NOVEMBER 2019

Privacy of Health Information, an IFHIMA Global Perspective

International Federation of
Health Information Management Associations

Issued November 2019

Updated September 2020

Privacy of Health Information, an IFHIMA Global Perspective

Introduction 3
What is Personal Information 3
Privacy and Trust 4
Challenge in Maintaining Trust – Technology Moves Faster Than Regulations and Standards 4
Privacy Stewardship Foundations 4
Why Is Privacy A Globally Important Topic? 5
Avoid Risks / Harm / Breach 5
Global Privacy Trends 6
How Technology Impacts Privacy 8
Emerging Technology 11
Privacy Management Program Overview 12
Privacy Awareness Training 12
Privacy in Developing Nations 15
Conclusion 16
About the IFHIMA Privacy Working Group Authors 17
Endnotes 18
References 19
Appendix A Data Protection Laws and Acts Among Selected Developing Countries 19
Case Studies in Privacy Around the World 24

IFHIMA

International Federation of
Health Information Management Associations

About IFHIMA

The International Federation of Health Information Management Associations (IFHIMA) is a non-governmental organization (NGO) in official relations with the World Health Organization (WHO). The Federation, founded in 1968, acts as the global voice of the health information management profession to support delivery of healthcare services and activities and to share best practices. IFHIMA is committed to the advancement of health information management practices and the development of its members for the purpose of improving health data and health outcomes.

- Would you like to keep informed on IFHIMA? Sign up here.
- Did someone kindly share this whitepaper with you? You can get your own digital copy here as a free download.
- Yes! You may share – reprint with permission when you use this citation:

  Source: Privacy of Health Information, an IFHIMA Global Perspective, © Copyright International Federation of Health Information Management (IFHIMA), November 2019. Reprint with permission.

Introduction

Privacy is the right of an individual to keep oneself and one's information concealed or hidden from unauthorized access and view by others[1].

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.

It is critical that the privacy of individual health information be protected throughout the transformation process.

This 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.

New technologies such as machine learning, artificial intelligence and biometric authentication will no doubt further compound these challenges; leading to new policies and regulations to support the privacy of health information.

These changes require principled stewardship by health information management (HIM) professionals and policy makers, to implement good privacy practices across the healthcare continuum by private, public, and community healthcare providers and data users.

In this white paper from the International Federation of Health Information Management Associations (IFHIMA), we explore how the expanding the use of health data is creating privacy challenges. And through this paper, IFHIMA aims to help HIM professionals, policy makers and regulators navigate the changing landscape of privacy of health information by:

- Guiding HIM professionals' understanding of emerging global trends in privacy and to self-identify career path options when managing health information in all its forms and formats;
- Moving health policy stakeholders to have informed discussions and take action in the development of privacy practices with regard to sharing of health information;

In this white paper, our IFHIMA Privacy Working Group authors have included perspectives on protecting privacy of health information from countries around the world and offer more detailed perspectives through case studies from Australia, the European Union, India, Qatar, the Republic of Korea (South Korea), and the USA.

We hope our readers will find this paper enlightening. For more on IFHIMA, visit our web site.

What is Personal Information?

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 our internet protocol (IP) addresses of our personal enabled mobile devices, photos, and biometric identifies such as fingerprints and retina scans.

Personal health information (PHI) is the information that relates to the physical or mental health of the individual.[2] The PHI applies to health information in all its forms (e.g., voice, structured and unstructured text, photography, video, facial recognition, wireless, codes, etc.).

Further, countries or regions, like the European Union, may have regulations that address a broad definition which includes "directly or indirectly" identifiable information, where record matching technology uses individual data elements or a combination of data to provide a reasonable basis to identify an individual.

Knowing what data elements are – and what data elements are not – included in the definitions

of personal information and personal health information directs us to correctly apply privacy rules in the management of the information. The specific data elements are generally defined by national legislation or regulations.

Privacy and Trust

Privacy and trust go hand in hand. As stated above, "privacy is the right of an individual to keep oneself and one's information concealed or hidden from unauthorized access and view by others."

Trust between the patient/consumer and their provider, healthcare organization or pharmacy is essential to health and well-being. When personal health information (PHI) is compromised, trust is eroded and a loss of trust can be detrimental to the patient – provider relationship.

... differing standards and practices can result in fractured or siloed PHI and result in medical errors...

Meanwhile, a data breach can have a significant economic impact on the provider. According to Cost of a Data Breach Study[3], 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.

Regulations and legislation provide a governance framework to keep personal health information safe and private.

Governmental agencies, policy builders, healthcare organizations, and providers, whether public or private, must value the intrinsic benefit of maintaining the privacy and security of data to promote patient safety and ensure trust with the patient.

Challenge in Maintaining Trust – Technology Moves Faster than Regulations and Standards

Securing health information is becoming increasingly complex. In the United States, it is estimated that health data doubles every 73 days[4]. Mobile and inter-connected medical devices and health and lifestyle applications generate reams of information. More vendors, more mobile devices, remote or cloud-based data centers make it increasingly difficult to manage the privacy and security of PHI.

Some information is shared by the individual with their healthcare providers and is managed by the organizations' privacy frameworks. Some information is managed by the individuals themselves or by health and allied health providers who may not be subject to the same legislative regulations and guidelines and generally accepted privacy principles. These differing standards and practices can result in fractured or siloed PHI and result in medical errors. With many entities "touching" data – including the patient/consumer - there may be less trust of the privacy of the PHI. This is something to consider as social and technological changes will continue to influence the privacy of health information.

Privacy Stewardship Foundations

"Stewardship is an ethic relating to the responsible handling of information; and governance sets forth the ground rules for execution of this responsibility."[5]

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.[6]

There are close similarities among these three tenets. For example, seven key elements of the Caldicott Principles are the foundation for stewardship practice and can serve in the development of a privacy framework.

- Justify the purpose(s)
- Don't use patient identifiable information unless it is necessary
- Use the minimum necessary patient identifiable information
- Access to patient identifiable information should be on a strict need-to-know basis

- Everyone with access to patient identifiable information should be aware of their responsibilities
- Understand and comply with the law
- The duty to share information can be as important as the duty to protect patient confidentiality

These decades-old principles continue to serve privacy practices around the globe. A chart of both the FIPPS and Caldicott principles can be found in the IFHIMA white paper, Advancing Information Governance: a Global Perspective, Oct. 2017.

More recently, the Global Data Protection Regulation (GDPR) of the European Union (2018), has taken privacy of information to the next level. It requires protection of an EU subject's data from country to country, not only within the EU, but also beyond the boundaries of the EU - with ramifications for HIM professionals responsible for health data stewardship in all parts of the globe. The GDPR is covered in greater detail later in this paper.

Why Is Privacy A Globally Important Topic?

We live in an increasingly mobile world. Data, like individuals, moves from country to country adding to the challenge of keeping health information private across boundaries. Healthcare organizations are obligated to know and respond to regulations outside of their service area, as health information is increasingly shared across jurisdictions and nations.

There is a general expectation in many countries that personal health information will be available when needed to support individuals receiving health services when the patient presents across town or across the nation. Secondarily, this personal information, in a de-identified or anonymized fashion, is frequently used to create sustainable healthy communities and inform public health policy, research, and for health planning nationally and internationally. These two generalized data uses apply to a variety of healthcare systems include direct healthcare providers and the vendors and infrastructure that support the primary care providers.

Understanding and use of privacy principles must be applied across jurisdictions and across the spectrum of healthcare providers and vendors across the world. These may include:

- Individuals' self-managed healthcare
- Community providers and allied health; (medical, dental, mental, physical therapy, rehabilitation)
- Investigative, diagnostic and therapeutic providers (laboratory, diagnostic imaging, pharmacy)
- Public health, (immunization, sanitation, environmental)
- Acute care organizations (hospitals, treatment centres: rehabilitation, palliative, inpatient, outpatient, private, public, for-profit, not-for-profit)
- Specialty providers
- Insurance / billing
- Vendors / business associates / data repositories / technology
- Healthcare research organizations

The diversity of healthcare systems in any geographical location, community, and state, province, or nation face the challenge of managing data privacy in a coordinated fashion while advancing better healthcare delivery. Establishing common privacy standards across these healthcare systems supports better decision making at an individual, organization, regional, national, and international level.

Avoid Risks /Harm / Breach

The trans-border flows of personal health information and the complexity of regulations around a data subject access, privacy rights, and compliance sanctions incentivize the avoidance of privacy risks. This environment challenges the HIM professional to keep abreast of applicable privacy legislation and ensure that organizations appropriately implement and comply with the regulations.

Global Privacy Trends

As health information moves from paper-based records to digital, the need for defining and applying robust privacy principles has accelerated. 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. 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 to meet new regulations. Healthcare practitioners and HIM professionals must be cognizant of the potential impact new regulations may have, and understand the applicability or exceptions.

> The GDPR applies to data created about an EU citizen, but its reach is global as EU citizens often live around the world.

The next section discusses examples of state, regional or national regulations that are changing the privacy landscape within the respective geographies, and beyond.

General Data Protection Regulation (GDPR), European Union

The GDPR was enacted by the European Union to cover its 28 member nations and 510 million plus citizens. GDPR went into effect May 2018. Once developed, two years between passage[7] and implementation allowed regulations to be promulgated and gave organizations time to comply with the new requirements. Such a time delay is commonly used by all nations to disseminate and advance the stronger privacy regulations.

Healthcare organization in the EU have ramped up their privacy notices and engagement with citizen/patients, as they are bound by GDPR. All organizations must now tackle harmonizing their pre-existing national privacy regulations and practices with GDPR.

The GDPR applies to data created about an EU citizen, but its reach is global as EU citizens often live around the world. Thus, almost any organization could find themselves receiving sanctions and penalties if not complying to the GDPR privacy regulations. The penalties can be up to two percent of an organization's worldwide annual revenue – not a risk that an organization would willingly undertake!

GDPR is often viewed as the new baseline for advancing privacy practices worldwide. For example, privacy breach notification must be made to the regulator within in 72 hours. Privacy professionals are considering that this may be the new de facto notification standard for other legislation which currently use 'as soon as possible' as their mandatory notification time periods.

The core principles of GDPR include:

1. Purpose limitation. Processing of information must be limited to the use for which is was originally collected as part of informed privacy consent. Internet users will recognize the plethora of new internet cookies notices and privacy policy updates attributed to this principle.

2. Data minimization. Data should be processed and used to the minimum necessary to achieve the original intent.

3. Accuracy. Personal information collected and used must be kept current, and be accurate.

4. Integrity and confidentiality. Data must be secured against unlawful and unauthorized use.

5. Storage limitation. Data must be stored only as long as is necessary to achieve the original intent. Individuals may request that their PHI be erased from the organization's data. This is often referred to as the right to be forgotten.

6. Fair and transparent. Organizations must be fair and transparent to the consumer about how their personal data is used.

Overarching accountability must be applied to all the noted principles; thus, it is sometimes considered the seventh principle. Read more on GDPR.

General Data Protection Law (LGPD), Brazil[8]

In 2018 Brazil passed their LGPD which addresses both public sector and private sector data, with compliance required by early 2020. This law, which is designed to protect the 210 million citizens of Brazil, will replace or supplement the current 40 plus federal and state laws that already govern data privacy.

The purpose of these new regulations is to create uniformity and transparency, as today there is a patchwork of state and federal regulations which impede commerce and consumer understanding of how the data is created, used, and secured. LGPD has many components similar to GDPR including extraterritorial application. That is, the law reaches beyond the Brazilian borders and applies to any company or service that has at least a branch office in Brazil and collects data related to a data subject/person in Brazil.

Breach notifications are mandatory, and the required timeframe will be established in the regulations that are not final as of this writing. LGPD requires a data protection officer (DPO) with the regulations needing to address if all entities must have such an officer, or when this is required. A data protection authority (DPA), is being formulated, with the DPA being an independent public authority responsible for promulgating regulations and ensuring enforcement. Both the DPO and the DPA, or a similar function, are becoming common elements of modernized privacy regulations.

California Consumer Privacy Act (CCPA)

Individual states in the United States of America have unique national and state-level privacy health legislation.

CCPA will be the strongest data privacy law in the U.S. California, the most populous state in the U.S. with 36 million people. Enacted the California Consumer Protection Act in 2018, it is scheduled to go into effect in 2020.[9] Like the GDPR, it is focused on consumer data privacy rights with control of information collected about a consumer, and many parallels between the Acts can be found.

CCPA specifically exempts non-profit entities from compliance, thus many California healthcare organizations will not have to comply. Today California has a long established and very detailed medical information privacy structure - California Confidentiality of Medical Act (CCMA). However, there are concerns from healthcare organizations as there is ambiguity about healthcare data that might have to comply with CCPA, such as from a website interaction. And, CCPA does not define medical information in the same way that CCMA does. While the final regulations clarify that information covered by CCMA and HIPAA are exempt from CCPA, healthcare organization should still be concerned with some aspects of compliance given the diverse information collected and used by for profit and not for profit healthcare organizations.[10]

Other Privacy Legislation

Many countries or regions have implemented specific legislation that addresses the unique health information management and privacy needs and risks of specific physical and mental health conditions. For example, regulations specific to mental health, sexual health, infectious diseases, public health, and more.

The challenge to HIM professionals is not only to be aware of specialized legislation, but to be prepared to participate in planning, implementation, and application of specialized legislation in their stewardship of health information.

Privacy legislation covering genetic testing results in most countries around the world is incomplete and scattered. The push for personalized healthcare, consumer engagement to promote wellness, and precision medicine (based upon genetic profiles) heightens the need for comprehensive privacy regulations with regard to genetic testing results. New regulations are being proposed or enacted by countries including Canada, India and the USA.

- In Canada, the federal government passed the Genetic Non-Discrimination Act Bill S-201 in May 2017 that prohibits an employer or insurance company to compel an individual to undergo a genetic test or to disclose test results to them. It is prohibited for any person to collect, use or disclose an individual's genetic test results without their written and voluntary consent. (https://www.priv.gc.ca/en/privacy-topics/health-genetic-and-other-body-information/02_05_d_69_gen/)

- In India, the Pre-Conception and Pre-Natal Diagnostic Techniques (Prohibition of Sex Selection) Act was enacted in 1994. See more in the Case Study: Health Care Privacy: An Indian Scenario.
- In the U.S., the Genetic Information Non-discrimination Act of 2008 prohibits insurance companies from using genetic test results to make decisions regarding eligibility, coverage, or cost. Further, it prohibits employers from using this information as a basis for decisions related to hiring, firing, pay, promotion and the like.[11]

Furthermore, with genetic testing, either clinical or recreational, the right to privacy can affect more than the individual. One person sharing genetic information also exposes those to whom they are closely related, as this article in Fortune Magazine explains: A Major DNA-Testing Company Is Sharing Some of Its Data With the FBI. Here's Where It Draws the Line (http://fortune.com/2019/02/01/genetic-testing-consumer-dna-familytreedna-fbi/)

HIM professionals "live in the trenches" with health data and should be the voice of clarity and transparency for consumers and regulators.

The examples above illustrate a rapidly changing regulatory landscape that will have profound implications to healthcare data stewards.

It is imperative that HIM professionals be involved as data privacy regulations are formulated. HIM professionals "live in the trenches" with health data and should be the voice of clarity and transparency for consumers and regulators.

How Technology Impacts Privacy

Technology is 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. Systems must be designed and deployed to support health record privacy consistent with cultures, regulations, and policy. This requires that privacy decisions and rules be understood by the developers and the users and applied consistently at each stage of development in technology driven initiatives. After all, it's a stewardship obligation.

Patient Portals

The rise of patient portals is seen as both an advantage and a burden. An example of patient portals includes diagnostic imaging centers providing physicians access to view DICOM images. In some cases, patients are granted permissions to view images too, or just the text interpretation report. Other patient portal options allow secure communication between the provider and the patient and can include lab test results, medication history, consultation reports, and appointment messaging. Portals are typically considered a more secure and timely method to share PHI than other options such as fax, email, and telephone messages.

However, this increased access to personal health information may be seen as transferring the burden and the security risk of PHI from the healthcare organization collecting the information to the patient or the third party user of the information.

Research by Canada Health Infoway indicated that 94 percent of patients who use portals said they valued viewing their health information online,[12,13] and found that patients who have access to their health records are more engaged and involved in their own care. This supports using privacy enabling technology to give patients access to their own information.

All too often, healthcare organization and the owners and managers of the portals make their own rules with little standardization within or across jurisdictions. Patient portals must be designed with rules to address privacy and provide secure, role based access. Organizations should establish appropriate timelines when health information will be published to a portal, user access permissions, view only access for limited times (not forever), etc. It may be that the use of patient portals is improving engagement, but it also creates new challenges on how to best educate patients on how to access and use their PHI.

Records Processing Standards

Technology assists with the transition of modalities of 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.[14] The Australian Records Processing Standards (AS 2828) 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

Health Information Exchanges (HIE)

The planned, automated standards-driven, electronic sharing of health information between multiple healthcare providers sometimes using a common defined set of data is known as a health information exchange (HIE). This use of HIE allows doctors, nurses, pharmacists, other health care providers and patients to appropriately access and securely share a patient's vital medical information electronically—improving the speed, quality, safety and cost of patient care.

HIE can greatly improve the completeness of patient's records, which can have a big effect on care, as past history, current medications and other information is available during health encounters.

"Compiling a patient's complete health record still requires a herculean effort involving, multiple web portals, with reams of data files in different formats and standards, and — more often than we'd like to admit — fax machines."[15]

Knowing the risk of using fax machines, government agencies have taken notice and have begun to enforce change. The Information and Privacy Commissioner of Ontario reported that there were 11,278 incidences of health breaches reported to their office in 2018. Of these 6,381 (nearly 57percent) were misdirected faxes.[16]

In the United Kingdom, the Health and Social Care Secretary has banned the NHS from buying fax machines and intends to phase out their use by March 31, 2020.[17]

Privacy enabling technology like patient portals and health information exchanges are more secure. However, appropriate reasonable safeguards must be implemented. HIM professionals must continue to be stewards to manage privacy awareness and ensure that local privacy and data governance rules are consistently applied at the data collection sources and whenever data sharing is anticipated.

Data exchange via a portal should be driven by appropriate role based permissions access, and the privacy conditions set out at the point of PHI and consented to by the individual. PHI data is matched amongst the data sources to ensure that the correct unique individual's information is properly combined.

Data Sharing: Opt-in or Opt-out?

Opt-in or Opt-out is a shorthand description of how the individual expresses their consent on how their information may be used in data sharing. In opt-in policies, an HIE has no data in it until patients give specific permission to contribute their data. In opt-out HIEs, patient data is automatically added to the repository and patients must explicitly request their data not be stored in it for the data to be removed.[18]

Organizations planning to implement HIE are expected to assess the pros and cons of HIE models to ensure better sustainability by addressing a number of important aspects such as interoperability, usability of content and information privacy. HIEs can be either in centralized, federated or in hybrid model in terms of availability and storage location of data. [19]

- Centralized – multiple local sources of data send their data to a central repository
- Federated – or decentralized model provides organizational control of the PHI and provides the framework for data-sharing capabilities
- Hybrid – provides a central data storage location where each data owner controls the access to its data

> Informed privacy consent at the time that the PHI is collected guides the use and disclosure of the PHI throughout the data journey.

Although a centralized model gives a fast response for queries than other models, individual organization might not consider the model as viable unless the model is well regulated and managed by an authorized/trustworthy entity. According to Kathleen M. LaTour[20], the ownership of centralized model will be questionable due to privacy concerns; whereas, federated model could be more acceptable as the data is maintained by respective organizations. As HIE involves multiple organizations, a significant prerequisite for exchanging data is obtaining and assuring patients' consents, through an Opt-In or Opt-Out model.

In the Opt-in model, the patient must proactively agree to participate in the health information exchange prior to when their information is being shared. The Opt-out model will have better participation of patients because the consent is obtained only when patients individually opt out from sharing their information through HIE[21].

Communicating with patients on HIEs and providing awareness of what information is being shared and in what circumstances are important considerations for effective HIE implementation.

In the case study, My Record Health Record: the Australian Experience, Australia's health record implementation offers an example of informed privacy consent by the individual and the need for clear communication about the opt-in and opt-out options.

There is a privacy risk when HIE's are limited in the ability to create granular data transfer rules, for example, based on an individual's opt-in or opt-out decisions. In the absence of an individual's informed consent, governance bodies, like health authorities, may determine that 'all' PHI should be transferred to a HIE for the greater good of all of its residents. Instead of using an opt-in model, data governance decision makers use a reasonableness test to determine if a PHI data set should be used in a HIE. For example, would it be reasonable to assume that an individual would consent to the use of their PHI in a national electronic health record so that the information is available to the benefit of the individual in the event of a health crisis.[22] In these situations, the EHR may have the option to allow individuals to request that their PHI, which is included in the automated data transfer, is masked from subsequent view and use.

HIE is deemed to be a critical element to support e-health initiatives to meet the National Health Strategy Goals 2030 for the country of Qatar as discussed in the case study, Health Information Exchange Implementation-Qatar, HIE Consent Model for Privacy Concerns - Privacy Regulatory Framework.

Information Sharing and Information Management Agreements

Information sharing agreements and information management agreements provide written privacy and security framework to assist in assuring appropriate safeguards and thoughtful planning and communication between participating organizations and healthcare providers.
For individuals/patients, it is necessary to communicate privacy expectations from the point of collection to the use of the information.

There are many sources for guidance on preparing information sharing agreements available to assist in the development of appropriate sharing of personal information. One example from Canada is its Guidance on Preparing Information Sharing Agreements Involving Personal Information – Government of Canada, Treasury Board of Canada Secretariat Privacy (2010, July). (https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/privacy/guidance-preparing-information-sharing-agreements-involving-personal-information.html#Toc267044428)

Emerging Technology

There are daily advances in the ability to transfer and use information in electronic format including application programing interface (API) calls, natural language processing, artificial intelligence, machine learning, and unstructured data queries.

For example, the anticipated adoption of APIs will promote an ecosystem of third-party API-enabled apps, running on smartphones and other mobile devices, as envisioned by the Department of Health and Human Services (U.S.). This will dramatically increase individuals' access to their electronic health records and other healthcare data and will move the U.S. healthcare industry towards a healthcare API economy.[23]

There is a privacy risk when HIE's are limited in the ability to create granular data transfer rules...

Integrated hardware such as smart phones, medical devices and sensors keep individuals in touch with their healthcare providers and help to self-manage their health. The data generated by these apps may be integrated into the electronic health record (EHR), with an expectation that privacy of this data will be managed in the same fashion as the data generated by the EHR.

HIM professionals will continue to be challenged to influence the blending of these patient generated and external health information sources into a traditional health information data repository while advocating for the privacy enhancing best practices.

Privacy Management Program Overview

Organizations which collect, use, or disclose health information are expected to have key components of a privacy accountability program. These include:

- Policies, procedures, training
- Dedicated personnel officers for privacy, compliance and data protection
- Privacy impact assessment and risk management plan
- Accountability requirements to report to the responsible individuals within the organization and to regulators when required
- Maintenance of a data breach register
- Documentation of privacy accountability program and each of its components

These points are taken from How to Build a State of the Art Privacy Program, by Nymity/Radar Privacy Program Webinar, 2019 June 20. https://www.radarfirst.com/offer/webinar/2019-june-webinar-on-demand

Privacy Awareness Training

Privacy awareness training is delivered at many levels – organization, provider, support staff, and to individual patients. Over and over we encounter 'snooping' cases where seasoned as well as new healthcare providers and support team members don't realize that looking at patient's health information without a need to know that information to provide a current health service is wrong. We still need privacy awareness training – even those who push back and say that they have been in the business for years still have more to learn. Many people have the mistaken impression that they can look, as long as they don't tell anyone else.

In her article, New snooping case for health privacy – Decision 74 of the IPC released,[24] Kate Dewhirst, a healthcare lawyer in Toronto, summarized this as "privacy equals don't look and confidentiality equals don't tell."

The Information and Privacy Commissioner of Ontario noted in the 2018 Annual Report that 28 percent of all privacy breaches reported by health information custodians were caused by unauthorized access (which includes "snooping") to PHI. The report also identifies an opportunity to use artificial intelligence technology to quickly identify potential unauthorized access episodes for appropriate follow-up.[25]

> … 'education' is learning information; 'training' is hands-on use of the education at the work site…

Privacy awareness training is considered a common reasonable safeguard to protect patient information and the reputation of the healthcare providers.

A privacy awareness education should include a variety of approaches and should be delivered multiple times throughout the year. This may include:

- Foundational privacy awareness education (in-person or on-line) for each new employee, vendor and business associate to be provided at orientation.
- Specific training when there is:
  - Remote or mobile access to personal or confidential information;
  - New software or changes in software, equipment, procedures or practices;
  - An employee who is promoted or changes roles.
- General reminders throughout the year, using newsletters, on-line interactive quizzes, posters, discussion items at team meetings and other learning approaches.
- Commitment to demonstrate good privacy and security practices and behaviors throughout the year.
- Recognition when individuals demonstrate following privacy principles that also add value to your client satisfaction or business efficiency.

Privacy awareness education is one part of the overall privacy management program.

The National Institute of Standards and Technology (NIST), U.S. Dept. of Commerce, NIST is developing a framework that can be used to improve organizations' management of privacy risk for individuals arising from the collection, storage, use, and sharing of their information. The NIST Privacy Framework: An Enterprise Risk Management Tool ("Privacy Framework"), is intended for voluntary use and is envisioned to consist of outcomes and approaches that align policy, business, technological, and legal approaches to improve organizations' management of processes for incorporating privacy protections into products and services.[26]

ISO TR 18638

In October 2013, the Korean Health Information Management Association (KHIMA) research team proposed to the ISO TC 215 an international standard document which was developed based on Korean educational experiences. The first edition entitled "ISO TR 18638 - Guidance on Health Information Privacy Education in Healthcare Organizations" was published in 2017 by the ISO Technical Committee ISO TC 215 Health Informatics.

Privacy awareness education should include written, formalized curriculum with competencies, educational objectives, and content in addition to informal content. The ISO standards provides guidance and examples to help you.

There are several models that have been developed to guide the development and implementation of privacy awareness education. One example can be found in our case study from Korea, Developing a Global Standard for Health Information Privacy Workforce Education.

Education of Patients

Individuals also have a role to play in the protection of the privacy of their PHI. A privacy awareness program must also include approaches to inform them about their privacy rights including the components of informed consent, safeguards, and

complaints process and their privacy responsibilities. The health workforce needs to understand how to share this information with patients on a practical basis. A privacy awareness program should also include the development of posters, brochures, and other resources to supplement the key messages.

Evaluation Methods

Every good training program needs an evaluation method to determine the effectiveness of the education. A competency based learning approach allows trainees to demonstrate mastery of their knowledge. This might include quizzes, activities, surveys and other techniques.

Audiences for privacy awareness education include:

- Health professionals (clinicians)
- Health information managers
- Administrators
- IT personnel
- Researchers
- Other personnel that comes in contact with healthcare information, such as pastoral workers, counselors, or contractors
- Patients, their family and/or representative and caregivers
- Third party data users
- Vendors who support the collection, use and disclosure of PHI

Auditing and Compliance

Privacy management in both public and private healthcare organizations is complex. Organizations must designate a compliance or privacy officer to act as an internal advocate for good privacy practices and to meet regulatory requirements.

The Ponemon Institute study indicates that simply appointing a privacy officer and forming an incident response team mitigates the overall cost of a privacy breach.[27]

The public also benefits when there are external regulators to ensure that private and public health care providers who collect PHI are in compliance with privacy regulations and best practices. The regulators provide mediation, oversight, and enforcement of sanctions when there are privacy breaches, refusals to access, and failures to maintain reasonable safeguards of health information.

Many jurisdictions have an autonomous Information and Privacy Commissioner (IPC), ombudsman or agency to monitor the government, public agencies, and private organizations to ensure compliance to legislation. These privacy oversight bodies often provide the individual residents a compliance mechanism to appeal access and disclosure practices. They also advise private and public organizations of privacy trends and often offer guidance to the business and issue warnings and advisories to the public when necessary.

The privacy oversight bodies may also review privacy impact assessments, receive and investigate non-compliance complaints, and issue investigative reports and refer investigations to the appropriate government lawyer for prosecution under the law.

Intrinsically, privacy is good for business. When an organization has a mature privacy management program in place, the organization's benefits include:

- Ongoing monitoring of the privacy environment which allows the organization to ensure continued compliance with current legislation and to plan for and adapt to impending privacy legislation changes.
- Avoiding privacy and security sanctions, penalties, and fines.
- Improving privacy by design and communication within the organization, with their business and strategic partners, and with their patients, clients, and customers.

Privacy Officer / Compliance Officer

The privacy officer is responsible for the development and implementation of privacy best practices and the communication with individuals, employees, vendors, and external regulators about privacy. Especially in smaller organizations, many privacy officers have multiple other roles in their organizations. Privacy officers don't need to know everything about privacy and legislation; but they do need to be sensitive to the issues and recognize when an inquiry or situation triggers privacy issues and be prepared to champion the issue and request assistance when necessary.

Privacy Incident Management

Identifying and managing a privacy incident is complex. Planning for a privacy incident is a necessary mitigation strategy that will often save time, anxiety, and money. A privacy incident plan should include these common steps.

- When an incident (or suspected incident) is identified, an incident response team comprised of internal and external experts to contain the risk and to investigate the circumstances around the incident is activated. Depending on the nature of the incident, this may be a simple matter or a potentially debilitating scenario.
- Assessing the risk and determining notification requirements should start quickly in order to meet notification requirements. Decisions and action plans must be made in the first few days of an incident; however, some incidents will necessitate lengthy investigation and notification activities.
- Reporting internally and to regulators (when required) helps to identify trends and evaluate if the mitigation strategies and sanctions implemented in response to an incident have the desired outcomes.

This image from Nymity and Radar illustrates the lifecycle of a privacy incident.

Lifecycle of a Privacy Incident

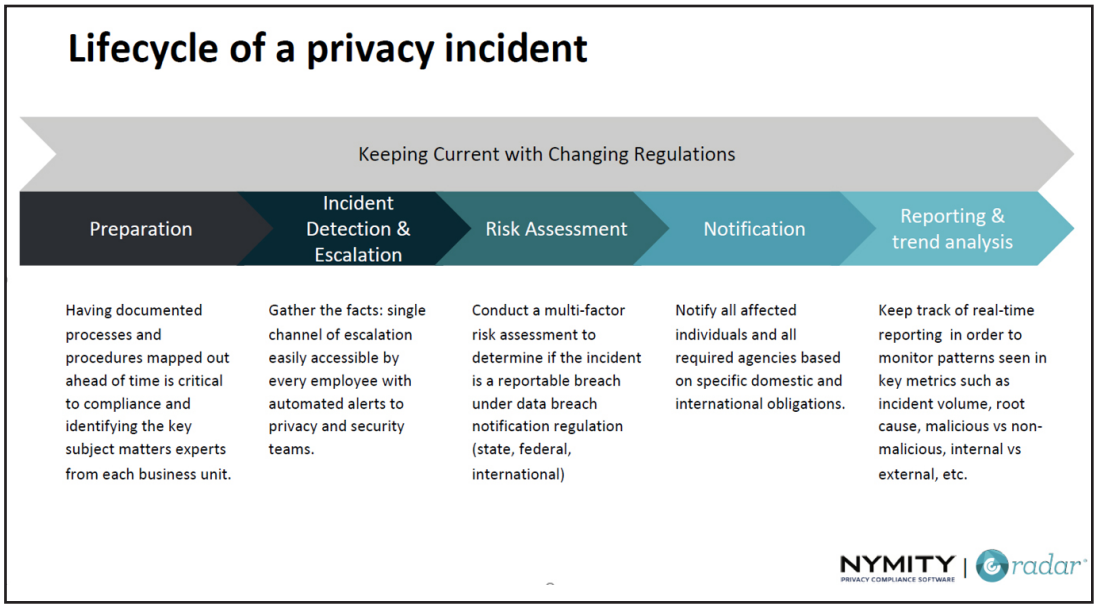
"How to Build a State of the Art Privacy Program", Nymity and Radar, webinar, June 20, 2019, Paul Breitbarth, Director of Strategic Research & Regulator Outreach, Nymity; Travis Cannon, Director of Market Development and Partnerships, RADAR.

Mandatory Privacy Breach Notification

The primary purpose of mandatory privacy breach reporting is to notify the affected individual(s) about the risk of harm as a result of the breach. Reporting the breach to the IPC or the oversight regulator allows trends monitoring and identification of systemic privacy breach so that an individual's right to privacy can be uniformly upheld and respected. In addition, applying sanctions, including penalties and fines, motivates collectors and users of health information to ensure appropriate and reasonable safeguards are implemented and maintained. For example, many websites and on-line commerce portals implemented or updated privacy policy and cookies statements in anticipation of the new GDPR requirements.

Country Perspectives on Breach Notification

As discussed earlier, regulations like the GDPR follow an individual data subject from their home to where they and their personal information may travel.



Other regulations are applied in the region where the data is collected. Some regulations are specific to private or the public sector, health or business information and there are often overlapping regulations.

A privacy incident may require mandatory notification requirements under multiple legislations. In these cases, the organization is expected to meet the shortest breach reporting requirements. Currently, many legislations have wording that requires notification to the regulators and patients "as soon as practicable" which often has been interpreted as weeks' duration. The GDPR uses "without undue delay and, where feasible, not later than 72 hours." We may see that other jurisdictions will be influenced to also expect notification within 72 hours.

A few examples of privacy regulations which require mandatory privacy breach notification are:

- Australia – Mandatory Breach Notification, February 2018
- Brazil – Data Protection Law, 2020
- Canada – Personal Information and Protection of Electronic Documents Act (PIPEDA), November 2018; health information specific mandatory breach notification regulations in most provinces
- EU - GDPR, May 2018
- India – draft Personal Data Protection Act
- Japan – GDPR adequacy recognition
- U.S. – CCPA and more than 11 state-specific breach notification bills; HIPAA

Privacy in Developing Nations

Health care data privacy is 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.

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. The table in Appendix A (at the end of this white paper) highlights data protection laws and acts among selected developing countries.

As a country moves from paper based to electronic records, developing nations have a unique opportunity to incorporate health data privacy into general data privacy regulations or create unique health privacy regulations. These nations can expedite the process by taking advantage of the long-standing data protection and privacy principles such as, the Fair Information Practice Principles or the Caldicott Principles which IFHIMA has discussed its white paper: Advancing Health Information Governance: A Global Imperative. The GDPR also offers a good baseline of regulations to consider.

Cultural, religious, geographic and political nuances may influence how developing nations prioritize and detail data privacy regulations, as will the maturity of the health systems, health funding, stable infrastructure - such as high speed internet and electricity, and technology adoption.

The case studies that follow – from Australia, European Union, India, Korea, Qatar and the USA – illustrate the development and application of privacy regulations from a variety of nations, and the focus that may be applied for managing the privacy of health information.

Conclusion

There are innumerable components to assuring health data privacy, with a select few discussed in this white paper. HIM 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 can be stored in numerous physical locations on servers, or in the cloud, that may be located anywhere in the world and subject to country specific regulations.
- The complexity of understanding all the factors continues to increase as technology is more readily available.

Therefore, IFHIMA recommends that HIM professions consider the following when privacy regulations are being explored or revised in their countries.

1. *Get involved as privacy or data protection regulations are developed and provide feedback to all principles, but especially to healthcare*
2. *Assess what the proposed regulations may mean to your organization and communicate your concerns and insight to leadership and legislative/regulatory bodies*
3. *Identify required changes to systems, policies, processes, and technologies as the regulations are finalized*
4. *Train your healthcare teams, administrators, and patients/ clients about their privacy rights and responsibilities.*
5. *Commit to ongoing professional growth through continuing education and take a leadership approach to data stewardship.*

Building trust is imperative when it comes to protecting the privacy of health information. HIM professionals live in the trenches and should be the “trust brokers” and privacy data stewards when it comes to health data. HIM professionals, in our role as stewards of health data, should be the voice of clarity and transparency for patients, consumers and regulators. HIM Professionals have an opportunity to take a leadership role with regard to the privacy of health information. It’s a matter of trust and good stewardship.

IFHIMA Privacy White Paper Working Group Authors

Jean L. Eaton

BA Admin (Healthcare), CHIM is the IFHIMA Privacy Whitepaper Working Group Lead and Practical Privacy Coach with Information Managers Ltd. which provides privacy, health information and practice management consultation services to healthcare providers throughout Canada. https://www.linkedin.com/in/jeaneaton

Lorraine Fernandes

RHIA serves on the IFHIMA Board of Directors as President-elect (2016-2019) and Liaison to IFHIMA Privacy Workgroup. Lorraine is Principal at Fernandes Healthcare Insights, a data governance focused practice. https://www.linkedin.com/in/lorraine-fernandes-07723b1/

Angelika Haendel

MA, B.Sc. is the immediate Past President of IFHIMA and Board Member of the German Association of Medical Documentation and Health Information Management (DVMD). As Board member of IFHIMA and DVMD, she brings together HIM associations from Europe, Middle East, Asia, and The Americas. She serves as co-chair of the EFMI working group HIME, and has been serving on AHIMA's Global Health Workforce. https://de.linkedin.com/in/angelika-haendel-0a44aba

Jenny Gilder

MRA, CHIM, FHIMAA is a Life Member and immediate past president of Health Information Management Association of Australia (HIMAA). Jenny is vitally interested in the international developments occurring in health information management, especially in the South East Asian region. https://www.linkedin.com/in/jenny-gilder-mra-fhimaa-chim-5712b6140/

Mujeeb C Kandy

M.App.Sc, MS, CPHQ, RHIA, a Health Information Management professional in the middle east for over 20 years, is currently working at Primary Healthcare Corporation, Qatar, as Head of Health Intelligence and actively engaged in HIE implementation, clinical coding and clinical documentation improvement program.

Ok Nam Kim

Ph.D. Health Management, KHIMA is the IFHIMA Regional Director, South East Asia and a Licensed Health Information Manager in Korea. Ok Nam is a professional member of Korean National Standard Committee for ISO/TC215, and a consultant working for developing the privacy regulation and educational program.

Dr. Sabu Karakka Mandapam

A Professor of Health Information Management and an Associate Dean, Manipal College of Health Professions, Manipal Academy of Higher Education, Manipal, India and IFHIMA Privacy White Paper Working Group Member.

Veronica Miller Richards

BSc, is the National Director to IFHIMA for the Jamaican Health Information Management Association. Veronica is the Regional HIM Director for the Southern Region Health Authority, Manchester, Jamaica.

Dorinda M. Sattler

MJ, RHIA, CHPS, CPHRM is a Clinical Assistant Professor of HIM at Indiana University Northwest. Dorinda is also the Consultant/Owner of Sattler Healthcare Consulting, Inc. which provides HIM and Risk Management Consulting services to healthcare providers throughout the state of Indiana. linkedin.com/in/dorinda-sattler-45414a92

Dr Rajesh Kumar Sinha

An Associate Professor and Head, Dept. Health Information Management, Manipal College of Health Professions, Manipal Academy of Higher Education, Manipal, India and IFHIMA Privacy White Paper Working Group Member.

Selvakumar Swamy

B.Sc, BMRSc., RHIA is a seasoned Health Information Management professional with 30 years of experience covering traditional medical records system, transition to EMR and information governance. Selvakumar is currently employed as Business & Health Intelligence Manager in Directorate of Strategy Planning & Health Intelligence of Primary Health Care Corporation, Doha, Qatar.

Christopher Wilde

MBA, RHIA, CHC, CHPS, CHPC is an IFHIMA Privacy White Paper Working Group Member and the Senior Manager, Compliance/Auditing/Third Party Oversite, Centene Corp. https://www.linkedin.com/in/christopher-wilde-rhia-chc-chps-chpc-b6337aa/

Endnotes

1. *Organization for Economic Co-operation and Development. (2013). The OECD Privacy Framework. Retrieved from https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf*
2. *ISO TR 18628:2017 [SOURCE: ISO 27799:2016, 3.8*
3. *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*
4. *Healthcare IT News, Former Cleveland Clinic CEO Toby Cosgrove on AI,data and joining Google, May 15,2019 https://www.healthcareitnews.com/news/former-cleveland-clinic-ceo-toby-cosgrove-ai-data-and-joining-google*
5. *L.L.Kloss, "Information Governance and Management," in Ethical Health Informatics: Challenges, and Opportunities, L. B. Harman and F. H. Cornelius, Eds., 3rd ed: Jones & Bartlett Learning, 2015, pp. 393-418*
6. *Organization for Economic Co-operation and Development. (2013). The OECD Privacy Framework. Retrieved from https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf*
7. *EU GDPR Knowledgebase, Understanding 6 key GDPR principles, Punit Bhatia https://advisera.com/eugdpracademy/knowledgebase/understanding-6-key-gdpr-principles/*
8. *International Association of Privacy Professionals, The new Brazilian General Data Protection Law – a detailed analysis, August 15, 2018 https://iapp.org/news/a/the-new-brazilian-general-data-protection-law-a-detailed-analysis/*
9. *National Law Review, The California Consumer Privacy Act What to Know – and what to do, April 17, 2019. https://www.natlawreview.com/article/california-consumer-privacy-act-what-to-know-and-what-to-do*
10. *Jergesen, A. (2019). The California Consumer Privacy Act of 2018. CHIA Journal, 70(6), pp. 16-17.*
11. *NIH Research Portfolio Online Reporting Tools, Genetic Information Non-discrimination Act, page updated June 30, 1018 https://report.nih.gov/nihfactsheets/ViewFactSheet.aspx?csid=81*
12. *Canada Health Infoway. Digital Health Myths, 15 May 2017. https://www.infoway-inforoute.ca/en/component/edocman/resources/3300-myth-patients-don-t-want-to-see-their-health-information-and-won-t-find-the-information-useful?Itemid=101*
13. *Knowing is Better Than not Knowing – When it Comes to Lab Test Results, Canada Health Infoway, September 9, 2015. https://www.infoway-inforoute.ca/en/what-we-do/news-events/newsroom/2015-news-releases/6653-knowing-is-better-than-not-knowing-when-it-comes-to-lab-test-results.*
14. *Australian AS2828*
15. *2019Mar08 - https://www.linkedin.com/pulse/why-chcf-investing-improve-data-exchange-again-hong-truong/*
16. *Information and Privacy Commissioner of Ontario, April 9, 2019 2018 Annual Report, https://www.ipc.on.ca/wp-content/uploads/2019/06/ar-2018-e.pdf*
17. *Department of Health and Social Care. Health and Social Care Secretary bans fax machines in NHS. gov.uk Dec 9, 2018 https://www.gov.uk/government/news/health-and-social-care-secretary-bans-fax-machines-in-nhs*
18. *https://healthitsecurity.com/news/should-a-health-information-exchange-be-opt-in-or-opt-out*
19. *Healthcare Information and Management Systems Society. A HIMSS Guide to Participating in a Health Information Exchange, HIMSS Healthcare Information Exchange, HIE Guide Work Group White Paper, November 2009. https://www.himss.org/sites/himssorg/files/HIMSSorg/Content/files/HIE/HIE_GuideWhitePaper.pdf*
20. *LaTour, K. (2013). Health information management: Concepts, principles, and practice (4th ed.). Chicago, Ill.: AHIMA. Retrieved from http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_033588.hcsp?dDocName=bok1_033588*
21. *AHIMA (January, 2013). Understanding the HIE landscape. Journal of AHIMA 84, no. 56-63. Retrieved from http://library.ahima.org /xpedio/groups/public/documents/ahima /bok1_049890.hcsp?dDocName=bok1_049890*
22. *Canada Health Infoway – Knowing Is Better Than Not Knowing; Digital Health for Health Care Providers, https://www.betterhealthtogether.ca/digital-health-and-you/digital-health-for-health-care-providers*
23. *Proposed rules from HHS open door to healthcare API economy, By Greg Slabodkin, February 14 2019 https://www.healthdatamanagement.com/news/proposed-rules-from-hhs-open-door-to-healthcare-api-economy?utm_campaign=ReinventRadiology-Feb%2018%202019&utm_medium=email&utm_source=newsletter%20.%20https://www.healthdatamanagement.com/news/proposed-rules-from-hhs-open-door-to-healthcare-api-economy*
24. *Kate Dewhirst. New snooping case for health privacy – Decision 74 of the IPC released. September 4, 2018. https://katedewhirst.com/blog/2018/09/05/new-snooping-case-for-health-privacy-decision-74-of-the-ipc-released/*
25. *Information and Privacy Commissioner of Ontario. 2018 Annual Report: Privacy and Accountability for a Digital Ontario Jun 27 2019 https://www.ipc.on.ca/2018-annual-report-privacy-and-accountability-for-a-digital-ontario/*
26. *National Institute of Standards and Technology, U.S. Department of Commerce, Developing a Privacy Framework, Nov. 14, 2018. https://www.federalregister.gov/documents/2018/11/14/2018-24714/developing-a-privacy-framework#footnote-1-p56824*
27. *Ponemon Institute. Figure 19 https://www.ponemon.org/local/upload/file/Sixth%20Annual%20Patient%20Privacy%20%26%20Data%20Security%20Report%20FINAL%206.pdf*

References

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

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

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

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

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

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

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

Arthur & Castillo. Dominican Data Protection Law 172 -13. Retrieved from http://www.dominicanlaw.com/dominican-data-protection-law/

CIS.Legislation. Law of the Republic of Kazakhstan: About Personal Data and Their protection. Retrieved from http://cis-legislation.com/document.fwx?rgn=59981

Laws of Malaysia: Act 709, Personal Data Protection Act 2010. Retrieved from http://ilo.org/dyn/natlex/docs/ELECTRONIC/89542/102901/F1991107148/MYS89542%202016.pdf

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%20the%20Data%20Protection%20Act%202017.pdf

Republic Act No. 1017, Republic of the Philippines. Retrieved from https://www.privacy.gov.ph/wp-content/uploads/DPA-of-2012.pdf

Appendix A: Data Protection Laws and Acts Among Selected Developing Countries

By Dr. Sabu K M, M.App.Sc, PhD

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. The table in Appendix A highlights data protection laws and acts among selected developing countries.

Country	Region	Privacy law/Act status	Major highlights
Angola	Central Africa	Data Protection Law 2011 (DPL)	• Protection of Personal information • Personal data containing sensitive information • Transparency in Data processing, legitimize collection and use of data and retention of data only for the period for the purpose data collected
Argentina	South America	Personal Data Protection Law (PDPL), Law 25,326	• Scope includes protection of personal data and sensitive personal data • Sensitive data (includes health and sexual activity) should not be disclosed and must be collected with consent as permitted by the law

Bahrain	Middle East	Law No 30 of 2018 on Personal Data Protection (Data protection Law)	• Under the law, a Personal Data Protection Authority will deal with Data protection violations • Scope includes protection of personal data and sensitive personal data • Law also governs; collection, sharing, security and breach notifications on personal data
Belarus	Europe	Law on personal Data 2018 (Draft under review)	• First Belarusian Legal Act for regulation of personal data protection issues. • Law will cover protection of sensitive personal data by inclusion of a term 'Special personal data'
Bosnia & Herzegovina	Balkan	Law on Protection of Personal Data (DP Law) 2006, amended 2011	• Scope includes protection of personal data and sensitive personal data • Same law also governs online data privacy
Brazil	South America	Brazilian General Data Protection Law (LGPD), 2018	• Scope includes protection of personal data and sensitive personal data • Covers manual and digital data protection
Burundi	East Africa	No specific Personal Data Protection law.	• However existing law and regulations including health sector laws impose some data protection requirements and confidentiality of patient information.
Cape Verde	Africa	Data Protection Law (Law 133/V/2001)	• Scope includes protection of personal data and sensitive personal data
Chile	South America	Law 19,628- Protection of Private life known as Personal Data Protection Law (PDPL) Law no 20.584 regulates rights and duties related to healthcare	• Law 20.534 terms all information containing or regarding healthcare procedures and treatments as sensitive data • Scope includes protection of personal data and sensitive personal data
China	East Asia	Covered by several laws, National Standard of Information Security Technology 2013	• PRC Cybersecurity law also address online data privacy protection • Scope includes protection of personal data and sensitive personal data

Dominican Republic	Caribbean	Law No. 172-13, the protection of Personal Data (DPL), 2013	• Scope includes protection of personal data and sensitive personal data • No obligation to report breach of data privacy
Egypt	Northeast Africa	No law available to regulate protection of personal data. However, some of the existing laws deal with data privacy to a certain extend.	• Scope includes of personal data only • No specific provision to regulate online data privacy
Ghana	West Africa	Data Protection Act, 2012	• Scope includes protection of personal data and sensitive personal data
Honduras	Central America	Several National law deal with the data protection and privacy. Law for Protection of Confidential Personal Data is under formulation in the Honduran congress	• Scope includes protection of personal data and sensitive personal data • National Civil Registry and Institute for the Access to Public Information are the two entities responsible for the enforcement of personal data protection
Indonesia	Southeast Asia	No specific law on Data Protection. Electronic Information and Transactions (EIT Law) covers protection of Personal Data	• Scope includes protection of personal data. • No specific mention about health data protection
Kazakhstan	Central Asia	Law of the Republic of Kazakhstan No 94-V, 2013 covers on personal data and its protection	• Personal data scope includes: Generally accessible personal data and Limited access personal data. • Law also governs; collection, sharing, security aspect of personal data. However, no specific provisions for breach notifications on personal data

Kenya	East Africa	No specific Data protection law. However Constitution of Kenya 2010, and few acts deals with data protection : Access to Information Act 2016, Health Act 2017 and Computer Misuse and Cybercrimes Act 2018	• Scope includes only protection of personal data, which also clearly states about various aspects of health data • Doesn't regulate online data privacy
Lesotho	Southern Africa	Data Protection Act (DP Act)	• Scope includes protection of personal data and sensitive personal data • Data Protection Authority and Commission control over DP Act and right of information privacy.
Malaysia	Southeast Asia	Personal Data Protection Act 2010 (PDPA) Personal Data Protection Standards 2015	• Scope includes protection of personal data and sensitive personal data • Security, Retention and Data integrity standards for Personal data processed electronically and Non- Electronically
Mauritius	East Africa	Data Protection Act 2017 (DPA 2017)	• DPA is in align with the GDPR
Mexico	North America	The federal law on protection of personal data, 2010 deals with Data protection	• Scope includes protection of personal data and sensitive personal data • The National Institute of Transparency for Access to Information and Personal Data Protection serves as the prominent authority for data protection
Panama	Central & South America	Draft Data Protection Law under formulation since 2018	• No law covers personal or sensitive data protection and privacy aspects
Philippines	Southeast Asia	Data Privacy Act of 2012/ Republic Act No 10173	• Scope includes protection of personal data and sensitive personal data includes health care data • Act suggest creation of a National Privacy commission

Peru	South America	The personal Data Protection Law 29733 (PDPL), 2011	• Scope includes protection of personal data and sensitive personal data
South Africa	Southern Africa	The Protection of personal Information Act 4 of 2013 (POPIA) under implementation	• Scope includes protection of personal data and sensitive personal data • Section 22 of POPIA deals about Data privacy breaches
Tajikistan	Central Asia	Personal Data Protection Law, 2018, Protection Data Law 2002 and Information Law 2002	• Scope includes protection of personal data and covers all forms of personal data
Trinidad and Tobago	Caribbean	The Data Protection Act , 2011	• Scope includes protection of personal data and sensitive personal data • Act do not have specific provision for online data privacy
Ukraine	Eastern Europe	Law of Ukraine No. 2997 VI on Personal Data protection , 2010 (Data Protection Law)	• It essentially complies with EU Data Protection directive 95/46/EC • Scope includes protection of personal data and data relating to health or sex life of an individual.
Zimbabwe	Southern Africa	No specific Data protection law. Covered under Zimbabwe constitution (chapter 10: 247) Access to Information and Protection of Privacy Act	• Most of Data protection provisions are covered under this chapter • National ICT policy 2016 address digital data protection • No law defines sensitive personal data

Case Studies In Privacy Around The World

My Health Record – the Australian Experience 25

Information Privacy in the GCC Region: Access and Disclosure 29

General Data Protection Regulation of the European Union Reaches Far Beyond Europe 37

Health Care Privacy: An Indian Scenario 43

Developing a Global Standard for Health Information Privacy Workforce Education – a Republic of Korea (South Korea) Case Study 48

Health Information Exchange Implementation-Qatar, HIE Consent Model for Privacy Concerns - Privacy Regulatory Framework 52

Laying the Foundation for Privacy Practice and Compliance in the Outpatient Setting: Policies and Procedures - Case Study – USA 55

IFHIMA

International Federation of Health Information Management Associations

About IFHIMA

The International Federation of Health Information Management Associations (IFHIMA) is a non-governmental organization (NGO) in official relations with the World Health Organization (WHO). The Federation, founded in 1968, acts as the global voice of the health information management profession to support delivery of healthcare services and activities and to share best practices. IFHIMA is committed to the advancement of health information management practices and the development of its members for the purpose of improving health data and health outcomes.

- Would you like to keep informed on IFHIMA? Sign up here.
- Did someone kindly share this whitepaper with you? You can get your own digital copy here as a free download.
- Yes! You may share – reprint with permission when you use this citation:

  Source: Privacy of Health Information, an IFHIMA Global Perspective, © Copyright International Federation of Health Information Management (IFHIMA), November 2019. Reprint with permission.

My Health Record – the Australian Experience

Jenny Gilder
MRA, CHIM, FHIMAA

Australia

Introduction

The objective of this case study is to outline the journey Australia has taken in the development of a Personally Controlled Electronic Health Record (PCEHR), which is called the My Health Record. It will also explore the pitfalls, potholes and unexpected challenges faced by consumers, government, the digital health agency and primary health networks over the last ten years, especially those identified by the Health Information Management Association of Australia (HIMAA). The case study will also explore the privacy concerns expressed by the Australian community including residents during the roll out phase which resulted in some major rethinking at the highest levels of government at the last minute.

The PCEHR, morphed into the My Health Record, and from 1 February 2019 all residents holding a Medicare card have a My Health Record with the exception of the 2.5 million Australians who chose to opt out.

Problem Statement/Background

The National Health and Hospitals Reform Commission made a recommendation in 2009 that a personally controlled electronic health record for every Australian would be an important step in improving the quality and efficiency of health care by developing an electronic health record (EHR) with access controlled by the health consumer, and containing minimal levels of health information that could be sourced from existing systems and then developed to source information from health services including primary health services.[1]

This was a Commonwealth approach with agreements from all the States through COAG (Council of Australian Governments).

The Australian Government announced in 2009 the funding of $467 million to commence the development phase of the PCEHR.

The PCEHR was launched in July 2012 and people were encouraged to register to enable them to participate. Initially, this was an “opt in” for both the consumers and health professionals. This became one of the flaws in the roll out and would cause consternation later.

The National e-Health Transition Authority (NeHTA) provided the initial framework of the PCEHR including unique identifiers, secure messaging and national clinical terminologies. Unfortunately, Australian Health Information Managers (HIMS) were left out at this stage to the detriment of the development of the PCEHR in the opinion of the Health Information Management Association of Australia and many others who were concerned with the opt in system of participation, governance arrangements, system usability and clinical content of the records.[2]

A review conducted by the Australian Government of the PCEHR system was undertaken in 2013. This review found that there was overwhelming support for the continued implementation of a consistent electronic health record system for Australians, but a change would be needed to mitigate early implementation issues. The review came up with thirty eight recommendations across eight key areas and the writer will concentrate on key concerns around privacy and security of records.

The renaming of the PCEHR was also a major recommendation by the Commonwealth Government of Australia to ensure engagement of consumers as owners of their medical record balanced with the needs of the clinicians. So, the My Health Record or MyHR was "born "and opt in was turned around to be opt out.[3]

(My Health Record does not replace the health records kept by individual health services. The My Health Record is a summary of information only, that is populated, with the patient's consent by their primary care giver i.e., the local GP and other care givers, and can include current medications, a patient health summary, discharge summaries, pathology results, radiology results and hopefully with further development a direct link to specialist physicians.)

Discussion and Recommendations

The Legislation and the Trial

The Government of Australia responded favorably to the 38 recommendations from the Commonwealth Government of Australia and allocated sufficient funds in in the 2015-16 Budget to continue with the implementation of the MyHR which included:

- Strengthening digital health governance and operations through the establishment of the Australian Digital Health Agency to manage governance and ongoing delivery including opt-out.
- Improving usability and the clinical content and providing education and training to healthcare providers.

Not much was really discussed about the privacy of the data which was covered by the Commonwealth (Cth) Privacy Act 1988, which under Australian law regulates the handling of personal information on individuals and includes thirteen Australian Privacy Principles which includes health information. In Australia, the health information manager has been a major gatekeeper of the health information within medical records and they are well versed in the use and disclosure provisions of the Privacy Act.

The My Health Records Act 2012 Cth established the role and functions of the systems operator, a registration framework for individuals and healthcare providers, and a privacy framework aligned with the Privacy Act 1988 specifying the use and disclosure of information in the system including the health information included in the My Health Record. The My Health Record Act 2012 (Cth) also imposed penalties for improper use, collection and disclosure of the health information. In my opinion and on reading of submissions and discussion papers around the development of the My Health Record, there was not enough emphasis on the privacy provisions apart from the legislation in place. There was an assumption by us all that the privacy acts would cover all concerns.

The opt-out required amendments to the MyHR Act which was passed in November 2015. Trials were commenced in 2016 which included the opt out trials. The trial sites included the Nepean Blue Mountains local health district and Northern Queensland and involved approximately one million people. It was pleasing to note that there was a positive response from individuals and health care providers for the creation of their health care record automatically as they were already in the Australian Medicare system. A national opt out approach was agreed upon by all State and Territory Governments in March 2017. The Australian government announced that all Australians would have a My Health Record by the end of 2018 unless they chose to opt out. The opt out period was to end on the 15 November 2018.

The Concerns Commence

It was during the opt out period that the My Health Record garnered a great deal of print and social media attention around privacy and use and disclosure, and then came some fierce debates on “talk back” radio and television most of it misinformed but whipped up as it is wont to do these days. One wonders if health information managers were consulted much earlier and well before the information technology crowd, if some of these concerns could have been addressed and highlighted. The concerns included release of information to law enforcement agencies, other government agencies, storage of information after a My Health Record was cancelled and the ability of the system operator to disclose health information. Other concerns related to disclosure of health information to insurers including sensitive health information that may affect a future claim. There was also a period during this phase where a level of distrust of the government and their ability to protect personal My Health Records was evident.

The writer was employed as a community engagement officer during a short period before the opt out period was to finish on the 15 November and during this time I was able to reassure many people who approached the My Health Record information desk, many of which were set up around the community, that legislation has always been in place to protect their health information and many went away confident that a My Health Record was more beneficial than what some of the more fervent media were making out.

Allaying the Concerns

To take some of the heat out of the situation, the government decided to extend the opt out period until 31 January 2019. The community engagement was to continue and the My Health Record Act was amended and strengthened on top of the very robust privacy framework already in place.

The My Health Care Records Amendment (Strengthening Privacy) 2018 Bill removed the ability for the MyHR systems operator to disclose health information to law enforcement agencies and government agencies without a judicial court order or the consent of the healthcare recipient. The bill also requires that health information can only be collected, used or disclosed for healthcare purposes with consent, and cancellation of a MyHR will mean permanent deletion of a record within 24 to 48 hours. (While a My Health Record Health Record is permanently deleted, this does not mean all their health information is deleted as their GP and other health services they will have attended will have the health information; it just will not be summarized in their on line MyHR.)

The Amendments Bill was passed and duly signed off, the opt out period ended on the 31 January 2019 with hardly a mention and Australian’s have a My Health Record unless they have opted out. In the end it was a bit of anticlimax after all the flurry and concerns. Now let’s hope for a roll out of electronic medical records across Australia to enable full integration of discharge information. The My Health Record is a boon for those with chronic medical conditions, remote communities, young families, and travelling older Australians.

Conclusion

This case scenario highlights a flaw in the development of systems, governance and legislation around health information management. It is my hope that any future developments and improvements in Australia's My Health Record will include a great deal more consultation by the subject matter experts, the health information management profession.

About the author

Jenny Gilder, MRA, CHIM, FHIMAA, Life Member of Health Information Management Association of Australia (HIMAA) and was its immediate past president. Jenny, an IFHIMA Privacy White paper working group member, is vitally interested in the international developments occurring in health information management, especially in the South East Asian region. Jenny is currently an active member of HIMAA.

https://www.linkedin.com/in/jenny-gilder-mra-fhimaa-chim-5712b6140/

Endnotes

1. *National Health and Hospitals Reform Commission*
https://www.ncbi.nlm.nih.gov/pubmed/19807629

2. *Keeve J. Allison Y. Personal Electronic Health Records: the start of a journey*
https://www.nps.org.au-prescriber/articles/personal-electronic-health-records-the-start-of-a-journey

3. *Review of the Personally Controlled Electronic Health Record December 2013 www.health.gov.au/internet/mainpublishing.nsf/content/eHealth*
Circulated by authority of the Minister for Health, the Hon Greg Hunt MP My Health Records Amendments (Strengthening Privacy) Bill 2018 The Parliament of the Commonwealth of Australia

Information Privacy in the GCC Region: Access and Disclosure

Salim Al Salmi
PhD, MSc, PGCert Med Edu, RHIT, CHIM

Raniya Al Kiyumi
PhD, MSc HIM, GradCertEd.

Hussein Albishi
BSc HIM, CHIM

Ahmed Al Hatlan
BSc, MS, CHIM, CPHIMS

Safia M. Dawood
MSc CS, HINF, CPHIMS

Haya Alkhatlan
PhD, MSc

Fatima Al Baloushi
BSc, MQM

Osama El-Hassan
MSc, PhD

Introduction

Like other countries around the world, the Gulf Cooperation Council (GCC) nations have invested in the adoption of Electronic Health Record (EHR) in their healthcare systems and, as a result, concerns about the privacy and security of health information have become a priority. The GCC comprises six countries that share similar cultures and common political identities, which are rooted in Islamic values. Thus, Health Information Privacy (HIP) in GCC countries is often practiced in a socio-cultural context. Information-sharing started with the motivation to identify the current health information uses, clarify access and disclosure practices, and reveal the challenges in this area. A comparative method among GCC countries was adopted in this article to identify the similarities and differences between the nations.

A brief discussion of the current access, disclosure practices and the challenges identified in four of the GCC nations, namely the Kingdom of Saudi Arabia (KSA), Kuwait, the Sultanate of Oman (Oman) and the United Arab Emirates (UAE), is introduced in this paper.

Background

The Ministry of Health (MOH) is a major government owner, operator, regulator, and financer of 60 to 85 percent of all healthcare services offered in the GCC countries of Saudi Arabia, Oman, and Kuwait. Most of the GCC countries provide health services free of charges to their citizens. Expatriate employees, “expats,” are granted special care in these countries, although expats working in the private sector typically have employer insurance coverage. All healthcare facilities are accessible to all residents during crises and emergencies.

There are several healthcare service providers in all GCC countries that are considered to be governmental, for example ARAMCO hospitals in Saudi Arabia, Armed Forces Medical Services in Oman, Zayed Military Hospital in the UAE, and The Kuwait Military Forces hospital in Kuwait.

In most GCC countries, the private sector also participates in the provision of healthcare services, especially for expatriates and insurance cardholders. For example, in the UAE, the private sector has a bigger share of the healthcare market as the country has been gradually transitioning to private health insurance since 2007.

Unlike the other GCC countries, healthcare in the UAE is regulated by a hybrid of federal authority, the Ministry of Health and Prevention (MOHAP), and local authorities of two major Emirates that are the Department of Health Abu Dhabi (DOH) and the Dubai Health Authority (DHA).

In the GCC, MOH is the primary provider for healthcare expenditure, variations in the service providers, government and private insurers presents challenges for health data privacy.

Electronic Health Record at a National Level

EHR was introduced as an innovate solution to transition patients’ paper medical records to electronic format. (Al Kiyumi, 2019). This, and other advancements in technology, have increased interest in health information.

In Saudi Arabia, an EHR system has been implemented on a national level. Because the information collected about patients varied from one medical organization to another, the Unified Electronic Health File Project was initiated in 2016. The system allows doctors to view data on patient medications, previous visits, diagnoses and allergies (Saudi National Health Information Center, 2018).

In the same vein, for the Omani health system, the MOH Ministry of Health developed its own tailored system. This proprietary EHR system has moved ahead rapidly to cover all hospitals and healthcare centers governed by the MOH on a national level (Al Kiyumi, 2019). The system is being used across all public healthcare institutions in the country (Al-Gharbi et al., 2015; Khan & Ismail, 2017).

In the UAE, most of the region has adopted well-known American EHR systems and has been profoundly influenced by US and international Health Information Exchange (HIE) models in general. Malaffi Platform is an example of an up and running HIE platform, it caters to patients across the country with both government-based and private hospitals.

In Kuwait, while no national-level EHR is available yet, electronic systems do exist at several institutions. For example, if a patient visits a primary healthcare facility, he or she will have an EHR, and if the same patient is referred to secondary or tertiary healthcare facility, he or she will obtain a second EHR.

Discussion and Recommendations

Health Information use and disclosure is essential to care processes. In this section, the overall similarities and differences within and between the four countries will be discussed.

Use and Disclosure of Health Information

Health information is used for the treatment of patients and continuity of care. Furthermore, all GCC countries use this information for quality management, such as in auditing for regulatory compliance and ensuring that healthcare providers are in compliance with the laws and regulations for healthcare provision. Other very important uses for health information include education and research, healthcare trend analysis, health promotion and public health.

The further major use of health Information in GCC countries is for the purposes of billing and reimbursement. With the advent of health insurance, it has become very important that health information be properly captured and represented through coding standards to support reimbursement. These standards allow for a unified reporting procedure of services to regulatory bodies and resulted in a reduction of redundancy in services, which is clearly visible in UAE healthcare systems in particular.

Access and disclosure policy and practice

All GCC countries follow either a documented manual or guideline concerning uses and disclosures of health information. However, the process of work and the responsible bodies vary, as do concerns over standardization of policies and procedures, documented manual or guidelines for uses and disclosure practices.

Kingdom of Saudi Arabia (KSA)

In KSA, the MOH has policies and procedures that require every HIE meeting point to successfully complete all access control elements conducted by Saudi HIE approved bodies. Access to personal health information through the Saudi HIE systems requires verification of consents managed according to a documented manual that follows the specifications of the Saudi HIE Consent and Access Control Policy (Saudi National Health Information Center, 2016).

With regard to personal health information disclosure and use, the manual mentioned above stipulates that both local Participating Healthcare Subscriber and HIE designated Institutional Review Board (IRB) shall comply with the regulations as presented in the document titled "National Committee of Bioethics Implementing Regulation of Law of Ethics on Living Creatures." Further, this document contains the Law and its regulations that shall apply to any research establishment conducting research on living creatures in the KSA (MOH, Saudi Health Information Exchange Policies version 1.0, 2015). The Saudi Health Information Exchange has to keep a record of all approved and accepted requests for identified information, unidentified health information, anonymized health information, and pseudonymized health information from the Saudi HIE. The record of all approved requests should be reviewed with the same frequency as audit report requirements as specified by the Audit Policy (Saudi National Health Information Center, 2016).

Kuwait

Kuwait does not have specific national law governing personal information privacy. However, the MOH has the policies and procedures governing the use of health information in both hard copy and electronic formats. The Kuwait Medical Records Supervision is the responsible body for preparing policies and procedures regarding HIP at a national level, and all the health care sectors should abide by those policies.

Sultanate of Oman (Oman)

Oman does not have an individual national law governing personal information privacy. The existing laws in Oman are embedded in broader or more general provisions of laws on information privacy. These general privacy laws in Oman do not precisely indicate the policies for information privacy in healthcare. Due to the rapid development in the EHR system in Oman, and the procedures followed in different health care organizations, the privacy policy and procedures at the MOH level are blurry. Healthcare workers are accountable for privacy through codes of ethics, which is considered insufficient (Al Salmi, 2015). However, various health care facilities have created their own policies and procedures in line with international standards to be followed with the EHR system, which involves the need for consent and authorization to release personal health information. The need for a healthcare privacy policy is now evident due to the MOH vision to establish a platform for patients, with health information specialists now able to participate in this process.

United Arab Emirates (UAE)

In the UAE, the MOH has multiple laws to govern the use and disclosure of health information in both paper-based and electronic formats. The UAE Federal Law No.4 of 2016 set the basic regulation for health information use and with the rapid move towards Health Information Exchange, the Ministry of Health and Prevention (MOHAP) issued the Federal Law No. 2 of 2019 on the use of Information and Communication Technology (ICT) in Healthcare. There are also other policies and standards at the local Emirate levels to govern the use of Health Information, such as the Health Information and Cyber Security Standards set by the Department of Health in support of Abu Dhabi HIE Platform establishment, and the Interoperability Standards set by the MOHAP in support of the national HIE platform.

In addition, all healthcare providers (private and governmental) are required to maintain minimum regulations for confidentiality and disclosure of information as stated in the Federal Law No.4 of 2016 on Medical Liability. This specifies disclosure purposes and appropriate procedures to disclose.

The Challenges in GCC Countries

Generally, Islamic counties are viewed as collectivistic cultures (Abu-Saad, 1998). Collectivistic cultures value privacy less than do individualistic cultures. (Petronio, 2002). The lesser emphasis on personal privacy in the collectivistic culture as compared to individualistic societies is due to certain humanitarian concerns which Islam appreciates, provided it is harmless. Culture is identified as an important component of privacy model for protecting patient health information in Islamic countries such as Malaysia (Samsuri et al. 2011), Pakistan (Humayun et al, 2008), Iran (Farzandipour et al., 2010) and Oman (AL Salmi, 2015).

The GCC countries are part of the Islamic world, where people are very close and concerned about each other, so they tend to share their private information with each other. Because of this collectivistic culture, it is an obligation for a community member to visit, ask, and know about people's health problems, even though they are not related to them, but it does not mean that they seek such information for negative designs.

One of the challenges to Health Information Privacy is the cultural context in which the health information is collected and used. Healthcare providers usually experience pressure from the patients' community to release private information. Such community pressure puts the healthcare providers in embarrassing situations, particularly in maintaining the right balance between patient privacy and the community members' satisfaction. This finding broadly supports the work of other studies in this area, which showed that cultural issues in Oman influenced the quality of HIM practices in general and privacy practice in particular (Al Salmi, 2015, Al Kiyumi, 2019). In this regard, the culture interpretation of privacy and confidentiality can give mixed signals. What we consider as confidential or sensitive information varies from one patient to another and even employees governed by the regulations cannot totally put aside their beliefs and cultural norms. In addition, patients have a limited awareness about their right to privacy and do not fully understand the extent of their privilege in this area.

Patients do not really understand the power access to information carries, especially where there is no policy on expiration of consent. There is also the right to NOT disclose, which is rarely used by patients, as they do not fully understand that part of access to their records either. Moreover, there is an 'excess' of trust and confidence among Muslim patients in their healthcare providers' ethics, especially doctors, as they are well respected in Islamic society (Al Salmi, 2015, Humayun et al, 2008, Amin et al, 2013)

Health Information Exchange (HIE)

With the GCC countries embarking on HIE initiatives, many new policies and procedures are being introduced around privacy, security and information disclosure in some countries, such as UAE and KSA. Some of these are replacing previously set policies, thus, it becomes a challenge for some health institutions and HIM professionals to stay up-to-date with standards.

In Oman, the HIE has been started, however, there is a challenge due to the absence of a national law to make healthcare providers accountable for standardized HIP practices (Al Salmi, 2015). In addition, the absence of documented policies and procedures on how patient health information is being collected, held, used and disclosed, as well as patient rights to access and amend their own medical records, is the challenge (Al Salmi, 2015). Moreover, there is a lack of standardization between HIP practices in different health care providers in Oman (Al Salmi, 2015).

In Kuwait, an electronic system is implemented in all primary healthcare facilities. Some secondary and tertiary health care facilities are also using electronic records provided by different vendors, but, so far there is no standardized system. The existence of different systems might be one of the major barriers to the adoption and implementation of a consolidated EHR at the national level. This presents another challenge, in addition to the lack of rules and regulations and a lack of training provided to staff working in the health information management.

Overall, GCC countries share the same systemic challenges to interoperability, despite attempts to address the procedures and other reforms. Most certainly there is a lack of coordination between private and government healthcare facilities around health information management. Furthermore, there is an absence of distinct health information national laws and regulations to govern and set a privacy and security framework in order to facilitate the health information exchange. Moreover gaps between policies and practice may accumulate when a culture of noncompliance persists.

Recommendations

This discussion suggests several general courses of action concerning uses of, access to and disclosure of health information in the GCC countries covered in this case study. The GCC countries can work together to implement such actions with the support of Gulf Health Council.

- Develop HIP regulations, up-to-date policies and procedures for health information management in those countries where policies do not exist or where they are outdated.
- Promote the standardization, transparency, and auditing of the health information at the regional level.
- Ensure the establishment of laws at the regional and national levels and/or national authorities to make healthcare providers accountable for HIP practices.
- Foster privacy awareness for patients and healthcare professionals.
- Organize training programs for healthcare members and establish a monitoring system created for the quality of health information.

Another broad recommendation is that as new staff are on-boarded at healthcare facilities, they be trained in information security, information governance and data quality. Most importantly, they must be empowered with leadership roles and budgets to enforce health information best practices across their organizations and thus avoid security incidents and data breaches, which might incur heavy fines and business interruption.

If such recommendations are considered, HIP best practices can be improved and expenditures reduced. The efforts to adopt these recommendations should be joint efforts across the GCC countries.

Conclusion

The GCC countries (KSA, Kuwait, Oman, and UAE) have invested heavily in the adoption of electronic health records. As with other nations around the world, this presents many challenges regarding information privacy.

As discussed in this case study, nature of privacy can be different in Islamic countries. The cultural and organizational environment must be considered when planning health information privacy policies and laws for GCC countries.

However, as our recommendations point out, standardization of processes including rules and regulations; an increased awareness of the importance of privacy and access to personal information; and training programs for HIM professionals, along with a recognition of the importance of their roles will be key to protecting information privacy in the GCC region.

About the Authors

Salim Al Salmi, PhD, MSc, PGCert Med Edu, RHIT, CHIM is the associate dean for HIM program in Oman College of Health Sciences. He has 29 years of experience in HIM. He is the national consultant and leader for the development of the HIM education and practice in Oman. https://www.linkedin.com/in/salim-al-salmi-phd-rhit-chim-pg-edu-a2262020

Raniya Al Kiyumi, PhD, MSc HIM, GradCertEd. is a qualified HIM professional with several years of experience working in service and academia. She is an IFHIMA associate member and a global member of AHIMA. https://www.linkedin.com/in/ranalkiyumi/

Hussein Albishi, BSc HIM, CHIM is the consultant for the HIM and clinical coding, Vision Realization Office, Ministry of Health, KSA. He is a part time Lecturer, Almaarefah University, Riyadh, KSA. He is the president of SHIMA and Board Regional Director, IFHIMA, East Mediterranean 2016-2019 and 2019-2022. https://www.linkedin.com/in/hussein-albishi-bsc-him-chim-68266a18

Ahmed Al Hatlan, BSc, MS, CHIM, CPHIMS is the General Director of medical coding at National Casemix Centre of Excellence, vision realisation office, Ministry of Health, KSA. He is the Vice President for SHIMA. He is active member in different national and international committees. http://linkedin.com/in/ahmed-alhatlan-33301a42

Safia M. Dawood, MSc CS, HINF, CPHIMS is the health information system program director, Almaarefa University, Riyadh, KSA. She is the academic quality coordinator and has academic and research experience in health informatics research at the University of Almaarefa, KSA. https://linkedin.com/in/safia-dawood-5849501b3

Haya Alkhatlan, PhD, MSc is assistant professor in HIM program, college of health sciences, Kuwait. She has more than 25 years of academic experience. She is an active member at AHIMA, FHIMA, and Kuwait Health Informatics Association. https://www.linkedin.com/in/haya-alkhatlan-18140269

Fatima Al Baloushi, BSc, MQM is the Strategy and Performance Management Director at Al Ain Hospital in UAE. Fatima has a total of 14 years' experience in the HIM, Operations, and Strategy Management fields. She is also an active member in different UAE based committees and being a member at the Global Healthcare Workforce Council. https://www.linkedin.com/in/fatima-albloushi-b9744aaa

Osama El-Hassan, MSc, PhD is a Health Informatics Specialist at Dubai Health Authority, UAE. He is also the Vice President of UAE Health Informatics Society and the co-founder & coordinator of the GCC Taskforce on Workforce Development. He contributes to academia through his adjunct lecturer role at Hamdan Bin Mohammed Smart University. https://www.linkedin.com/in/osama-elhassan-7507a91b

Endnotes

Abu-Saad, I. (1998). Individualism and Islamic work beliefs. Journal of Cross-Cultural Psychology, 29, 377–383. http://dx.doi.org/10.1177/0022022198292007

Al Kiyumi, R. (2019). A Road Map for Health Information Management in Oman. PhD thesis, Queensland University of Technology. https://eprints.qut.edu.au/130603/9/Raniya%20Humaid%20Matar%20Al%20Kiyumi%20Thesis.pdf

Al Salmi, S. (2015). Health Information Private Policy and Practice in Oman: A Health Information Management Perspective. [Unpublished PhD thesis]. Swansea University, Swasea.

Al-Gharbi, K., Gattoufi, S., Al-Badi, A., & Al-Hashmi, A. (2015). Al-Shifa Healthcare Information System in Oman: A debatable implementation success. Electronic Journal of Information Systems in Developing Countries, 66(1), 1–17. https://doi.org/10.1002/j.16814835.2015.tb00471.x

Al-Hujurat: 12. The Holy Qur'an, Al-Hujurat: 12 (49:12).

Farzandipour, M., Sadoughi, F., Ahmadi, M., & Karimi, I. (2010). Security requirements and solutions in electronic health records: lessons learned from a comparative study. Journal of Medical Systems, 34, 629–642. http://dx.doi.org/10.1007/s10916-009-9276-7

Khan, S., & Ismail, M. (2017). Al-Shifa: Case study on Sultanate of Oman's National Healthcare Information System. Indian Journal of Science and Technology, 10(17). doi:10.17485/ijst/2017/v10i17/113060

Petronio, S. (2002). Boundaries of privacy: Dialectics of disclosure. Albany: State University of New York Press.

Samsuri, S., Ahmad, R., & Ismail, Z. (2011). Towards implementing a privacy policy: An observation on existing practices in hospital information systems. Journal of e-health Management, 10, Article No. 345834. http://dx.doi.org/10.5171/2011.345834

Saudi National Health Information Center. (2016). Enabling Standards-Based eHealth Interoperability, Saudi Health Information Exchange Policies, Version 1.0. Kingdom of Saudi Arabia. Retrieved from https://nhic.gov.sa/eServices/STD/Documents/IS0303 Saudi Health Information Exchange Policies v1.0.pdf

Saudi National Health Information Center. (2018). The Shared E-Health File. Retrieved from nhic.gov.sa: https://nhic.gov.sa/en/Initiatives/Pages/default.aspx

Weber, A.S. Cloud Computing In Education In The Middle East And North Africa (Mena) Region: Can Barriers Be Overcome? International Scientific Conference ELearning and software for education Bucharest, aprtil 28-23,2011.

Department of Health Policy on The Abu Dhabi Health Information Exchange April 2020

Dhabi's Health Information Exchange Looks at Privacy from a Global Perspective, Journal of AHIMA, https://journal.ahima.org/abu-dhabis-health-information-exchange-looks-at-privacy-from-a-global-perspective/?unapproved=321075&moderation-hash=9237a6080d41ebf6ff70a97342e80fa9#comment-321075, accessed on 29/05/2020

Emirate of Abu Dhabi Law No. (23) of 2005 on Health Insurance in the Emirate of Abu Dhabi (Health Insurance Law) and Chairman of the Executive Council Decision No. 25 of 2006 Issuing the Implementing Regulations of the Health Insurance Law (Implementing Regulations)

Health Authority – Abu Dhabi, General Confidentiality Policy (P30/60/ 012)

Health Authority – Abu Dhabi, Health Information and Cyber Security Standards 2019

Health Authority – Abu Dhabi, Patient Rights and Responsibilities

Ministry of Health. (2013, March 6). National E- Health Strategy . Retrieved from www.moh.gov.sa: https://www.moh.gov.sa/en/Ministry/nehs/Pages/Ehealth.aspx

Ministry of Health. (2015, Februrary 22). SaudiHealth Information Exchange Policies version 1.0. Retrieved from www.moh.gov.sa: https://www.moh.gov.sa/en/Ministry/ehealthstd/Documents/eHealth%20Standards%20Fi les/Policies/IS0303%20Saudi%20Health%20Information%20Exchange%20Policies%20 v1.0.pdf

Ministry of Health. (2017, March 21). Healthcare Transformation Strategy. Retrieved from www.moh.gov.sa: https://www.moh.gov.sa/en/Ministry/vro/Documents/Healthcare-Transformation- Strategy.pdf

Ministry of Health. (2018, September 1). Digital Health Strategy Update. Retrieved from www.moh.gov.sa: https://www.moh.gov.sa/Ministry/vro/eHealth/Documents/MoH-Digital-Health-Strategy- Update.pdf

Ministry of Health. (2019, August 29). MOH News. Retrieved from www.moh.gov.sa: https://www.moh.gov.sa/en/Ministry/MediaCenter/News/Pages/News-2019-08-29- 002.aspx

The National Medical Records Standards Committee - the Terminology, Interoperability and Integration Standards for Health Information Exchange March 2020

United Arab Emirates Federal Law No (2) of 2019 The Use of Information and Communications Technology (ICT) in Health Care

United Arab Emirates Federal Law No(4) of 2016 on Medical Liability

United Arab Emirates Federal Law No. (1) of 2006 on Electronic Commerce and Transactions and Federal Law

General Data Protection Regulation of the European Union Reaches Far Beyond Europe

Lorraine Fernandes
RHIA

Angelika Haendel
MA, B.Sc.

Introduction

The General Data Protection Regulation (GDPR) of the European Union (EU) came into force on May 25, 2018. This new regulation, which replaces the 1995 Data Protective Directive 95/461/EC, was formulated over four years and ratified in May 2016 by the EU Parliament.[1] During the four-year period 2012-2016 the impact of the proposed regulation with regard to key stakeholders was explored in detail. GDPR encompasses all data captured by any organization anywhere in the world, including all healthcare organizations, related to a person who is an EU resident, also known as a data subject. Many components of GDPR address the privacy of the data subject's information.

The purpose of the GDPR is to provide standardized data protection laws across the EU. GDPR makes it easier for an EU citizen to understand how their data is being used and also to make a complaint about its misuse.

The GDPR has significant implications for privacy regulations of healthcare data. The International Federation of Health Information Management Associations (IFHIMA), a forum that brings together national organizations committed to the improvement in the use of health records, health information management and information technology, considers this a significant regulation for its members and all health information management professionals and the nations where they work. And while there have been many documents and opinions written on this regulation, IFHIMA feels it is worthy of focus in this case study.

A short discussion of select components of GDPR's healthcare applicability, and key terms, follows in this case study.

Background

GDPR was intended to advance the harmonization of European data protection laws and to address the requirements of the changing nature of today's digital environment. A key driver for the GDPR was the modernization of the 1995 Data Protective Directive (DPD), as the internet was in its infancy when DPD was developed. The 99 articles of GDPR address the requirements and remedies. A European Data Protection Board will ensure consistency in implementing GDPR across the member states.

While data protection principles and laws have existed for 30+ years in European nations, a key new requirement is that compliance with these long-standing principles **must be proven**. This means that the documentation effort will increase significantly compared to before GDPR. While GDPR is new, the principles of data processing previously recognized by national legislatures of the EU countries will continue to exist, but GDPR will be the higher authority and take precedence.

Discussion

The important opening sections of the 99 articles of GDPR articulate the core purpose - that is, protecting the processing of EU persons' data with the intent to harmonize the associated processing functions across EU member states. Below are some key sections that are particularly relevant to healthcare. For illustrative purpose, we have bolded key phrases.

- The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that **everyone has the right to the protection of personal data concerning him or her.**

- The principles of, and the rules on the protection of natural persons with regard to the processing of their personal data should, **whatever their nationality or residence**, respect their fundamental rights and freedoms, in particular their right to the protection of personal data. This Regulation is intended to contribute to the accomplishment of an area of freedom, security and justice and of an economic union, to economic and social progress, to the strengthening and the convergence of the economies within the internal market, and to the well-being of natural persons.

- Directive 95/46/EC of the European Parliament and of the Council (4) seeks to **harmonize** the protection of fundamental rights and freedoms of natural persons in respect of **processing activities** and to ensure the free flow of personal data between Member States.[2]

Articles 5-11 of the GDPR Address the Core Data Principles of GDPR

The persons responsible (i.e. data protection officer through hospital management, health information management) must guarantee compliance with these core principles of GDPR:

- Purpose limitation. Processing of information must be limited to the use for which is was originally collected as part of informed privacy consent. Internet users will recognize the plethora of new internet cookies notices and privacy policy updates attributed to this principle.

- Data minimization. Data should be processed and used to the minimum necessary to achieve the original intent.

- Accuracy. Personal information collected and used must be kept current, and be accurate.

- Integrity and confidentiality. Data must be secured against unlawful and unauthorized use.

- Storage limitation. Data must be stored only as long as is necessary to achieve the original intent. Individuals may request that their PHI be erased from the organization's data. This is often referred to as the right to be forgotten.

- Fair and transparent. Organizations must be fair and transparent to the consumer about how their personal data is used.

These tenets are not unlike the longstanding Caldicott Principles of the United Kingdom, as well as the Principles of Fair Information Practice (FIPPS) of the United States and the Organization for Economic Co-operation and Development (OECD) Privacy Framework.[3] These three examples offer policy makers guidance in crafting stewardship frameworks for governing health and other sensitive information in physical or digital form.

GDPR is often viewed as the new baseline for advancing privacy practices worldwide. For example, **privacy breach notification must be made to the regulator within in 72 hours**. Privacy professionals are considering that this may be the new de facto notification standard for other legislation which currently use 'as soon as possible' as their mandatory notification time periods.

The GDPR also defines three types of health data that require special protection: data concerning health, genetic data, and biometric data. These are classified as sensitive personal data, and the regulation generally prohibits any kind of processing for these unless explicit consent is given or very specific conditions are met.[4]

Below are examples of the practical aspects of GDPR as they pertain to compliance in healthcare.

List of Processing Activities

Hospitals must keep a record of processing activities. The record or "procedure directory" of processing activities, however, goes beyond the requirements of national directory of data processing procedures, more information must be given about the processing activities. Controllers, as defined by the GDPR in the context of data controllers, must ensure that the processors have well documented data processing rules including data subject rights and security of processing activities. This helps to prevent 'supply chain compromise,' where a vendor's security compromises the patient/client sensitive health information. Each organization must designate the individual who is responsible for this control function.

Rights Concerned

The existing rights of data subjects (right of access, rectification, blocking, deletion) still exist from previous regulations. However, there are also changes here. For example, the legal basis of the processing must be communicated prospectively, as well as the storage period or when the data will be deleted.

Security of Processing

A major topic of the GDPR is the safety of processing. The GDPR follows a risk-oriented approach, whereby the risk for the person/data subject concerned is always addressed. Predominantly three regulations are to be considered here:

1. Data protection by design/default (Art. 25 GDPR)

Privacy by design/by default concerns both technical and organizational components, i.e. requirements for IT systems as well as organizational processes. The requirements must be taken into account both during planning and during processing. Since the term "processing" in Art. 4 No. 2 GDPR is very broadly defined, the measures must be guaranteed for the entire life cycle of the data. Since the requirements regarding the suitability of the measures can change over time, Privacy by Design/Default is not a one-off process, but rather a continuous process.

2. Security of processing (Art. 32 GDPR)

The GDPR requires the introduction of an IT security management system. Art. 32 GDPR stipulates that appropriate technical and organizational measures must be taken to ensure a level of protection appropriate to the risk, taking into account the state of the art, the implementation costs, the nature, scope, circumstances and purposes of the processing, as well as the different probability of occurrence and severity of the risk to personal rights and freedoms. The effectiveness of the measures taken must be regularly reviewed and evaluated.

3. Data protection impact assessment and Prior Consultation (Art. 35/36 GDPR)

A data protection impact assessment is intended to help minimize risks in cases where processing is likely to pose a high risk to the rights and freedoms of individuals and to provide third parties with a clear picture of how data controllers deal with these risks by outlining the measures taken to reduce the risks.

An impact assessment is an essential first step as organizations around the globe determine if GDPR applies to them.

Data Subject Rights

Rights are explicitly stated in Chapter 3, Articles 12-23 of GDPR.[5] These include

- Right to information
- Right to access
- Right to rectification
- Right to withdraw consent
- Right to object
- Right to object to automated processing
- Right to be forgotten
- Right for data portability

These rights are consistent in large part with long-established policies and practices that emanated from the 1995 Data Protective Directive. Generally speaking, the data subject can access, review, inspect and request changes to their data. The rights give natural persons (data subjects) far more insight and control over who sees and uses their personal information. Rights requests must be made in writing by the data subject or the subject's legal representative.

Perhaps most challenging to many data processing stakeholders and healthcare in particular is the "right to be forgotten". The data subject can request to have their personal information removed from the processor and the controller's data holdings. While debated in all circles, this requirement is particularly challenging in healthcare since removing or redacting data can be very onerous, and sometimes contrary to the initial data collection. And, this concept poses a particularly vexing issue for healthcare since a longitudinal patient record is created to promote patient safety, cost effective care delivery, and informed decision making. Removing any portion of a record may render the record incapable of supporting these common goals, and could compromise patient safety and clinical decision making.

GDPR Beyond the EU

As explored in the body of this whitepaper, this new privacy regulation is having a profound impact on data privacy policies, regulations, and processes around the globe. Nations outside of the EU are reviewing their privacy laws to maintain its adequacy status[6] – that is, "how the EU determines if a non-EU country has an adequate level of data protection." Adequacy status of a nations' private sector law with the EU allows for the transfer of European citizens' personal data to that nation. This has, potentially, a significant impact to economics, trade, and services between EU and non-EU nations.

The adequacy status is a mechanism for compliance with the data protection requirements when transferring data from the EU to another nation. In the absence of an adequacy status, nations may need to consider alternate legislation to enable the transfer of data between EU and non-EU nations.

While in healthcare, data transfer between nations is not common, in business and commercial operations it happens all the time – consider banking or retail as a common examples of frequent data transfer among nations.

GDPR Penalties for Non-Compliance[7]

Compliance with the Global Data Protection Regulation is required in all segments of a global society and economy when interacting with an EU person's data.

There are ten criteria used in determining the economic penalty for non-compliance with GDPR, including, for example, the nature of the infringement, the intent and data type. The EU individual member state authority (where the complaint was lodged) evaluates the complaint and determines the fine.[8]

The highest discretionary penalties for non-compliance are:

1. Up to €10 million, or 2% annual global turnover – whichever is higher.

2. Up to €20 million, or 4% annual global turnover – whichever is higher.

With GDPR, the EU can levy stiff penalties for non-compliance. It is wise for EU and non-EU nations and organizations to be well informed with this regulation.

Conclusion

The purpose of the GDPR is to provide standardized data protection laws across the EU. GDPR makes it easier for an EU citizen to understand how their data is being used and also to make an inquiry or complaint about its use or mis-use. While the key focus for GDPR is data residing within the EU nations, this regulation has global implications.

Processing of data, including healthcare data, for EU persons must be fair, transparent, and lawful. These three data drivers sound simple, but implementing them can be costly, complex, and sometimes confusing. To aid in regulatory compliance the EU has published many documents providing guidance.

GDPR is having a profound impact on privacy and data governance. Healthcare organizations in non-EU nations should review their data management and privacy breach management processes to ensure that they meet the GDPR requirements, including breach reporting timelines when the breach includes the personal health information of EU citizens.

Nations who are developing their initial regulations or are updating existing regulations are wise to consider GDPR as a framework.

IFHIMA encourages all readers and, especially health information management professionals, to understand the core principles of GDPR, as they may serve as a model for healthcare data governance and privacy in their country, state or region.

About the authors

Lorraine Fernandes, RHIA serves on the IFHIMA Board of Directors as President (2019-2022) and Liaison to IFHIMA Privacy Workgroup. Lorraine is Principal at Fernandes Healthcare Insights, a data governance focused practice. https://www.linkedin.com/in/lorraine-fernandes-07723b1/

Angelika Haendel, MA, B.Sc., Clinical Documentation at the University Hospital of Erlangen, Nuremberg, Germany, is the Past President of IFHIMA and Board Member of the German Association of Medical Documentation and Health Information Management (DVMD). As Board member of IFHIMA and DVMD, she brings together HIM associations from Europe, Middle East, Asia, and The Americas. She serves as co-chair of the EFMI working group HIME, and has been serving on AHIMA's Global Health Workforce.
https://de.linkedin.com/in/angelika-haendel-0a44aba

Endnotes

1. *EUGDPR.ORG https://eugdpr.org/*
2. *REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1528874672298&uri=CELEX%3A32016R0679*
3. *The OECD Privacy Framework, http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf*
4. *Trend Micro, Patients and Privacy: GDPR Compliance for Healthcare Organizations, June 2018. https://www.trendmicro.com/vinfo/dk/security/news/online-privacy/patients-and-privacy-gdpr-compliance-for-healthcare-organizations*
5. *EU GDPR Academy, Data Subject Rights According to GDPR. https://advisera.com/eugdpracademy/knowledgebase/8-data-subject-rights-according-to-gdpr/*
6. *European Commission, Adequacy decisions. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en*
7. *GDPR Non-compliance penalties. Web learning resource for the EU General Data Protection Regulation. ttps://www.gdpreu.org/compliance/fines-and-penalties/*
8. *GDPR EU.ORG, Fines and Penalties. https://www.gdpreu.org/compliance/fines-and-penalties/*

References

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 - On the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1528874672298&uri=CELEX%3A32016R0679#document1

Accountability on the ground: Guidance on documenting processing operations for EU institutions, bodies and agencies

https://edps.europa.eu/data-protection/our-work/publications/guidelines/accountability-ground-provisional-guidance_en

Myth busting: General Data Protection Regulation, Fact Sheet January 2019 https://ec.europa.eu/commission/sites/beta-political/files/100124_gdpr_factsheet_mythbusting.pdf.

References: all websites accessed March 26, 2019.

Health Care Privacy: An Indian Scenario

Dr Sabu Karakka Mandapam

Dr Rajesh Kumar Sinha

Introduction

An Overview of the Healthcare System and Privacy in India

The Indian healthcare system is unique in its blend of modern medicine, various Indian traditional systems of medicine and homeopathy. People's access to and use of multiple system of medical facilities for their healthcare presents particular challenges for privacy, confidentiality, and patient rights. In India, people accessing health care services at any level; primary, secondary, tertiary or speciality care are vulnerable to privacy breaches of their protected health information due to lack of strong data protect and privacy regulations. [1] The integration of Information Technology in the healthcare delivery system has enabled more healthcare facilities to connect and share patient data for effective healthcare management. [2] Widespread adoption of Electronic Medical Records (EMR) and a large amount of patient data stored in the EMR is also a threat to privacy of data at different levels.[3,4] An Indian citizen can access various information through a formal request to authorities as per Right to Information (RTI) Act of 2005; however, this has led to misuse. [5] There have been incidences reported on leakage of a huge amount of patient data from EMRs, some from laboratory settings. [6] On the other hand, in recent times there has been an increase in awareness among patients on protection of their personal information available to the health care providers. [7] The complex legal and regulatory frameworks governing various stakeholders in the healthcare sector are inadequate to address privacy issues at different levels of the health care delivery system. The practice of medicine integrated with teaching and research in the realms of modern and traditional medical system is another area of concern in terms of patient privacy. India needs stronger reforms and regulatory mechanism put into practice to address the overall privacy aspects of patients.

Problem Statement/Background

Provision of Protecting Privacy under Code of Ethics of Modern and Traditional Medicine in India

Healthcare Privacy is not only a concern of the providers and patient, but also to the statutory and regulatory bodies, which are associated with the provision of health care service to the individual and the community. These bodies are responsible for the formulation of the code of ethics and to ensure that the guidelines are accepted and practiced by all the stakeholders. In India, the practice of modern medicine is regulated under the Medical Council of India (MCI), Dental Council of India (DCI), Indian Nursing Council (INC) whereas the traditional medical practices fall under the guidelines of the Ministry of AYUSH (Ayurveda, Yoga, Unani, Siddha and Homeopathy).

These statutory bodies have formulated various specific code of ethics and guidelines for the protection of healthcare data and to maintain privacy during and after the patient care. These statutory guidelines are enforced and applicable to all those who are the members of the healthcare professions. The code of ethics formulated by Medical Council of India [8], Dental Council of India [9] and Ministry of AYUSH [10] states that the medical and dental

professionals should never reveal the information shared by the patient without getting the informed consent from the patient. They further stated the revelation without the consent is only when such revelation is required by the law of the state.

The Indian Nursing Council also directs the nurses to respect the individual's right to privacy of their personal health information and maintains confidentiality of privilege information except in life threatening situations and use discretion in sharing information. The nurses should take informed consent and maintains anonymity in using such information for quality assurance/academic/legal reasons. For digital data, the nurses should limit the access to all personal records written and computerized to authorize persons only. [11]

Statutory and Legal Framework in Protecting Privacy in India

In spite of having many robust healthcare policies, the Indian legal framework governing healthcare delivery and management is not effectively implemented across the country. Protection of patient data and privacy is one of the neglected areas in this perspective. With a 1.3 billion population, the Indian healthcare system generates around 1021 gigabytes of patient data in a day through several platforms at different levels. [12] In addition, India does handle a large scale of health Information of patients from other countries through Business Process Outsourcing activities and laws, like General Data Protection Regulation (EU GDPR) are also putting a lot of pressure on India to take serious measures on the protection and privacy of healthcare data. [13] Historically, India has passed several legislative Acts in healthcare and many of these laws, are attributed to privacy and protection of data as well. These Acts are listed below:

- Epidemic Diseases Act, 1897
- Mental Health Act, 1987
- Medical Termination of Pregnancy (MTP) Act, 1971
- Pre-Conception and Pre-Natal Diagnostic Techniques (Prohibition of Sex Selection) Act, 1994
- Insurance Regulatory and Development Authority Health Services Regulations, 2001
- National Policy for Persons with Disabilities, 2006

Electronic Health Records Standards 2016 for India and the proposed Digital Information Security in Healthcare Act are expected to address the patient data privacy and protection of health information to a larger extent in this evolving digital era.

Discussions and Recommendations

Resolution of Healthcare Privacy Beaches in India: Case Reviews

This section deals with the cases of healthcare privacy disclosure and breaches and their remediation by the Apex Court of India. [14]

Case Title	Privacy Breach Details	Remediation
Neera Mathur v. Life Insurance Corporation of India, 1992, AIR 392, 1991 SCR Supl. (2) 146	Disclosure of personal health information and wrongful termination. The disclosure of menstrual cycle, conception, pregnancy etc. by the women applicant at the time of joining Life Insurance Corporation Ltd. India.	Supreme Court ordered the corporation to delete such details from the application as these held to be intrusive, embarrassing and humiliating.
Selvi v. State of Karnataka,2010. 7 SCC 263	Violation of right to privacy during the Narco analysis by physically restraining the subject to a location and intruding into his/her mental privacy.	Supreme Court directed to limit the interrogation only to the case and avoid any cruel or unhuman treatment to the subject.
Raghunath Raheja vs. Maharashtra Medical Council, 1996, AIR 1996 Bom 198	A case of privacy breach where the near relative demand for patient's medication records from the hospital without the permission and authorization of the patient.	Bombay High Court made it mandatory for the hospital to furnish the case sheet of the patient to his/her near relative on demand. This judgement fails to provide any rights to the healthcare facility to protect the healthcare privacy breach.
Surjit Singh Thind. V. Kawaljit Kaur. AIR 2003 P H 353	Husband demand for the medical examination about the virginity of his wife to prove the consummation of marriage. This act itself is a violation of right to privacy under article 21 of Indian Constitution.	The high court of Punjab and Haryana held this act a violation of right to privacy and dismissed the case.

Recommendation to Strengthen Healthcare Privacy

As stated, India has the statutory and legal framework to protect the unethical practice in healthcare, but no guidelines or framework exists that specifically address the privacy of healthcare and healthcare data. A large percentage of the population is unaware of their right to health and right to privacy and not much effort has been taken by the local, regional and national health authority to create awareness among the population about ethical dissemination and use of healthcare data by the stakeholders. Due to large geographical area and the availability of a wide variety of healthcare service providers and centres, the patients are managed in an environment where they interact with multiple healthcare workers from students and trainees to the trained and qualified professionals. This vulnerable environment is a threat to patient privacy in many instances. The information technology application used in hospitals does not comply with the uniform global standards, especially related to the sharing of patient data between different providers and stakeholder resulting in breach of patient privacy.

Being the second most populated country in the world, the Indian healthcare system needs:

- Stringent law and statutory framework for addressing the privacy of patients in all aspects including the implementation of information technology application.
- More effective education and awareness program on privacy for both healthcare providers and patients.
- A controlled environment at all levels of healthcare facility to protect the privacy of the patient and the dissemination of healthcare data.
- Advocacy groups to monitor and address the issues pertaining to healthcare privacy on a timely basis.
- More effective curriculum and training components for healthcare programs to inculcate and promote the culture of protecting the patient privacy.

Conclusion

The healthcare system in India is a unique. A variety of healthcare data is stored in manual and digital platforms at different locations. Managing data in compliance with the existing privacy and confidentiality regulation is a challenge due to lack of specific guidelines and commitment of healthcare professionals and providers. This exposes the demand for a strong regulatory mechanism to strictly implement and monitor the privacy and confidentiality aspects. This could be achieved by educating healthcare providers about their duties towards the protection of patient data and the public about their right to privacy. The Government of India is in the process of implementing stringent regulations to address the privacy and confidentiality aspects which would change the current scenario of managing, sharing and protecting healthcare data.

About the authors

Dr. Sabu Karakka Mandapam is a Professor of Health Information Management and an Associate Dean, Manipal College of Health Professions, Manipal Academy of Higher Education, Manipal, India and IFHIMA Privacy White Paper Working Group Member.

Dr Rajesh Kumar Sinha is an Associate Professor and Head, Dept. Health Information Management, Manipal College of Health Professions, Manipal Academy of Higher Education, Manipal, India and IFHIMA Privacy White Paper Working Group Member.

References

Abdul Rahim Fiza, Salahuddin Lizawati, Ismail Zuraini, Samy Ganthan Narayana. Safety and Privacy Issues of Electronic Medical Records. Indian Journal of Science and Technology. 2016 Nov; 9(42). Available at URL. http://www.indjst.org/index.php/indjst/article/view/100811/74918

R K Gorea. Legal Aspects of Telemedicine: Telemedical Jurisprudence. JPAFMAT. 2005; 5 (1). Available at URL. http://medind.nic.in/jbc/t05/i1/jbct05i1p3.pdf

Economic Law Practice. Data Protection and Privacy Issues in India. 2017 Sep. Available at URL. https://elplaw.in/wp-content/uploads/2018/08/Data-Protection-26-Privacy-Issues-in-India.pdf

Nimisha Srinivas, Arpita Biswas. Protecting Patient Information in India: Data Privacy Law and Its Challenges, NUJS Law review, Rev. 411, 2012. Available at URL. http://docs.manupatra.in/newsline/articles/Upload/B3C7F081-838F-489F-9F77-AF1E209C26F8.pdf

N N Mishra, Lisa A Parker, V L Nimgaonkar, S N Deshpande. Privacy and the Right to Information Act, 2005. Indian J Med Ethics. 2008; 5 (4): 158-161.

Akhil Deo. Without Data Security and Privacy Laws, Medical Records in India are Highly Vulnerable, The Wire. 2017 Jan. Available at URL. https://thewire.in/law/without-data-security-and-privacy-laws-medical-records-in-india-are-highly-vulnerable

PwC. An overview of the changing data Privacy Landscape in India. Jan 2018. Available at URL. https://www.pwc.in/assets/pdfs/publications/2018/an-overview-of-the-changing-data-privacy-landscape-in-india.pdf

Indian Medical Council (Professional Conduct, Etiquette, and Ethics) Regulation 2010. Available at URL. https://www.mciindia.org/documents/rulesAndRegulations/Ethics%20Regulations-2002.pdf

Dental Council of India Regulation. Available at URL. http://www.dciindia.gov.in/Rule_Regulation/Gazette_Notification_reg_DCI_Revised_Dentists_Code_of_Ethics_Regulations_2014_27.06.2014.pdf

AYUSH - Professional Conduct, Etiquette, Code of Ethics Regulation. Available at URL. http://ayush.gov.in/sites/default/files/8208071887-Professional%20Conduct%20Etiquette%20and%20Code%20of%20EthicsRegulations%20 1982%20%208.pdf Code of Ethics for Nurses in India. Available at URL: http://hmis.ap.nic.in/APNMC/pdfs/ethics.pdf

Express Healthcare. Big Data Analytics and Indian Healthcare. 2019 Jan. Available at URL. https://www.expresshealthcare.in/features/big-data-analytics-and-indian-healthcare/162330/

Roedl & Parnter. Indian Data Privacy Laws and EU GDPR. 2018 May. Available at URL. https://www.roedl.com/insights/india-eu-gdpr-data-privacy-law

Vaz, Natasha, Health Privacy in India: A Legal Mapping. 2014. University of Amsterdam, Amsterdam Privacy Conference 2012 (APC 2012). Available at SSRN: https://ssrn.com/abstract=2457959

Developing a Global Standard for Health Information Privacy Workforce Education

Ok Nam Kim
PH.D., Health Management

Korea

Introduction

Addressing the Need for Privacy Education and Development of Educational Programs

The expanding adoption of health information technology (HIT) including the use of the electronic health record (EHR) systems necessitates a new understanding of health information privacy concerns. Both the increasingly legislated environment around privacy and the increasing need for information sharing between patients, providers, payers, researchers, and administrators contribute to the growing need for information privacy education. In spite of increasing awareness of and sensitivity to patient privacy, until recently, there have been no guidelines or standardization for education for privacy of the healthcare information within healthcare organizations.

The Republic of Korea (South Korea) healthcare field has been protecting patients' healthcare information in accordance with domestic regulations and laws. Since 2010, the Korean Health Information Management Association (KHIMA) research team has participated in the development of patients' privacy education programs for healthcare organizations. In accordance with the Korea Personal Information Protection Act, KHIMA has been conducting the privacy education for Health Information Managers and health organizations' employees.

Discussion and Recommendation

There are various programs on privacy education that exist today in developed countries. Developing countries that are implementing EHRs and mobile health (mHealth) applications also recognize the need to address concerns with protecting patient privacy in a consistent manner. However, some have yet to establish privacy education programs. The International Organization for Standardization's (ISO) Technical Committee (TC) on health informatics can provide a roadmap for countries needing guidance in the area of privacy education.

ISO/TC 215

ISO TC 215 works on the standardization of Health Information and Communications Technology (ICT), to allow for compatibility and interoperability between independent systems. Wikipedia https://en.wikipedia.org/wiki/ISO/TC_215

In October 2013, the KHIMA research team proposed to the ISO TC215 an international standard document which was developed based on Korean educational experiences. The first edition is entitled ISO TR 18638- Guidance on Health Information Privacy Education in Healthcare Organizations was published in 2017 by the ISO Technical Committee ISO TC215 Health Informatics.

Introduction of ISO TR 18638

The ISO TR 18638 document for privacy education is based on international guidelines for information protection, including the Organization for Economic Cooperation and Development (OECD) Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data; United Nations Guidelines for the Regulation of Computerized Personal Data Files; European Union Data Protection Directive (also known as Directive 95/46/EC); and the Asia-Pacific Economic Cooperation (APEC) Privacy Framework. Basic educational content specified in the document was developed accordingly with the principles formulated in these guidelines.

- Purpose: The ISO TR 18638 document describes the essential educational components recommended to ensure health information privacy in a healthcare organization. This document describes the concepts of health information privacy, the components of a privacy education program for healthcare organizations and basic health information privacy educational content that can be applied to various jurisdictions.[1]

- Scope: The ISO TR 18638 document specifies the essential educational components recommended to establish and deliver a privacy education program to support information privacy protection in healthcare organizations. The primary users are those responsible for planning, establishing and delivering healthcare information privacy education to a healthcare organization.[2] The components of privacy education are within the context of roles and job responsibilities. The organization is responsible to define and apply privacy protection policies and procedures and, in turn, ensure that all staff in the healthcare organization understands their privacy protection responsibilities.

The ISO TR 18638 describes:

- The concept of information privacy in healthcare;

- The challenges of protecting information practices in the healthcare organization;

- The components of a healthcare information privacy education program;

- The basic health information privacy educational content.[3]

Contents: ISO TR 18638 document consists of the main content and several educational program samples, making it available and useful as a privacy educational content for HIM's practices and healthcare institutions worldwide.

It is the responsibility of the adopting healthcare organization to define and apply best practices on patients' privacy protection, and to ensure workforce members understand their privacy protection responsibilities. Privacy education and other administrative safeguards such as patient rights on personal health information, privacy breaches, and other topics-within the context of roles and job responsibilities, need to be included in a proper educational program on privacy of health information.

The health information privacy protection program at a healthcare organization should enable personnel to:

1. Understand the importance of privacy and confidentiality of PHI and their relationship to information security in a continually changing healthcare environment
2. Understand privacy legislation, policies, principles, and practices of applying those within an organization
3. Understand their roles in protecting patient privacy when managing patient information and the consequences for violations
4. Recognize potential threats to patient privacy, as well as understand risk mitigation approaches
5. Acquire knowledge of legal, administrative, technical, and physical safeguards
6. Learn effective approaches for protecting patient privacy in relation to patient information
7. Understand the behaviors required to deal with personal and sensitive information

The targeted audience is divided in to six groups based on the role and responsibilities within an organization. They include:

1. Health professionals (clinicians)
2. Health information managers
3. Administrators
4. IT personnel
5. Researchers
6. Other personnel that comes in contact with healthcare information, such as pastoral workers, counsellors, or contractors

An additional educational program is recommended for patients, their family and/or representative and caregivers.

ISO TR 18638 will be helpful for healthcare organizations that are implementing their own privacy protection practices and procedures. It will contribute to overcoming diverse variation between countries in the context of legislation and culture on protecting Personal Health Information (PHI). Additional efforts are needed to standardize the development and delivery of privacy educational programs across the globe, to tailor these competencies to roles and responsibilities of the healthcare workforce, country-specific regulations, and jurisdictional and cultural differences in the management of sensitive patient health information.

Conclusion

In my experience, many countries and healthcare organizations will have different types of rules and requirements, so it will be necessary to develop appropriate privacy educational programs for each situation. Developing a privacy educational program for a country or institution should start with a precise understanding of their situation to address the country's legal requirements. We, the research team, have studied the guidelines, regulations, and laws of other countries and international standard documents and have developed the ISO TR 18638 with reference to the content.

Health Information Managers who wish to act as privacy leaders must have a rich knowledge of various legal requirements and health field environments, and must take the opportunity to participate in the information management committee of their country or healthcare organization. For the HIM expert, this will be a sure way to expand the scope of activities.

The HIM practitioner of healthcare institution should have the proper knowledge and ability to establish the privacy educational plan and to carry out the program as the secretary role of the medical information committee. To do this, HIM professional in all countries are encouraged to participate in leading the education programs, and study with interest and stay abreast of new information technologies and changing trends.

About the author

Oknam Kim, Ph.D. Health Management, KHIMA, is an IFHIMA Privacy White paper working group member and the IFHIMA Regional Director for the Western Pacific and Licensed Health Information Manager in Korea. Oknam is a professional member of Korean National Standard Committee for ISO/TC215, and a consultant working for developing the privacy regulation and educational program.

Bibliography

Cooperation APE (APEC). Privacy Framework. 2005. URL: http://www.apec.org/Groups/Committee-on-Trade-and Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx

Organization of Economic Cooperation and Development (OECD), Guidelines on the protection of privacy and transborder flows of personal data, 2002. Amended 2013.
URL: https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf

The Australian Privacy Principles. URL:https://www.oaic.gov.au/privacy-law/privacy-act/australian-privacy-principles

The United States Health Insurance Portability and Accountability Act(HIPAA) 1996. URL:https://www.gpo.gov/fdsys/pkg/PLAW-104pub191/html/PLAW-104publ191.htm

ISO 27000 Series of Standards on Information Security. URL: http://www.27000.org/

American Society for Testing and Materials (ASTM). E1869:04(2014) Guide for confidentiality, privacy, access and data security principles of health information including electronic health records. URL: https://www.astm/org/Standards/E1869.htm

American Health information Management Association (AHIMA). Global Academic Curricula Competences for Health Information Professionals. 2015.
URL: http://www.ahima.org/about/global/global_curricula

Merriam-Wester Dictionary. An Encyclopedia Britannica Company.
URL: http://www.merriam-webster.com/dictionary/education

Endnotes

1. *ISO/TR 18638:2017(E), Introduction, page 5.*
2. *ISO/TR 18638:2017(E), Scope, page 1*
3. *ISO/TR 18638:2017(E), Scope, page 1*

Health Information Exchange Implementation - HIE Consent Model for Privacy Concerns - Privacy Regulatory Framework

By Selvakumar Swamy B.Sc, BMRSc., RHIA

Mujeeb C Kandy, M. App. Sc, MS, CPHQ, RHIA

QATAR

Introduction

Qatar issued its privacy protection law (Law no 13, 2016) through Ministry of Transport and Communication. The law includes provisions related to the rights of individuals to protect the privacy of their personal data and mandates individuals' consent be obtained before personal information can be used by an organization. However, as the law purports to address data privacy and protection across organizations in general, specific privacy and security matters associated to personal health information are yet to be developed.

In 2015, the Ministry of Health of Qatar conducted a situational analysis across healthcare organizations in government and private sector to assess the readiness of organizations on national e-Health implementation. The report identified technological and governance gaps within health information technologies and systems. In an effort to promote use of healthcare information technology by healthcare organizations and to support effective e-Health implementation, the Ministry of Health conducted bench marking studies with PwC Privacy Consultants and reviewed relevant practice standards and privacy laws from the United States, Australia, UK, UAE and Canada. As a result, a Privacy and Security Architecture frame for Qatar has been developed based on fundamental privacy and security principles already adopted by these other countries. It has been envisaged that a standard practice and principles will be implemented in Qatar in near future.

As of today, the privacy principles practiced in healthcare organizations are primarily based and cited on international standards (WHO, HIPAA-US, AHIMA)[1] developed and introduced through Health Information Management professionals. The practice models adopted institutionally depended on the experience and background of the HIM professionals. These policies are considered as effective in terms of establishing best practices, data governance and accreditation requirements within respective healthcare organizations; nevertheless, they are often deficient and less effective in disputes or in medico-legal discourses as they are not comprehensive enough to address legal interests in a healthcare context.

Problem Statement/Background

Since public sector is a major healthcare provider in the country, covering 80% of inpatient and outpatient services, implementation of integrated EHR in public hospitals and primary healthcare centers by August 2016 moved the majority of healthcare settings to paperless medical records based systems; subsequently, more HIT implementations like Health Information Exchange and patient portal were scheduled for implementation. As a result, questions and concerns over privacy of personal health information started arising with regard to ensuring individuals' trust over exchanging their personal health information between different healthcare organizations.

HIE is deemed to be a critical element to support the e-Health initiative to meet the country's National Health Strategy goals for 2030. However, it is imperative to have strategies to support HIE's sustainability; patient consent management being one of the key sustainability factors of HIE. Different consent models were evaluated by the HIE implementation team. By the end of 2017 and prior to HIE implementation, it was agreed between participating healthcare organizations to adopt an Opt-out Consent model in phase one HIE implementation; nevertheless, implementing privacy policy consent management system became a challenge from the beginning because unified health information privacy

had not been in practice within the participating organizations. Furthermore, sharing patients information to an organization before establishing an encounter became a concern due to lack of Record Locator Services (RLS) through a legitimate agency like an Health Information Organization (HIO). As a result, all participating organizations are provided with RLS functionality that enables all facilities to search for information of patients across all systems.

The following entities are involved the ongoing development of Health Information Exchange policy for Qatar:

- Ministry of Public Health (As Supreme Council of Health prior to 2016)
- Ministry of Transport & Communication (MoTC)
- Primary Healthcare Corporation (PHCC)
- Hamad Medical Corporation (HMC)
- Healthcare Providers, private sector
- ICT Qatar
- Cerner Corporation

Discussion and Recommendations

During the last 15 years, Health Information Management systems have evolved and grown rapidly in and among Gulf Cooperation Council (GCC) countries, in particular, Qatar, United Arab Emirates, Oman, and Saudi Arabia. Major Health Information Management transformations in Qatar began in 2012 as a result of National Health Strategies plan, and EHR and national insurance system implementation. HIM professionals have transitioned from their traditional role of health records custodian to data stewards and information privacy advocates. HIM professionals in the Middle East now take up accountability over the security, privacy and confidentiality aspects.

Healthcare organizations in the region have begun to recognize the role of Medical Records/ Health Information Management professionals and rely on them to develop organizational information governance framework and associated policies and procedures; however, standards and regulations at national level and proper enforcement over the integrity and protection of information has become inexorable due the growth of Health IT applications. Therefore, continuous efforts in this area at national level are needed to help healthcare organizations to gain trust in healthcare information from the clients/patients and other stakeholders including government, judiciaries, law enforcement departments, payers and third-party administrators.

Conclusion

In light of further advancements in HIT and its application in healthcare that include artificial intelligence, mobile devices and block chain security etc., more viable standards and practices need to be developed. This will require better regulations and jurisdictional support specific to healthcare. Therefore, developing privacy regulations that bring together emerging technology, healthcare processes and individual rights should take a pragmatic approach with consideration to future HIT solutions such as, telemedicine, Internet of Things and big data. They should include adoption of international best practices and strategies, participation with HIE management organizations, on developing and empowering health information management professionals and practices within the stakeholder group. Adopting such a philosophy will be the essential to advancing the privacy regulatory framework.

About the authors

Selvakumar Swamy, B.Sc, BMRSc., RHIA. IFHIMA Privacy White paper working group member and a seasoned Health Information Management professional with 30 years of experience; that covers traditional medical records system, transition to EMR and information governance. Selvakumar is currently employed as Business & Health Intelligence Manager in Directorate of Strategy Planning & Health Intelligence of Primary Health Care Corporation, Doha, Qatar.

Mujeeb C Kandy, M. App. Sc, MS, CPHQ, RHIA. IFHIMA Privacy White Paper Working Group Member and Mujeeb has served as Health Information Management professional in the middle east for over 20 years. He is currently working at Primary Healthcare Corporation, Qatar, as Head of Health Intelligence and actively engaged in HIE implementation, clinical coding and clinical documentation improvement program.

References:

Law No. 13 of 2016, Promulgating the protection of the privacy of personal data law. https://qatarlaw.com/wp-content/.../05/Personal-Data-Privacy-Law-No.-13-of-2016.pdf

Qatar National E Health & Data Management Strategy. https://www.who.int/goe/policies/qatar_ehealth2016_2020.pdf?ua=1

Endnotes

1. *World Health Organization (WHO), Health Insurance Portability and Accountability Act (HIPAA) and American Health Information Management Association (AHIMA)*

Laying the Foundation for Privacy Practice and Compliance in the Outpatient Setting: Policies and Procedures

Dorinda M. Sattler
MJ, RHIA, CHPS, CPHRM

Christopher Wilde
MBA, RHIA, CHC, CHPS, CHPC

USA

Introduction

In healthcare, there are federal regulations, state licensure requirements, and accreditation standards that require specific policies and procedures.

In this case study we will discuss the challenges that outpatient providers face with respect to compliance to standards and regulations and the role health information management (HIM) professionals can play in helping to facilitate the practice of policies and procedures for protecting health information, especially in outpatient settings.

In the experience of both authors, outpatient providers typically lack policies and procedures to ensure compliance with federal and state regulations, specifically related to privacy and security of patient health information. One author's study of data, compiled from malpractice liability risk assessments performed for 46 outpatient providers in Indiana from 2014 – 2018, revealed that only 30 percent had written policies and procedures related to health information.[1] The majority of these providers were physicians and dentists in solo or small group practices.

The case for policies and procedures has been made evident by findings of investigations by the Office for Civil Rights (OCR) as a result of numerous breaches of protected health information throughout the United States. Nearly 30 breaches affecting 85.5 million individuals occurring between 2016 and 2018 have resulted in resolution agreements between the providers and the OCR.[2] Of these resolution agreements, all contained corrective action plans where some form of policy and procedure attention was required. A root cause for a majority of these breaches was the absence of or the failure to implement policies and procedures to protect health information.[3, 4] Nearly half of the involved providers were outpatient or included outpatient care in their overall health system. [5]

When policies and procedures are not followed, when they are not current, or when they do not exist, patient safety and quality of care issues, unsuccessful legal defense and noncompliance with regulatory or accreditation body requirements may result.[6]

Legal Landscape

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) required the development of federal regulations protecting the privacy and security of identifiable health information. To satisfy this requirement, the U.S. Department of Health and Human Services (HHS) created HIPAA Standards for Privacy of Individually Identifiable Health Information (Privacy Rule) establishing national standards for the protection of health information (5)[7] and the Security Standards for the Protection of Electronic Protected Health Information (Security Rule) establishing a national set of security standards for protecting health information that is held or transferred in electronic form.[8]

The Privacy Rule provides a base of privacy protections for health information that is held by a covered entity or its business associates. The Federal requirements pre-empt state laws that are contrary to the Privacy Rule unless a specific exception applies.[9]

Healthcare providers who are subject to HIPAA, known as covered entities, must adopt policies and procedures to comply with the provisions of the Privacy and Security Rules. The policies must be periodically reviewed and updated based on regulatory or organizational changes that can affect the security of electronic protected health information. The policies must be maintained until six years after the last date of their creation/revision or last effective date.

The Health Information Technology for Economic and Clinical Health (HITECH) Act, was enacted as part of the American Recovery and Reinvestment Act of 2009, to promote the adoption and meaningful use of health information technology. Subtitle D of the HITECH Act strengthened both civil and criminal enforcement of the HIPAA rules. It also established Breach Notification Rules that require covered entities and business associates (individuals or organizations providing services to covered entities where protected health information is involved) to provide notification to affected individuals, HHS, and in some cases, the media when a breach of unsecured protected health information occurs.[10]

Healthcare providers must be concerned with much more than HIPAA. It appears that a new patchwork of state data protection laws from California, Oregon, Colorado, Alabama, and others are following suit from the European Union's General Data Protection Regulation (GDPR), all of which place additional data privacy requirements upon healthcare providers who are already heavily regulated. Both the GDPR and Colorado specifically require data protection policies.[11] US providers may be subject to GDPR if they provide care to the citizens of the European Union, regardless of where the healthcare provider is located.

Background and Consequences of Non-Compliance

The Office for Civil Rights (OCR) enforces and investigates compliance with the HIPAA Privacy, Security and Breach Notification Rules. The OCR completed the year 2018 with a record of enforcement activity. Settlements and judgments against covered entities totaled $28.7 million, eclipsing the prior record by 22 percent set in 2016 of $23.5 million.[12] Recent OCR HIPAA enforcement actions against non-compliant covered entities highlight the importance of written policies and procedures. Of 28 corrective action plans levied from 2016 through 2018, all included a requirement for the covered entity to develop, implement and train on policies and procedures to protect patient information.[13, 14] Nearly half of the covered entities are outpatient providers or include outpatient care within an integrated health system. The types of outpatient providers included physician group specialty practices, cancer treatment centers, pediatric providers, physical therapy, clinics, and other diagnosis-specific treatment centers.[15]

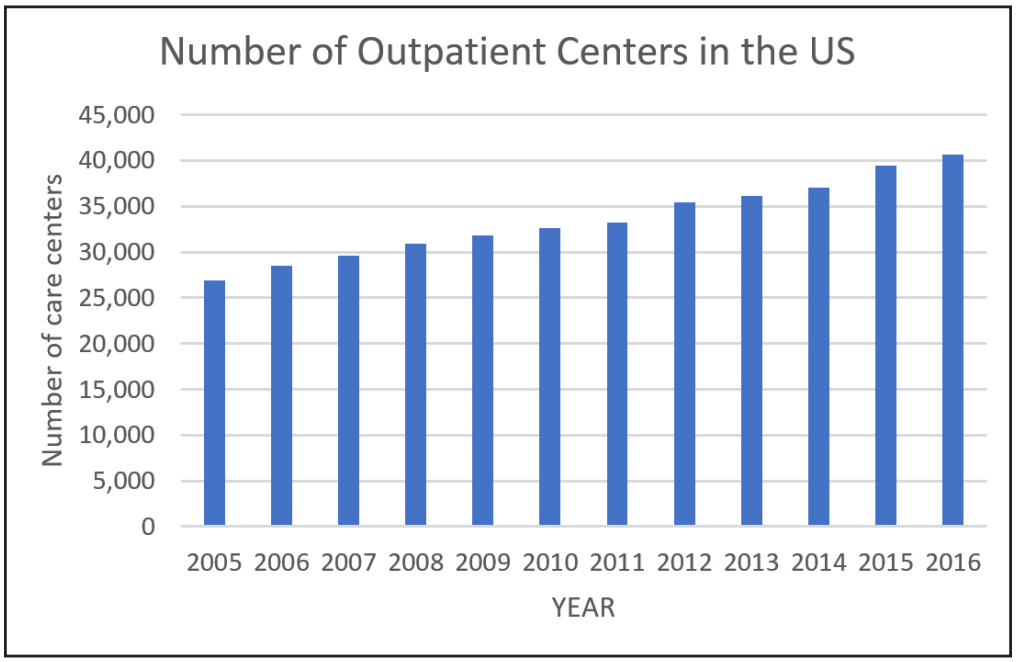
Accreditation by The Joint Commission for ambulatory care did not begin until the mid-1970s, while long-term care and hospital accreditation began roughly 10 and 20 years earlier, respectively. Outpatient facilities have not had the same maturity as hospitals and long-term care facilities related to meeting accreditation requirements and, therefore, are challenged to meet the Privacy and Security Rules.

Outpatient Landscape

The number of Outpatient facilities in the US has grown as the health care industry has tried to improve efficiency and patient satisfaction, while reducing costs. The types of outpatient services can include:

- Diagnostic centers (imaging, labs)
- Wellness and prevention centers (counseling and weight-loss programs)
- Treatment facilities (surgery, chemotherapy, radiation)
- Rehabilitation (Physical therapy, drug and alcohol rehab)
- Urgent Care

In an article from Modern Healthcare, from December 20, 2018, The Number of Outpatient Facilities Surges as Industry Values More Convenient, Affordable Care, " The number grew 51 percent from 26,900 in 2005 to 40,600 in 2016.(2)[16]



Source: CBRE analysis of U.S. Census data[17]

Problem Statement

The importance of, and focus on, direct patient care, often makes it difficult for practice managers to find time to create, review or update policies and procedures. The lack of creating or updating policies can have negative consequences on the organization. Policies can quickly become outdated, which may lead to processes being carried out which do not meet the regulatory requirements, leading to issues with patient care, non-compliance with privacy and security safeguards, and or problems with billing practices.[18] Updated policies and procedures are used to mitigate these risks to the organization through formalized processes that ensure regulatory compliance and promote quality patient care.

In one author's experience as a former Privacy Officer and Director of Health Information Management for an oncology management company, several years of observation revealed that the staff in these practices were already overworked and found it difficult to implement new procedures, let alone keep up with the requirements. A management company was able to come into these practices and provide all of the policies, training and administrative support to ensure the practices were compliant and met all of the regulatory requirements, through regular education of staff and monitoring of the organizations.

Outpatient Settings Present New Opportunities for the HIM Profession

The expansion of technology and regulations require HIM professionals to increase and solidify their expertise beyond what was learned during their post-secondary HIM education. HIM professionals should consider obtaining AHIMA's Certified in Healthcare Privacy and Security (CHPS) credential as a means to increase their knowledge and to advertise their expertise.

Many providers are not aware that the expertise of HIM professionals expands beyond coding and are unaware of what HIM can do for them regarding privacy and security. HIM professionals need to make themselves known.

HIM professionals looking for employment or consulting opportunities should expand their search to include privacy officers, legal counsel or c-suite members of ambulatory surgery centers (ASC), specialty practices, dialysis centers, home health care organizations and other outpatient healthcare providers.

Recommendations and Solutions

To ensure comprehensive privacy and security policies and procedures, outpatient providers would do well to bring HIM professionals on board. HIM professionals know the regulatory framework. They know where the data resides. Consequently, they can help providers create and maintain complete data inventories and information governance structures. Without these, privacy policies and procedures will be lacking.

Whether the provider seeks the assistance of an HIM professional or decides to "go it alone," determining which laws the healthcare organization is subject to is imperative.

- Create a matrix of the health information privacy and security requirements to identify what must be followed and which requirements are most stringent.
- Conduct a gap analysis to determine the need for new or revised policies and procedures is the next step, followed by actual implementation.
- Consider opting for policy management software for keeping an inventory of policies and establishing timelines for review.

To promote and educate on the needs and benefits of privacy and security policies and procedures, AHIMA and state HIM associations should consider:

- Developing outpatient-oriented training modules and toolkits on privacy and security
- Partnering with malpractice insurers or vendors who provide continuing medical education credits (CMEs) to their insureds
- Collaborating with national, state and local medical and professional societies to advance privacy and security practices.
- Promoting the HIM profession to healthcare business associates.

HIM programs whose colleges have medical schools can work to develop a partnership to educate medical students on privacy and security and the importance of policies and procedures.

Conclusion

Policies and procedures bridge the gap between privacy regulations and practice. However, the mere existence of policies and procedures will not suffice. They must be reviewed and updated as often as the legal landscape changes, when new technologies are introduced or when adverse outcomes result related to weak or nonexistent privacy practices occur.

Health information management professionals possess knowledge and experience in health information, they have a passion for patient privacy, they are leading the charge in information governance, and they have embraced technology in healthcare. As a result, HIM professionals are ideally situated to consult with and assist providers in the outpatient setting to create, implement, monitor, and revise health information privacy policies and procedures.

The HIM profession as a whole has a unique opportunity to promote the field of HIM and to lead privacy practice endeavors by being a partner or resource to professional associations, business associates, vendors and malpractice insurers of the outpatient care arena.

Outpatient providers do not know what they do not know about protecting patient information or about health information management, in general. It is up to HIM professionals to make themselves known to them and to educate them to advance privacy practices.

About the authors

Dorinda M. Sattler, MJ, RHIA, CHPS, CPHRM is an IFHIMA Privacy White Paper Working Group member and Clinical Assistant Professor of HIM at Indiana University Northwest. Dorinda is also the Consultant/Owner of Sattler Healthcare Consulting, Inc. which provides HIM and Risk Management Consulting services to healthcare providers throughout the state of Indiana. linkedin.com/in/dorinda-sattler-45414a92

Christopher Wilde, MBA, RHIA, CHC, CHPS, CHPC – is an IFHIMA Privacy White Paper Working Group member and Senior Manager, Compliance/Auditing/Third Party Oversite. Centene Corp. https://www.linkedin.com/in/christopher-wilde-rhia-chc-chps-chpc-b6337aa/

Endnotes

1. *Sattler Healthcare Consulting, Inc. Compiled data of risk assessment 2015-2018*
2. *U.S. Department of Health and Human Services, Office for Civil Rights (2019). Retrieved and compiled from: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html*
3. *U.S. Department of Health and Human Services, Office for Civil Rights (2018). Report to Congress on HIPAA Privacy, Security, and Breach Notification Rule: Compliance For Calendar years, 2015, 2016 and 2017. Retrieved from https://www.hhs.gov/sites/default/files/compliance-report-to-congress-2015-2016-2017.pdf*
4. *HHS.gov 2018 OCR HIPAA Summary: Settlements and Judgments. Retrieved from: https://www.hhs.gov/sites/default/files/2018-ocr-hipaa-summary.pdf*
5. *U.S. Department of Health and Human Services, Office for Civil Rights (2019). Retrieved and compiled from: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html*
6. *Policy and Procedure: A Healthcare Business Owner's Guide to Developing, Reviewing and Implementing Written Protocols (2016). CNA Healthcare Perspective, Issue 8. Retrieved from: http://www.hpso.com/Documents/Risk%20Education/Businesses/CNA_HP16-8_021016p_CF_PROD_SEC.pdf*
7. *US Department of Health and Human Services (2019). The HIPAA Privacy Rule. Retrieved from: https://www.hhs.gov/hipaa/for-professionals/privacy/index.html*
8. *US Department of Health and Human Services (2019). The HIPAA Security Rule. Retrieved from: https://www.hhs.gov/hipaa/for-professionals/security/index.html*
9. *US Department of Health and Human Services (2019). Does the HIPAA Privacy Rule preempt state laws? Retrieved from: https://www.hhs.gov/hipaa/for-professionals/faq/399/does-hipaa-preempt-state-laws/index.html*
10. *US Department of Health and Human Services. Breach notification requirements. 45 CFR § 164.406- 164.410. Available at https://www.govinfo.gov/content/pkg/FR-2013-01-25/pdf/2013-01073.pdf*
11. *Serrato, K.S. & Cwaline, C. & Rudawski, A.(July 9, 2018) US states pass data protection laws on the heels of the GDPR. Retrieved from: https://www.dataprotectionreport.com/2018/07/u-s-states-pass-data-protection-laws-on-the-heels-of-the-gdpr/*
12. *US Department of Health and Human Services. 2018 OCR HIPAA Summary: Settlements and Judgments. Retrieved from: https://www.hhs.gov/sites/default/files/2018-ocr-hipaa-summary.pdf*
13. *U.S. Department of Health and Human Services, Office for Civil Rights (2018). Report to Congress on HIPAA Privacy, Security, and Breach Notification Rule: Compliance For Calendar years, 2015, 2016 and 2017. Retrieved from https://www.hhs.gov/sites/default/files/compliance-report-to-congress-2015-2016-2017.pdf*

14. *US Department of Health and Human Services. 2018 OCR HIPAA Summary: Settlements and Judgments. Retrieved from: https://www.hhs.gov/sites/default/files/2018-ocr-hipaa-summary.pdf*

15. *US Department of Health and Human Services. 2019 Resolution Agreements: Resolution Agreements and Civil Money Penalties. Retrieved from: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html*

16. *Kacik, A. (2018). Number of outpatient facilities surges as industry values more convenient, affordable care. Retrieved from: https://www.modernhealthcare.com/article/20181220/NEWS/181229992/number-of-outpatient-facilities-surges-as-industry-values-more-convenient-affordable-care*

17. *CBRE (2019). Strong Demand, Aging Population Fueling Growth. Retrieved from: https://www.cbre.us/research-and-reports/2018-US-Medical-Office-Buildings?utm_source=cbre-us&utm_medium=media&utm_term=report&utm_campaign=2018-US-Medical-Office-Buildings*

18. *Irving, A. (October 13, 2014). Policies and Procedures for Healthcare Organizations: A Risk Management Perspective. Retrieved from: https://www.psqh.com/analysis/policies-and-procedures-for-healthcare-organizations-a-risk-management-perspective/*