MEDINFO 2021: One World, One Health – Global Partnership for Digital Innovation
P. Otero et al. (Eds.)

doi:10.3233/SHTI220068

Protecting Privacy of Health Information, a Global Perspective

Nona Gatchalian[a], Mujeeb C Kandy [b], Dorinda M. Sattler[c]

[a] *Manager, Health Information Management (HIM), Healthcare Services, Toronto, Ontario, Canada,*
[b] *Head of Health Intelligence, Primary Health Care Corporation, Doha, Qatar*
[c] *Clinical Assistant Professor of HIM, Indiana University Northwest, Indiana, United States*

Abstract

The expanded use of data is part of healthcare transformation that is underway in most countries around the world. While transformation is good for the advancement of healthcare, it presents new challenges for health information professionals. It is critical that the privacy of individual health information be protected throughout the transformation process.

In this abstract, we explore how transformation is taking place in various countries and at different stages as paper-based records are digitized, as electronic health records are adopted, and as health data is used in new data-sharing methods for population health, analytics, and patient engagement.

It is imperative for all health information stakeholders to learn about emerging trends and new rules that will impact their work to protect the privacy of health information in an increasingly digital, mobile, and global world. These requirements, and more are explored in the whitepaper: Privacy of Health Information, an IFHIMA Global Perspective.

Keywords:
Privacy, Digital Health, Global Trends

Introduction

What is the state of healthcare data privacy throughout the globe? To understand the answer to this question, we must know what information is created and used in healthcare, how it is used, and we must understand the concept of privacy as applied globally.

First, there is personal information. What is Personal Information and how do we protect this commodity?

Personal information is data that can uniquely identify an individual. This is defined at the granular, data element level and includes the typical data elements of name, date of birth, and other identifiers. Increasingly, personal information also includes electronic personal identifiers like the internet protocol (IP) addresses of our personal enabled mobile devices, photos, and biometric identifiers such as fingerprints and retina scans.

Personal health information (PHI) is the information that relates to the physical or mental health of the individual.1 The PHI applies to health information in all its forms (e.g., voice, structured and unstructured text, photography, video, facial recognition, wireless, codes, and other technologies). To support the confidentiality and privacy of PHI, individuals need to make privacy a priority.

As electronic health records replace paper-based records, health data is being used for a wide range of purposes including improving population health, disease surveillance and the study of health economics. There are also dramatic changes in how patients, consumers, or individuals access and use their health data. While health information is most often managed by the primary or specialty care provider or organization (provider), it is increasingly shared across platforms and providers, sometimes without the knowledge, understanding, or consent of the patient.

The expanded use of data is part of healthcare transformation that is underway in most countries around the world. While transformation is good for the advancement of healthcare, it presents new challenges for health information professionals. It is critical that the privacy of individual health information be protected throughout the transformation process. A global survey conducted by an IFHIMA privacy workgroup in September 2019 revealed such challenges do exist and it indicated education and awareness on healthcare data privacy would be beneficial for effective implementation.

The survey was attended by 79 participants from 17 countries who responded to questions predominantly on the status of privacy law, challenges in implementation and with stages of electronic health record (EHR) implementation. While 30.4 percent of participants agree that a privacy law was developed and implemented in their countries, 54.4 percent of them responded that the law not fully developed or not implemented effectively. On the question "What do you consider to be the greatest barrier to promoting and preserving the privacy of health information?" 50 percent of responses were "lack of education regarding privacy, 21.8 percent stated, "absence of law" and 17.9 percent of responses on the "lack of resources."

Bringing change to the data privacy landscape requires principled stewardship by health information managements professionals, medical informatics professionals, and policy makers, working together to implement good privacy practices across the healthcare continuum.

Methods

Data related to the privacy of health information was collected from a variety of sources to include law and regulation, journal articles, and peer reviewed journal articles. Professional practice standards and guidelines from associations including the American Health Information Management Association, American Nurses Association, ASTM International, California Health Information Association, Canada Health Infoway, Health Information Management Association of Australia,

Healthcare Information and Management Systems Society, International Association of Privacy Professionals, International Standards Organization, National Institute of Standards and Technology, Organization for Economic Co-operation and Development, World Health Organization, and others were also utilized. Additionally, data was gathered from textbooks, news articles, and legal case reviews. Quantitative analysis of policy and procedure compliance of a United States healthcare provider sample, and a survey of International Federation of Health Information Management Association member countries' privacy readiness was also performed.

Results

Assuring the privacy of health information presents challenges regardless of the level of sophistication of policy, regulation, education, or awareness.

As health information moves from paper-based records to digital, the need for defining and applying robust privacy principles has accelerated. Over the past five years, many countries have developed and promoted a broad array of privacy regulations to address consumer concerns. The applicability of these new regulations to healthcare varies, with some countries specifically exempting healthcare data and other countries or regions, such as the European Union, requiring healthcare data to meet new regulations.

Many of today's privacy regulations have been built upon prior internationally recognized privacy frameworks, dating back to the 1970's. The Principles of Fair Information Practice (FIPPS) of the United States, the Caldicott Principles of the United Kingdom, and the Organization for Economic Co-operation and Development.

The US HIPAA privacy rule has also become a model for other countries.

The European Union's new regulation, General Data Protection Regulations (GDPR), has expanded privacy law to include consumer information across a broad spectrum of industries, including health, and applies to EU citizens' data, irrespective of where their citizens' data is created.2 Many discuss GDPR privacy tenants in the context of the "right to be forgotten." Similarly, the state of California has enacted the California Consumer Privacy Act3 which focuses on consumer data privacy, yet exempts medical data due to robust, pre-existing medical privacy regulation.

Developing countries exhibit a wide spectrum of privacy readiness that may parallel their move to digital health. (refer to Appendix A in the whitepaper) As awareness of the need for privacy, especially as a digital health world increases, governments are looking toward established privacy frameworks.

This awareness has dramatically increased in the past decade due to data sharing in healthcare and supporting industries. Thus, data no longer remains in the silos or applications where it was originally created. Data is still being used for its originally intended purposes, but also for a multitude of other purposes, sometimes without patients/consumers/persons knowledge and without proper oversight being applied.

Healthcare practitioners and health information professionals must be cognizant of the potential impact new regulations may have and understand the applicability or exceptions.

The complexity of health information privacy is illustrated by the case studies of Australia, the Gulf Cooperative Council Region, the European Union, India, Republic of South Korea, Qatar, and the United States as explored in the whitepaper: Privacy of Health Information, an IFHIMA Global Perspective.

Discussion

Health care data privacy is a major concern across the globe. Most of the developed countries have created new, or updated existing, laws and regulations to put forth stringent, focused requirements that address health care data privacy. It is important to note that developing countries are also taking steps to address this important topic. According to the case study by Dr. Mandapam, and Dr. Sinha, Healthcare Privacy is not only a concern of the providers and patient but also to the statutory and regulatory bodies in India.4 A variety of healthcare data is stored in manual and digital platforms at different locations. The risk of privacy breaches is prevalent in hybrid systems.

Among the majority of developing countries, healthcare data privacy has been included under sensitive personal data having some kind of data protection and privacy laws or acts.

It is important that health information professionals are involved in the development and revision review of privacy regulations.

New and emerging technologies are both a benefit and a risk to privacy and health information management. Technology can add privacy enabling safeguards, document compliance, improve transparency, and improve patient access to their own information. Technology must be built and implemented with appropriate privacy rules and practices in mind. Privacy should not be an afterthought.

When new technology uses health information and is stored in the system, a Privacy Impact Assessment (PIA) should be completed prior to new or upgraded technology being used and implemented. The PIA is a privacy risk management tool that identifies gaps in the privacy rules of the technology and workflow. In Canada, it is a mandatory tool in circumstances in health care and government.

Examples of technology that create privacy implications, given their inherent use by consumers and providers, include the following:

1. Patient Portal
2. Records Processing Standards
3. Health Information Exchange
4. Data Sharing: Opt In or Opt Out
5. Information Sharing and Information Management Sharing Agreements

Technology assists in the transition of records that contain PHI, for example, the digitization of paper records. It is important that the processes for creating and managing digitized health records support conformance with a record-holders' various legal obligations, including the production and attestation of copies of material held in digitized health records on request. The Australian Records Processing Standards (AS 2828)5 reminds us that the processes used by an organization for managing digitized health records shall ensure the following:

1. Retention periods
2. Audit trails
3. Protection from alteration
4. Amendments to be annotated and documented

5. Requirements of rules of evidence maintained
6. Consents are to be collected, and information is to be used only as authorized

Privacy and trust go hand in hand. Trust between the patient/consumer and their provider, healthcare organization or pharmacy is essential to health and well-being. When PHI is compromised, trust is eroded, and a loss of trust can be detrimental to the patient - provider relationship. Meanwhile, a data breach can have a significant economic impact on the provider. According to Cost of a Data Breach Study6, by the Ponemon Institute, 36.2 percent of the cost of a privacy breach comes from the lost business, indicating that patients have lost trust in their healthcare providers' ability to uphold the privacy and security of their PHI. In Qatar, health information professionals have transitioned from their traditional role of health records custodian to data stewards and information privacy advocates. According to Mr. Swamy and Mr. Kandy, Health information professionals take up the responsibility of advocating security, privacy, and confidentiality best practices. The Qatar Case Study7 emphasized emerging privacy challenges with healthcare information technology advances and Health Information Exchange (HIE) implementation. As Qatar's comprehensive eHealth privacy policy is in the development phase which incorporates international standards, health information professionals in the country refer existing best practices from AHIMA other international organizations and use HIPAA standards as baseline for their privacy practice implementation.

Regulations and legislation provide a governance framework to keep PHI safe and private. However, according to Ms. Sattler and Mr. Wilde, policies and procedures bridge the gap between privacy regulations and practice8, but it may not meet current legislation and legal landscape if they are not reviewed and updated when new technologies are introduced or when adverse outcomes result due to weak or nonexistent privacy practices. Please see: Privacy Incident Lifecyle, p14 in the IFHIMA whitepaper.

As PHI flows across borders, the complexity of regulations increases along with access, privacy rights and compliance sanctions that incentivize the avoidance of privacy risk. This environment challenges the health information professional to keep abreast of applicable privacy legislation and ensure that organizations appropriately implement and comply with the regulations.

Another framework is stewardship. It is an ethic relating to the responsible handling of information; and governance sets forth the ground rules for execution of this responsibility. Standards for crafting stewardship frameworks for governing health and other sensitive information in physical or even digital form have been around since the 1970s with the Caldicott Principles of the United Kingdom, the Principles of Fair Information Practice (FIPPS) of the United States and the Organization for Economic Co-operation and Development (OECD) Privacy Framework.9

The COVID-19 pandemic clearly illustrates the importance of privacy, where responses necessitated quick decision regarding the capturing and dissemination of personally identifiable health information. A recent IFHIMA article discusses operational issues and challenges in select countries as they rapidly addressed policy and practice regarding COVID-19 data.

Conclusions

There are innumerable components to assuring health data privacy. Health information professionals are challenged to understand basic privacy principles in their respective countries and execute these principles in their chosen roles. This is not easy given the following:

• The rapid digitization of data is creating an explosion in the volume of data that can be created in many different mediums.

• Data is stored in numerous physical locations in paper-based records, on servers, or in the cloud, and may be located anywhere in the world, subject to various countries' regulations.

• Use cases of Personal Health Information (PHI) is on the raise in an unprecedented manner due to advancements in healthcare, clinical transformations, interoperability standards and exchange of information within and beyond healthcare settings.

The COVID19 pandemic has created a tsunami of health information for use by governments, world health agencies and researchers, to control the spread of disease, develop vaccines, share new learning to prevent future outbreaks.

The complexity of understanding privacy of health data continues to increase as technology is more readily available. Health information professionals have been recognized to have a pivotal role in acting as privacy advocates, digital health leaders and data custodians to support the decision makes at the administrative level and at the person level.

Acknowledgements

We would like to acknowledge the International Federation of Health Information Management Associations' Privacy White Paper Working Group authors:

- Jean L. Eaton, Workgroup Leader, Canada
- Lorraine Fernandes, Board Liaison and Author, USA
- Angelika Haendel, Germany
- Jenny Gilder, Australia
- Mujeeb C. Kandy, Qatar
- Dr. Ok Nam Kim, Republic of Korea
- Dr. Sabu Karakka Mandapam, India
- Veronica Miller Richards, Jamaica
- Dr Salim Salmi, Oman
- Dorinda M. Sattler, USA
- Dr. Rajesh Kumar Sinha, India
- Selvakumar Swamy, Watar
- Christopher Wilde, USA

Endnotes

[1] International Organization for Standardization, "Guidance on Health Information Privacy Education in Healthcare Organizations" was published in 2017 by the ISO Technical Committee ISO TC 215 Health Informatics. ISO TR 18628:2017 [SOURCE: ISO 27799:2016, 3.8

[2] EU GDPR Knowledgebase, Understanding 6 key GDPR principles, Punit Bhatia https://advisera.com/eugdpracademy/knowledgebase/understanding-6-keygdpr-principles/

[3] Jergesen, A. (2019). The California Consumer Privacy Act of 2018. CHIA Journal, 70(6), pp. 16-17.

[4] Health Care Privacy: An Indian Scenario, Case Study - India Dr Sabu Karakka Mandapam and Dr Rajesh Kumar Sinha

[5] Australian AS2828

[6] Cost of a Data Breach Study 2019 IBM and Ponemon Institute, https://www.ibm.com/security/data-breach, https://www.ibm.com/downloads/cas/ZBZLY7KL

[7] Health Information Exchange Implementation, HIE Consent Model for Privacy Concerns - Privacy Regulatory Framework, Case Study - Qatar, Selvakumar Swamy and Mujeeb C Kandy

[8] Laying the Foundation for Privacy Practice and Compliance in the Outpatient Setting: Policies and Procedures - Case Study - USA, Dorinda M. Sattler, MJ, RHIA, CHPS, CPHRM and Christopher Wilde, MBA, RHIA, CHC, CHPS, CHPC

[9] Organization for Economic Co-operation and Development. (2013). The OECD Privacy Framework. Retrieved from https://www.oecd.org/sti/ieconomy/oecd_privacy_ framework.pdf

References

[1] Arthur & Castillo. Dominican Data Protection Law 172 -13. Retrieved from http://www.dominicanlaw.com/dominican-dataprotection-law/

[2] CIS.Legislation. Law of the Republic of Kazakhstan: About Personal Data and Their protection. Retrieved from http://cislegislation.com/document.fwx?rgn=59981

[3] Data Protection office, Ministry of Technology, Communication and Innovation – Republic of Mauritius. Data protection Act 2017. Retrieved from http://dataprotection.govmu.org/English/ Publications/Documents/Publications/Leaflet%20on%20 the%20Data%20Protection%20Act%202017.pdf Republic Act No. 1017,

[4] DLA PIPER, Data Protection Laws of the World. Accessed from https://www.dlapiperdataprotection.com/

[5] DLA PIPER, Data Protection Laws of the world. Retrieved from https://ntic.ch/wp-content/uploads/2018/04/Data-ProtectionAll-countries-of-the-world.pdf

[6] ICLG. Angola: Data Protection 2019. Retrieved from https://iclg. com/practice-areas/data-protection-laws-and-regulations/ angola

[7] J. Duffiled, C.Ly, N. Walton. (2015). Privacy Impact Assessment Professional Practise Brief. Retrieved from www.echima.ca.

[8] Laws of Malaysia: Act 709, Personal Data Protection Act 2010. Retrieved from http://ilo.org/dyn/natlex/docs/ELECTRONIC/89542/102901/F1991107148/MYS89542%20 2016.pdf

[9] Law of the Republic of Belarus "On information, Informatization and Protection of Information". Retrieved from https://www. right2info.org/resources/publications/laws-1/laws_belarusfoi-law

[10] Maximiliano & Ines, Practical law: Data protection in Argentina: Overview. Associate of Corporate Counsel. Retrieved from http://www.ebv.com.ar/images/publicaciones/trdatap.pdf

[11] Official Gazette of BiH, 32/01. Law on the protection of personal data. Retrieved from https://rm.coe.int/ CoERMPublicCommonSearchServices/DisplayDCTMContent?do cumentId=09000016806af037

[12] Republic of the Philippines. Retrieved from https://www.privacy.gov.ph/wp-content/uploads/DPAof-2012.pdf

[13] Srikant Ranganathan & Omar Ryan. Keypoint. Bahrain personal data protection law (PDPL). Retrieved from https://www. keypoint.com/media/files/PDPL.pdf

Address for correspondence

Contact@IFHIMA.org