwords and not signing out of their computers for others to use (Kierkegaard, 2013). An audit is conducted twice a year on a random sample of log files from the Sundhed.dk portal to identify any discrepancies that may have occurred. With these procedures and practices in place, another study has found that the number of cases abusing the EHR system detected each year is low and only a small portion of cases result in a sentence (Nøhr, et al. 2017).

In Denmark, citizens do not have the option to opt-out of the Sundhed.dk system. However, the data obtained through the Sundhed.dk portal is also not used for research and they do have the right to opt out of research on biological samples.

England

NHS England provides a range of free cyber security training to health care providers including a free Government Communications Headquarters (GCHQ) certified board-level cyber security training. This includes a two-hour briefing session followed by online learning modules that are designed for the board members. NHS England has also partnered with IBM to provide health care organisations with a limited number of free user licenses to their Immersive Labs cyber security eLearning platform. This platform helps cyber security professionals in a healthcare organisation develop their cyber security skills. Between 25th of May 2018 and 31st of December 2018, 683 notifications have been made to the Information Commissioner's Officers (NHS England, 2018).

When NHS England first rolled out its Summary Care Report, it was mandatory for all the users of its services. However, due to the public pressure, NHS England adopted an opt out model. The opt out model was also used for care.data even though there is no legislation that regulates this.

Australia

MHR provides online training modules for healthcare professionals that cover topics such as privacy and security of MHR. MHR has also published a checklist that healthcare organisations must follow to be compliant with the MHR's policies. This includes the requirement to train the staff on how to operate the system and the legal obligations that surround the use of it. Despite these learning modules and checklists, it has been found that only one third of the healthcare organisations implement cyber security awareness and training (Health Informatics Society of Australia, 2018).

In 2012, when MHR was initially known as PCEHR, it adopted an opt-in model. In 2014, after it was rebranded to MHR, it used an opt out model. Between 2012 and 2013, less than 400,000 people were registered in the system (Department of Health and Ageing, 2013). This figure grew significantly to over than 22 million people by April 2019, representing 90.1% of the number of people eligible for Medicare (Australian Digital Health Agency, 2019).

Discussion

Technology

The technology for all the three countries must be robust enough to maintain the confidentiality, integrity and the availability of the data. These three factors are known as the CIA triad, which is a widely used benchmark that assesses the effectiveness of the information system security (Fenrich, 2008). A summary of the security features can be found in Table 2.

Table 2: Summary of Security Features

	Denmark (Sundhed.dk)	**England (SCR)**	**Australia (MHR)**
Multi-Factor Authentication	NemIDs	Smart Cards	Temporary Access Codes
PKI	Yes	Yes	Yes
Who has access?	Healthcare Staff and Citizens	Healthcare Staff	Healthcare Staff and Citizens
Access Controls	Through Sundhed.dk	A visit to the GP	Through My Health Records

All three countries use PKI. This is a system that provides a framework for the encryption and authentication of a user. A common challenge in PKI is authenticating remotely for the first time. However, each country has a system in place to address this challenge. For example, in Australia, only organisations registered through the Healthcare Identifier service can request a public key certificate. Studies have found that using PKI can reduce the complexity of the security systems whilst compartmentalising the security risks (Weise, 2001). The multifactor authentication has also been utilised by all the countries to authenticate all the users of the system.

Assurances need to be made that the integrity of the data is maintained even after the authentication of its users. In both Denmark and Australia, the citizens can access the logs through their portals to see who has accessed and/or modified their information. Moreover, biannual audits are conducted in Denmark by the Data Protection Agency. Since there is no technological solution for patients from England to view the access and modification logs, patients will have to rely on the privacy officers of each healthcare organisation. Since the privacy officer is a member of the organisation, if a user has doubts about the staff's use of their data, it can lead to an erosion of trust in the accuracy of the information presented to the patient.

Availability of data is crucial in EHR systems especially in sensitive situations when someone's life is at risk. The adoption of EHR systems has improved the access to health data by healthcare professionals who are in direct care of patients. All three countries have a distributed system in their implementation of their EHR systems. Research has shown that distributed systems can improve the availability and reliability of the data through the replication of data at several locations (Nadiminti, et al. 2006). One of the differences between Australia's implementation of the EHR system compared to the other two countries is that Australia uses multiple repositories to store its data. This provides a greater administrative flexibility in terms of managing multiple essential services. One of the greatest threats that a distributed system faces is a distributed denial of service.

Policy and Practices

One of the key reasons why care.data had failed relative to the other EHR systems is because it had failed to obtain its social license. The social license can be described as the expectations of a society that exceeds the legal requirements and regulations. One research notes that care.data had failed to obtain the social license in three areas: erosion of public trust in care.data, disruption of the traditional role of a GP and the public's doubts on whether the care.data system can benefit the public good (Carter, et al. 2015). The erosion of trust can be attributed to the legislation that was passed to circumvent the data protection laws. Table 3 summarises the Secondary Use of Patients' Data.

Table 3: Secondary Use of Patients' Data

	Denmark	England	Australia
Programme	DAMD and Danish National Patient Registry	Care.data	MHR
Use of patients' data for research	DAMD abandoned in 2014 but Danish National Patient Registry still operates	Care.data was abandoned in 2016	Yes

Australia's MHR has a similar structure for the secondary use of its data to that of care.data, and therefore faces similar challenges. To address the first challenge on trust as well as to show that this system will be used for the good of the public, MHR has vowed not to sell the data or provide the data to the insurance companies, but they can still provide pharmaceutical companies with the data only if they can prove that they will use the data for a good purpose. Care.data had promised the same assurances, but the new legislations allowed care.data to still sell the data to these companies.

Sundhed.dk did not face this challenge because it does not permit the secondary use of its data. As a result, a survey of a group of Sundhed.dk's users had found that most of the participants had expressed positive attitudes towards the use of this service and half of the participants could see the benefits of combining data from various sources (Karampela, et al. 2018).

Furthermore, Anderson has defined nine principles in his research that will lead to a more effective privacy policy (Anderson, 1996). For the most part, all three countries have policies in place that are compliant to these principles. For example, these countries maintain an access control list and have a responsible officer in charge of maintaining this list. However, these countries' access control lists do not include the people who have access to the health data of many people. This is more of an issue in larger healthcare organisations such as hospitals. Typically, in a hospital, there will be a large number of staff members that can access an even larger number of patients. This is magnified when all the data is connected in a network. In Australia, the MHR system only allows the access controls for healthcare providers who have already accessed the record. In Denmark, all healthcare providers have access to all patients' data by default. For SCR, there is no access control list that a patient can easily configure. However, patients can visit their GPs and choose to seal their data in sealed envelopes and dictate who can access them. Although these countries have role-based access controls in place, they fail to place healthcare providers in a patient-controlled access control list before the healthcare provider has accessed the data.

Human Factors

One study has identified that one of the principal sources of privacy breach is the inappropriate disclosure of data where the data has been exported from an organisation without authorisation (Neame, 2014). In England, an incident in 2009 occurred where one GP downloaded a complete patient database, including the medical histories of 10,000 people, on an unsecured laptop (Savage, 2009). This laptop was then stolen and never retrieved. Incidents like this have also occurred in Denmark and Australia. Cyber security training and awareness are required to reduce such incidents.

All three countries have awareness programs in place. England is the only country that provides tailored cyber security training programs based on the role of the user. This is achieved through a strategic partnership with organisations that provide cyber security services. Australia also provides online learning modules to its users in the area of privacy and security, but the module is only aimed at clinicians such as the GP and nurses, not at other staff members such as the management team of the larger healthcare organisations. All of that combined with the fact that only one third of the healthcare organisations implement cybersecurity awareness and training, 55% of Health Sector data breaches in Australia have occurred due to human errors compared to the average of 35% across all other sectors (Office of the Australian Information Commissioner, 2019). Denmark does not provide any direct cybersecurity training, and as a result, unsafe practices can be found in clinics such as sharing passwords with other staff members.

In terms of the opt in/out models used, all three countries have used different approaches and therefore yielded different results from them as displayed in Table 4. The mandatory approach that Denmark took, has contributed to the high rate of monthly users. It can be argued that this mandatory approach was successful due to the transparency of its legislation regarding data protection. The summary care record and the care.data programme were both initially mandatory, but due to the inadequacy of the legislations and regulations, the public pressure forced NHS England to adopt an opt out model. Australia started with an opt-in model that lets individuals decide on whether they want to participate or not. This model will give individuals a greater control over their personal information. However, this also poses a challenge to register the huge mass of the population. In the first two years, there were less than 400,000 individuals registered to the MHR compared to the 22 million people after the opt-out model was used (McLoughlin, Garrety and Wilson, 2017).

Table 4: Opt in/out method used by each country and its respective number of patients registered to the service.

	Denmark	**England**	**Australia**
Opt in/out	Mandatory	Opt-out	Opt-out
Number of Patients Registered	Total Population (5.8 million)	96% of population (55 million)	90.1% of Population (22 million)

Limitations

This paper was restricted only to the data available from public sources that are in English. There were documents published in Denmark that may have provided meaningful insights but were not included in this paper as they were written in Danish. Furthermore, the healthcare sector is constantly evolving in terms of both technology and legislation. For example, NHS England are rolling out a new strategy that will enable patients to view their own data through a portal like Denmark and Australia (NHS England, 2019). Since these are proposed projects, they are not included in this research.

This paper only examined the security measures in place for Denmark, England and Australia. However, there are many more countries that have implemented their EHR systems with varying levels of success. Further research is needed to examine the security measures adopted in these countries and their relative success in protecting the patients' data.

Conclusion

All three countries utilise secure technologies such as PKI and multifactor authentication to ensure that the EHR systems can protect the patient's data. However, from the results, it is apparent that strong policies and practices as well as cyber security awareness and training are equally important to keep the patient's data protected. Weak policies and practices allowed government entities in England to sell patients' data to insurance companies without their consent. The lack of cyber security awareness and skill has also contributed to higher rates of data breaches.

At the core of a successful implementation of a shared EHR system is the trust and support of its users. Whether it is a mandatory, opt-out or opt-in model. If there is no trust in the system, people will opt out or force the abandonment of the project like what happened to care.data. To combat against this, it is vital that governments pay greater attention to the development of security policies and human factors to strengthen its cyber security measures. These policies should not contain ambiguity on the right of access or the ownership of patients' data. Providing more tailored cyber security awareness programs to both organisations and the end users can promote safer security practices. Adopting these approaches can in turn help build the trust from their users and contribute to the success of a shared EHR system.

References

- Agency for Digitisation (2017), *NemID for the future becomes MitID*.
- Anderson, RJ (1996), *Security in clinical information systems*, British Medical Association London.
- Australian Digital Health Agency (2019), *9 out of 10 Australians have a My Health Record*.
  Australian Digital Health Agency (2019), *My Health Record Statistics*.
- Burdon, M, Siganto, J and Coles-Kemp, L (2016), 'The regulatory challenges of Australian information security practice', *Computer Law & Security Review*, vol. 32, no. 4, pp. 623-633.
- Carter, P, Laurie, GT and Dixon-Woods, M (2015), 'The social licence for research: why care. data ran into trouble', *Journal of medical ethics*, vol. 41, no. 5, pp. 404-409.
- Christiansen, T and Rudkjøbing, A (2015), *Deletion of the Danish General Practice Database (DAMD)*.
- Department of Health (2018), *Framework to guide the secondary use of My Health Record system data a*.
- Department of Health and Ageing (2013), *Annual Report*.
- Fenrich, K (2008), 'Securing your control system: the" CIA triad" is a widely used benchmark for evaluating information system security effectiveness', *Power Engineering*, vol. 112, no. 2, pp. 44-49.
- Flowerday, SV and Tuyikeze, T (2016), 'Information security policy development and implementation: The what, how and who', *computers & security*, vol. 61, pp. 169-183.
- General Data Protection Regulation (2018).
- Godlee, F (2016), 'What can we salvage from care.data?', *BMJ*, vol. 354, p. i3907.
- Grace, J and Taylor, MJ (2013), 'Disclosure of confidential patient information and the duty to consult: the role of the Health and Social Care Information Centre', *Medical law review*, vol. 21, no. 3, pp. 415-447.
- Hadlington, L (2018), 'The "human factor" in cybersecurity: Exploring the accidental insider', in *Psychological and behavioral examinations in cyber security*, IGI Global, pp. 46-63.
- Health Informatics Society of Australia (2018), *Cybersecurity across the Australian healthcare sector*.
- Kanwal, S, Lonie, A and Sinnott, R (2018), 'Understanding reproducibility of bioinformatics workflows', *F1000Research*, vol. 7.
- Karampela, M, Grundstrom, C and Isomursu, M (2018), 'Personal Health Data: Access and Perceived Value in Denmark', *Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*, pp. 4081-4084.
- Kierkegaard, P (2013), 'eHealth in Denmark: a case study', *Journal of medical systems*, vol. 37, no. 6, p. 9991.
- McCumber, J (2004), *Assessing and Managing Security Risk in IT Systems: A Structured Methodology*, Auerbach Publications.
- McLoughlin, IP, Garrety, K and Wilson, R (2017), *The digitalization of healthcare: Electronic records and the disruption of moral orders*, Oxford University Press
- Menachemi, N and Collum, TH (2011), 'Benefits and drawbacks of electronic health record systems', *Risk management and healthcare policy*, vol. 4, p. 47.
- Nadiminti, K, De Assunçao, MD and Buyya, R (2006), 'Distributed systems

and recent innovations: Challenges and benefits', *InfoNet Magazine*, vol. 16, no. 3, pp. 1-5.

- Neame, RL (2014), 'Privacy protection in personal health information and shared care records', *Journal of Innovation in Health Informatics*, vol. 21, no. 2, pp. 84-91.
- NHS England (2018), *Notified Incidents Reports 2018.*
- NHS England (2019), *NHS App*.
- Nøhr, C, Parv, L, Kink, P, Cummings, E, Almond, H, Nørgaard, JR and Turner, P (2017), 'Nationwide citizen access to their health data: analysing and comparing experiences in Denmark, Estonia and Australia', *BMC health services research*, vol. 17, no. 1, p. 534.
- OECD (2019), *Health in the 21st Century: Putting Data to Work for Stronger Health System,* OECD Publishing, Paris.
- Office of the Australian Information Commissioner (2019), *Notifiable Data Breaches Scheme 12-month Insights Report*.
- Paulsen, MS, Andersen, M, Thomsen, JL, Schroll, H, Larsen, PV, Lykkegaard, J, Jacobsen, IA, Larsen, ML, Christensen, B and Sondergaard, J (2012), 'Multimorbidity and Blood Pressure Control in 37 651 Hypertensive Patients From D anish G eneral P ractice', *Journal of the American Heart Association*, vol. 2, no. 1, p. e004531.
- Privacy Act (1988).
- Saleem, T (2009), 'Implementation of EHR/EPR in England: a model for developing countries', *Journal of Health informatics in developing countries*, vol. 3, no. 1.
- Savage, M (2009), 'NHS 'loses' thousands of medical records', *Independent*.
- Shouran, Z, Priyambodo, T and Ashari, A (2019), 'Information System Security: Human Aspects', *International journal of scientific & technology research*, vol. 8, no. 03, pp. 111-115.
- Smith, RC, Creighton, N, Lord, RV, Merrett, ND, Keogh, GW, Liauw, WS and Currow, DC (2014), 'Survival, mortality and morbidity outcomes after oesophagogastric cancer surgery in New South Wales, 2001–2008', *Medical Journal of Australia*, vol. 200, no. 7, pp. 408-413.
- Sterckx, S, Rakic, V, Cockbain, J and Borry, P (2016), '"You hoped we would sleep walk into accepting the collection of our data": controversies surrounding the UK care. data scheme and their wider relevance for biomedical research', *Medicine, health care and philosophy*, vol. 19, no. 2, pp. 177-190.
- Weise, J (2001), 'Public key infrastructure overview', *Sun BluePrints OnLine, August*, vol., pp. 1-27.