Quality Evidence, Quality Decisions: Ways to Improve Security and Privacy of EHR Systems

Hamzah Osop
Electrical Engineering and Computer Science
Queensland University of Technology
Brisbane, Australia
hamzah.osop@qut.edu.au

Tony Sahama
Electrical Engineering and Computer Science
Queensland University of Technology
Brisbane, Australia
t.sahama@qut.edu.au

***Abstract*— The readily available and accessible large collection of electronic health records has encouraged an increasing interest on its secondary use. It is especially true for the approach of practice-based evidence where the secondary use of EHR data, collected during routine care, has the potential to improve healthcare professionals' decision-making capabilities and effectiveness, and broadens their knowledge regarding treatments, medications and clinical conditions. Through effective and quality decision-making, healthcare professionals are able to deliver care that positively improves patient health outcomes in a cost-effective and safe manner. However, privacy and security breaches potentially impact the integrity of data captured in electronic health records, and this invalidates its perceived usefulness in providing evidence to support care. In order to design a secure and effective EHR system for the adoption of practice-based evidence approaches, recommendations for privacy and security measures can follow the security control protocol of preventive, detective and corrective control. Within each control, different security solutions are recommended so that security design is truly holistic.**

Keywords—electronic health records, privacy, practice-based evidence, security

I. INTRODUCTION

The healthcare industry benefits from the widespread adoption of information and communication technologies (ICT) within healthcare organizations [1]. As healthcare becomes highly dynamic and complex, characterized by an increasing number of patients with multiple chronic conditions [2], ageing populations and surging healthcare costs, the use of clinical information systems like electronic health record systems (EHRs), have enabled healthcare delivery improvements [3], such as the reduction of medical errors [4, 5]. Coincidentally, the adoption of ICT has resulted in large collections of digital health data or electronic health records (EHR), which itself contain comprehensive and longitudinal patient health and health related information [6].

The data captured in electronic health records, especially those during actual clinical care practice, contain highly rich and valuable practical clinical information that can be used for patient-centered research, improving the overall care of patients and even in helping to manage healthcare costs and expenditure [7]. It has sparked a growing interest amongst healthcare professionals, researchers and academics alike, on the potential secondary uses of EHR for healthcare delivery improvements. One such potential use is in the enablement of the practice-based evidence (PBE) approach. In this approach, EHR from multi-sourced information systems are integrated and analyzed through a series of healthcare analytics. Findings discovered through analytics usually reinforces known knowledge but has potential in uncovering new information which acts as practical clinical evidence for healthcare professionals, helping them in improving their clinical decision-making.

Research has shown that utilizing EHR data can assist with clinical care and decision-making [8-10]. However, known privacy and security issues are concerns that can have a major impact on data integrity, a data quality aspect of EHR. Relying on inaccurate data can adversely affect the quality of care as well as the quality of decision-making, because it can lead healthcare professionals to make clinical and medical errors. As such, this raises the questions of suitability in utilizing EHR for secondary uses and the applicability of PBE approaches for improved decision-making. Most often, answers commonly point towards developing a "secure" information system that can prevent privacy and security breaches. Some recommend measures such as designing a usable system that makes the information system easy to use while having security and privacy measures that prevent errors from occurring [11]. Others suggest the implementation of strict security measures that can safeguard from unauthorized data access and manipulation. However, such measures may not solve the privacy and security concerns as users might not adhere to them or information systems are not equipped to detect and handle a security breach.

Therefore, in this paper, the authors aim to highlight ways to implement privacy and security measures through the three security control measures of preventive, detective and corrective control, offering a holistic approach to the security design of information systems suited for the implementation of a practice-based evidence approach.

II. PRACTICE-BASED EVIDENCE

Practice-based evidence (PBE) is a complementary paradigm to the leading approach in the practice of medicine, evidence-based practice (EBP). Initially, the PBE approach started as an initiative to answer the calls to close the widening gap between what is available from research and what has been

adopted in practice. Barkham and Margison [12] defined the approach of practice-based evidence as the process of integrating both clinical expertise with that of best evidence drawn from research activities carried out in practice settings to make decisions about individual patients. In this approach, Barkham and Mellor-Clark [13] identified the use of practice research networks (PRN) as structures required in the delivery of practice-based evidence. A PRN typically consists of "a large number of clinicians who agree to collaborate, to collect and report data'. A PRN entails collaborating clinicians to collect, share and use data gathered during routine clinical practice as standards and benchmarks to improve the delivery and development of care services [13].

However, the adoption of ICT has enabled the availability and accessibility of rich clinical and medical information stored in electronic health records (EHR). It has therefore allowed for a similar practice-based evidence approach to be implemented. Instead of developing a PRN which may have varying formats, standards and tools used across collaborating healthcare organizations, the authors recommend the use of a more standardized format in electronic health records. Electronic health record systems have made the collection of patients' health and healthcare related information such as medical prescriptions, treatments provided, laboratory test results and clinical diagnoses, easier yet extensive. EHR represents the collection of evidence that can be used to direct and assist healthcare professionals to make better informed decisions. With healthcare becoming more complex and complicated, clinical decision-making becomes an integral aspect in healthcare. Practice-based evidence thus represents an appropriate approach to be adopted, especially in primary care settings. The term 'practice' in practice-based evidence refers to actual clinical practices performed by healthcare professionals in the process of providing care. The term 'evidence' points to the information captured in EHR such as medication prescribed or clinical notes in which the clinical practices have resulted in positive patient health outcomes. Through the use of healthcare analytics, the analysis of EHR data has the potential to uncover new clinical findings that can assist healthcare professionals in making effective decisions.

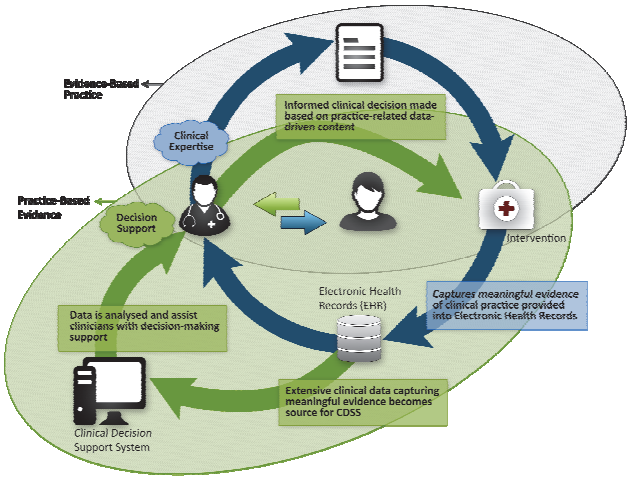

Fig. 1. Practice-based evidence cyclic approach [14].

For example, secondary users of EHR data has led to the improvement of detecting and screening type 2 diabetes [8], improvement in the identification of patients with heart failure [9] and prediction of condition severity of congestive heart failure patients [10].

As such, PBE can be defined as the process where meaningful evidence of clinical practice performed by healthcare professionals as part of their routine practice is captured, into a structured and standardized electronic data format, and used to support and inform clinical decision-making towards the care of individual patients [14]. As illustrated in Figure 1, PBE is represented as a cyclic process where continuous capturing of practical clinical evidence (EHR) further improves the resources and reinforces the evidence upon which clinical decisions can be derived.

Therefore, EHR plays an integral role in the cyclic approach of practice-based evidence in facilitating improved decision-making by healthcare professionals. Equally important is maintaining the quality of EHR data as it influences the overall findings which will be used to help in directing decisions. As such, EHR data quality maintenance requires privacy and security measures to be addressed, and the basic principle of security in information systems to be met.

III. Privacy and Security Concerns For Practice-based Evidence

To protect patients' health information and its privacy, many countries have implemented legislative privacy policies and regulations. In the United States for example, the *HIPAA Privacy Rule*, under the *Health Insurance Portability and Accountability Act (HIPAA)*, establishes national standards which protect patients' medical records and their other personal health information by setting limits and conditions on its uses and disclosures. The Rule also provides the patients their rights to their health information; their rights to have a copy of the records and rights to information corrections [15]. In Australia, the *Privacy Act 1998 (Cth)* regulates how healthcare providers handle patients' health information from its collection, usage and to its disclosure [16]. In Singapore, the *Personal Data Protection Act (PDPA)* provides guidelines for organizations on how to collect, use and disclose personal data including personal health information within the organizations and between external organizations [17]. These legislative policies and regulations have been in place to ensure that personal information, especially personal health information, adheres to requirements that can keep it safe against unscrupulous use. As such, information system such as EHR systems require privacy and security measures in order to meet the legislative requirements set out as to protect patients' private and sensitive information.

So, what exactly is meant by privacy and security? Mackenzie, et al. [18] defined privacy as "the right of an individual to control the circulation of information about him/her within social relationships; freedom from unreasonable interference in an individual's private life; and an individual's right to protection of data regarding him/her against misuse or unjustified publication". Security, on the other hand, is defined as "a series of mechanisms and processes designed to protect

data from inappropriate release". In that sense, privacy and security are intertwined where the need to maintain privacy requires security measures and protocols to be in place, keeping personal information private and confidential, accessible only when the user is authorized.

This need to enforce privacy and security measures arises because privacy and security breaches are major risks when it comes to the use of information systems. Such breaches have a high tendency to pose adverse effects to patient care, be it an accidental or a deliberate one. The success of any healthcare information system hangs on its ability to address and prevent privacy and security breaches. For example, unauthorized access to an individual's personal health information can have negative impacts such as information theft or unauthorized data modification, but a lack of access can also potentially lead to poor decision-making and errors when needed to provide clinical care [19]. Although privacy is very important, security measures have potentially led to patients being prevented from seeking genuine medical help [18]. In such a scenario, privacy concerns have hindered the effective use of eHealth systems and the improvements of health services [19].

Hence, to have a successful adoption of practice-based evidence approach, privacy and security measures have to be holistic, seamless, friendly and easy enough that it does not interfere with use of EHR systems and degrades its usability.

A. Data integrity

The privacy and security of health information is essential for the healthcare industry and hence, necessary measures need to be taken. Information security thus is an approach that strategically addresses these concerns. Information security as defined by the US Code (US Code Title 44, Chapter 35, Subchapter III, § 3542) [20] refers to the process of "protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality and availability". Confidentiality, Integrity and Availability, known as the CIA-triad [21, 22], forms the basic principles of information security. It is a model that is used to denote security and privacy attributes [22] and is the fundamental goals for security [23].

Lebdaoui, et al. [24] on the other hand, employs the CIA-triad as dimensions of data quality, so that effective decisions can be made from EHR data. For the context of PBE, we will also be focusing instead on this integrity aspect. Integrity in information security refers to "guarding against improper information modification or destruction, and includes ensuring information repudiation and authenticity" [20] or data that cannot be modified without authorization [21]. This is especially important as health information needs to be accurate at the time of access in order to make effective decisions [22]. With electronic health records containing comprehensive and longitudinal patient health and health related information such as medication prescriptions, treatments provided, laboratory test results and clinical diagnosis, this information needs to be constantly accurate, correct and updated. This is especially the case when EHR has the potential to discover new findings such as drug-drug interactions, medication recommendations or remains in support of diagnosis and identification of patients at risk of chronic conditions. The modification of EHR data without authorization can lead to data being unreliable and affect the overall effectiveness of decisions made. It may also provide an incorrect summary of patients' actual health conditions or treatments provided if information had been deleted or edited without permission and authority. In the case of PBE, analysis of EHR data to generate new findings becomes unreliable as the data gathered is inaccurate. Applying these findings to treat patients is dangerous and can be detrimental to the patient's health and their doctor's practices.

With the practice-based evidence approach relying on EHR data to provide relevant and reliable evidence to support and improve clinical decision-making, it is crucial that the EHR data is kept accurate and correct.

B. Breaches and controls

There have been many reported cases of privacy and security breaches of EHR systems. These privacy and security breaches can come in several types and forms. Highlighted below are some of the breaches that affect the integrity aspect of data quality and the integrity dimension of the CIA-triad security principle, which are relevant to the successful adoption of PBE.

Security breaches can happen in the form of a physical or technological breach. A physical breach can happen, for example, in the event of a disaster such as a building fire or electrical failures which puts the information systems at risk. If there was a process running during the breach, data might not be captured correctly or information might not be retrieved fully. Hardware devices, software applications, networks and data are usually at risk of being lost or damaged during such events. Technological breaches can occur when unauthorized individuals try to gain access into 'secure systems' to illegally update the data with inaccurate information or delete it from the system. In some cases, hackers infiltrate into databases to steal patient records or remove it from the database, causing severe data integrity issues.

Privacy breaches are typically categorized as either accidental or deliberate breaches. An example of a deliberate breach occurs when a doctor unlawfully re-identifies individuals from an otherwise de-identified or anonymized database for purposes not related to providing healthcare. In some cases, a doctor deliberately exposes sensitive patient information such as mental illness or HIV-positive information for personal gain. An accidental breach can occur when the information system mistakenly reveals identifiable data to the wrong doctor or when doctors accidentally leave patient files and information open for others to view [18].

By understanding these possible privacy and security breach scenarios, we get to understand the weakness of information systems in use and the implications that can arise from it. From there, we are able to design better security controls in order to prepare for and prevent such scenarios happening. Hence a more holistic approach to the design of privacy security measures can be taken when designing an information system, and at the same time, when enabling the

implementation of a practice-based evidence approach that can improve the clinical decision-making and delivery of care.

The design of privacy and security measures can adopt the three different types of security controls; preventive, detective and corrective. This design therefore affords the information system, prevention and protection before, during and after a breach has occurred. Preventive control is a measure taken before the event occurs, preventing an incident from occurring. For example, locking out unauthorized users from accessing the EHR systems would prevent any illegal data modification from occurring. Detective control occurs during the event. When a breach is detected, detective controls are taken to identify and characterize the incident's progress. This can be done by sounding the intruder alarm, alerting the security guards or shutting down the system from further loss. However, when a breach is discovered only after the event has ended, then corrective control measures need to be taken to limit the extent of damage caused by the incident. This can be done by recovering the system or organization to normal working status as efficiently as possible.

IV. Possible Solutions

Understanding the implications arising from privacy and security breaches help design a more secure and usable information system. By adopting the three security control measures of preventive, detective and corrective control as a guide in proposing security and privacy breach solutions, a more holistic solution can be achieved.

A. Preventive control solutions

Preventive control is designed to prevent a breach before it can happen. One of the most common preventive control solutions is password and authentication measures. Authentication measures aim at allowing access to information and data to authorized users only and access differs base on the level of access allocated. Traditionally, authentication measures require users to key in their username and password in a secured log in form.

Password authentication:

Passwords are generally unique to users, providing a level of security where no one else would know their passwords. In order to make passwords less hackable or "crackable", different password formats and structures have been deployed. For example secure passwords should be 8 characters or longer, with a combination of alphabets and numeric, a mix of upper-case and lower-case characters and the use of special characters. Unfortunately, this makes passwords difficult to remember and therefore, users have resorted to using the same password to access other information systems. This practice increases the chances for hackers to gain access to multiple systems using the same password. Therefore to discourage users from using the same password for all their login purposes, new password alternatives have been proposed which can be adopted. Payne and Edwards [25] recommended 6 different and alternative password formats that can be implemented in information systems to improve the password authentication measures.

Passphrase:

The strength of passwords lie in the difficulty for a hacker to guess the password. Therefore, increasing the length or character used in a password would naturally increase the difficulty. As such, passphrase which consists of a series of words which makes a sentence would be much more difficult to hack. Passphrases increases the length of the password without making it difficult to remember or use.

Password: htyai!89

Passphrase: It is easier to use a passphrase than a password.

Pass-algorithms:

Pass-algorithms work on the notion that remembering secure passwords is a problem for users. Therefore, Haskett [26] introduced the password authentication technique called 'pass-algorithms'. For example, an implementation of pass-algorithm can involve the user logging in as per normal using the system's log in procedure. Instead of immediately being granted access after authentication, in pass-algorithm, the user is next prompted with a random generated text. To successfully complete the log in process, the user may be required to respond by typing in the next alphabetic character corresponding to the prompted text. The benefit of this method is that there are many algorithms that can be used to generate the prompt text and expected response, while logging-in location can also be used to determine which proper prompt response to use, hence overall providing multi-level security.

Prompted text: BEL

Response text: CFM

Some other examples of alternative password formats that have been proposed are cognitive passwords, passfaces, graphical passwords and passpoints [25]. While such alternative methods work well for mobile devices, they may not work well for authenticating users for information systems.

Besides using passwords solely to authenticate, additional devices or biometrics can be used. Two factor authentication, biometric authentication and continuous user authentication are some alternative forms of authentication that can improve usability of systems and at the same time, reduce the risk of privacy and security breaches.

Biometric authentication:

Biometric authentication is a system that relies on the unique biological characteristics of individuals to verify for secure access to electronic systems [27]. The best biometric characteristics that can be used for authentication is fingerprints, voice, iris, retina, hand, face, handwriting, keystroke and finger shape. Biometric authentication can be used in place of a name, identification number or other forms of identification as the biometrics, like fingerprint or eye scans, do not reveal any personal information [28]. The main advantages that biometric authentication brings, especially to healthcare, is that it is easy and safe to use, saves time and improves security [29].

Two factor authentication:

Two factor authentication (2FA) is a method where two or more mechanisms are being used together to protect from security or privacy breaches. For example, a 2FA mechanism

can consist of a password or passphrase, a physical device like a key fob or key card, or biometrics like fingerprints or retinal scans [30]. 2FA mechanisms have seen prominent use in online banking services to strengthen security measures. Customers are issued tokens that generate codes needed to confirm payments or execute remittance to other bank accounts. It would then present a much more familiar practice for users and would be easily adopted as an improvement to current authentication methods.

Continuous user authentication:

Traditionally authentication is performed once, when a user provides a password and the identity is verified. This authentication session becomes valid until the user kills the session or logs out from the system. The disadvantage of this authentication method is that the system would not be able to detect if there has been a change in users. A continuous user authentication will instead continuously monitor the system and the user to check if a change of user has occurred. This diminishes the risk of privacy breaches when an unauthenticated user has access to a logged-in system. Unfortunately, continuous user authentication does not work for all types of authentication methods. It is best suited for biometric authentication where facial recognition, fingerprint or keystrokes can be used to continuously authenticate [31].

B. Detective control solutions

Detective controls respond during the occurrence of an event. When a breach is detected, detective control is taken to identify and characterize the incident progress. There are several ways to employ detective controls and the most common would be the use of anti-virus software. However, anti-virus software may not be as effective as the following systems which work best at detecting as well as preventing intrusions and breaches before or while it is happening.

Intrusion Detection System (IDS):

The intrusion detection system is a security system which monitors the network by collecting and checking for unnecessary network packets and inspecting its behaviors. The aim is to detect the occurrence of an unnecessary event and perform security measures to reduce the possibility of an attack [32]. The intrusion detection system is able to provide visibility through the monitoring of traffic on the network. The intrusion detection system comes in two forms, the Network Intrusion Detection System (NIDS) and the Host Intrusion Detection System (HIDS). The difference is that HIDS looks at both the network as well as the systems files for unnecessary processes.

Intrusion Prevention System (IPS):

The intrusion prevention system is a network device which monitors the network to look out for malicious behaviors, in order to prevent attacks before it enters the network. Upon identification of an attack, the intrusion prevention blocks and logs the attacking data [33]. Intrusion prevention systems also come in two forms, network based IPS and host-based IPS. Network-based IPS is usually placed in a strategic location like the gateway to be able to analyze all the network traffic passing through it. Host-based IPS is installed on host systems to protect servers and workstations. It is usually a software that blocks attacks against the host system.

C. Corrective control solutions

When a breach is discovered after the event has ended, then corrective control measures need to be taken to limit the extent of any damage caused by the incident. This can be done by recovering the organization to normal working status as efficiently as possible. In such circumstances, system back-up measures can be adopted.

System back-up measures:

The backup system is defined as a security tool that is designed to provide an easy, simple and comprehensive way to protect data and restore data [34]. Backup systems are necessary because with the huge generation of digital health records, healthcare organizations need the data archiving capabilities to cope with the growing use of information systems. Furthermore, an effective and efficient security of a huge collection of data is often neglected by managers, as the lack of resources and knowledge dictates which are more critical. Therefore system backup allows for information systems to fall back to the latest saved state, ensuring that data captured at that particular point is most accurate.

Therefore, by implementing one of the solutions provided, depending on its suitability and needs, from each security controls will enable an effective design of an information system done with a holistic approach to privacy and security considerations. Besides adhering to the needs of legislative policies and regulations, this design has also the potential to prevent, protect and correct should an event or a breach occurs.

V. CONCLUSION

Demands from patients for effective and efficient care have burdened healthcare professionals with the need to make well-informed clinical decisions. The paradigm of practice-based evidence has emerged as a complementary approach to evidence-based practice, utilizing practical clinical evidence from electronic health records to direct and improve clinical decision-making by healthcare professionals. Effectively, practice-based evidence has the potential to improve patient health outcomes and reduce healthcare expenditure. However, privacy and security breaches pose risks and concerns to the effective implementation and deployment of PBE. One of the three basic principle of information security (CIA-triad), integrity, can potentially derail the adaptation of PBE where EHR data accuracy and correctness becomes questionable. In order to effectively maintain quality EHR data and subsequently implement a successful approach of practice-based evidence, a holistic privacy and security design needs to be implemented. Therefore, the use of the three security control protocols of preventive, detective and corrective controls, becomes a guide to the implementation of an information system that has a holistic security design in place. By addressing the different solutions to each control, EHR system implementation will be better equipped to protect against undesirable attacks and maintain quality EHR data that can be used to benefit patients at large.

REFERENCES

[1] E. Bélanger, G. Bartlett, M. Dawes, C. Rodríguez, and I. Hasson-Gidoni, "Examining the evidence of the impact of health information technology in primary care: An argument for participatory research with health professionals and patients," International journal of medical informatics, vol. 81, pp. 654-661, 2012.

[2] M. E. Salive, "Multimorbidity in older adults," Epidemiologic reviews, vol. 35, pp. 75-83, 2013.

[3] M. B. Buntin, M. F. Burke, M. C. Hoaglin, and D. Blumenthal, "The benefits of health information technology: a review of the recent literature shows predominantly positive results," Health Affairs, vol. 30, pp. 464-471, 2011.

[4] K. M. Cresswell and A. Sheikh, "Health information technology in hospitals: current issues and future trends," Future Hospital Journal, vol. 2, pp. 50-56, 2015.

[5] C. L. Goldzweig, A. Towfigh, M. Maglione, and P. G. Shekelle, "Costs and benefits of health information technology: new trends from the literature," Health Affairs, vol. 28, pp. w282-w293, 2009.

[6] A. Hoerbst and E. Ammenwerth, "Electronic health records," Methods of Information in Medicine, vol. 49, pp. 320-336, 2010.

[7] N. G. Weiskopf and C. Weng, "Methods and dimensions of electronic health record data quality assessment: enabling reuse for clinical research," Journal of the American Medical Informatics Association, vol. 20, pp. 144-151, 2013-01-01 00:00:00 2013.

[8] A. E. Anderson, W. T. Kerr, A. Thames, T. Li, J. Xiao, and M. S. Cohen, "Electronic health record phenotyping improves detection and screening of type 2 diabetes in the general United States population: A cross-sectional, unselected, retrospective study," Journal of Biomedical Informatics, vol. 60, pp. 162-168, 4// 2016.

[9] D. Banerjee, C. Thompson, A. Bingham, C. Kell, J. Duhon, and H. Grossman, "An Electronic Medical Record Report Improves Identification of Hospitalized Patients With Heart Failure," Journal of Cardiac Failure, vol. 22, pp. 402-405, 5// 2016.

[10] C. Sideris, B. Shahbazi, M. Pourhomayoun, N. Alshurafa, and M. Sarrafzadeh, "Using electronic health records to predict severity of condition for congestive heart failure patients," presented at the Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct Publication, Seattle, Washington, 2014.

[11] J. Zhang and M. F. Walji, "TURF: Toward a unified framework of EHR usability," Journal of Biomedical Informatics, vol. 44, pp. 1056-1067, 12// 2011.

[12] M. Barkham and F. Margison, "Practice-based evidence as a complement to evidence-based practice: From dichotomy to chiasmus," in Handbook of evidence-based psychotherapies: A guide for research and practice, C. Freeman and M. Power, Eds., ed: Wiley, 2007, pp. 443-476.

[13] M. Barkham and J. Mellor-Clark, "Rigour and relevance: the role of practice-based evidence in the psychological therapies," Evidence-based mental health. London: Routledge, pp. 127-44, 2000.

[14] H. Osop and T. Sahama, "Data driven and practice-based evidence: Design and development of efficient and effective clinical decision support system," in Improving Health Management through Clinical Decision Support Systems, ed Hershey, PA: IGI Global Publishing, 2015.

[15] U.S. Department of Health & Human Services. (2016, August 2016). Health Information Privacy. Available: http://www.hhs.gov/hipaa/for-professionals/privacy/

[16] Office of the Australian Infotmation Commissioner. (2016, August 2016). Business resource: Handling health information under the Privacy Act: A general overview of health service providers. Available: https://www.oaic.gov.au/engage-with-us/consultations/health-privacy-guidance/business-resource-handling-health-information-under-the-privacy-act-a-general-overview-for-health-service-providers

[17] Personal Data Protection Commission Singapore, "Advisory guidelines for the healthcare sector," ed. Singapore, 2014.

[18] I. S. Mackenzie, B. J. Mantay, P. G. McDonnell, L. Wei, and T. M. MacDonald, "Managing security and privacy concerns over data storage in healthcare research," Pharmacoepidemiology and Drug Safety, vol. 20, pp. 885-893, 2011.

[19] D. Grunwell, P. Batista, S. Campos, and T. Sahama, "Managing and sharing health data through Information Accountability protocols," in 2015 17th International Conference on E-health Networking, Application & Services (HealthCom), 2015, pp. 200-204.

[20] Legal Information Institute. 44 U.S. Code § 3542. Available: https://www.law.cornell.edu/uscode/text/44/3542

[21] H. K. Yau, "Basic Principle of Information Security," Advances in Robotics Automation, vol. 3, 2014.

[22] K. T. Win, "A Review of Security of Electronic Health Records," Health Information Management, vol. 34, pp. 13-18, March 1, 2005 2005.

[23] J. L. Fernández-Alemán, I. C. Señor, P. Á. O. Lozoya, and A. Toval, "Security and privacy in electronic health records: A systematic literature review," Journal of Biomedical Informatics, vol. 46, pp. 541-562, 6// 2013.

[24] I. Lebdaoui, G. Orhanou, and S. El Hajji, "Data Integrity in Real-time Datawarehousing," in World Congress on Engineering 2013, London, UK, 2013.

[25] B. D. Payne and W. K. Edwards, "A Brief Introduction to Usable Security," IEEE Internet Computing, vol. 12, pp. 13-21, 2008.

[26] J. A. Haskett, "Pass-algorithms: a user validation scheme based on knowledge of secret algorithms," Commun. ACM, vol. 27, pp. 777-781, 1984.

[27] M. Rouse. (2016, August 2016). Biometric Authentication. Available: http://searchsecurity.techtarget.com/definition/biometric-authentication

[28] J. Wayman, A. Jain, D. Maltoni, and D. Maio, An introduction to biometric authentication systems: Springer, 2005.

[29] R. Raju. (2016, August 2016). The advantages of a Biometric Identification Management System. Available: http://blog.m2sys.com/biometric-hardware/advantages-biometric-identification-management-system/

[30] J. Cooperband. (2016, August 2016). Two-factor Authentication. Available: https://www.linkedin.com/pulse/two-factor-authentication-jared-cooperband

[31] P. Bours and H. Barghouthi, "Continuous authentication using biometric keystroke dynamics," in The Norwegian Information Security Conference (NISK), 2009.

[32] H. Vaidya, S. Mirza, and N. Mali, "Intrusion Detection System," International Journal of Advanec Research in Engineering, Science & Technology, vol. 3, 2016.

[33] P. Bijaya Kumar, P. Manoranjan, and P. Sateesh Kumar, "Intrusion Prevention System," in Network Security Attacks and Countermeasures, ed Hershey, PA, USA: IGI Global, 2016, pp. 245-258.

[34] D. Sampaio and J. Bernardino, "Open Source Backup Systems for SMEs," in New Contributions in Information Systems and Technologies: Volume 1, A. Rocha, M. A. Correia, S. Costanzo, and P. L. Reis, Eds., ed Cham: Springer International Publishing, 2015, pp. 823-832.