Personal health records, global policy and regulation review

Yakov Flaumenhaft, Ofir Ben-Assuli *

Ono Academic College, Faculty of Business Administration, 104 Zahal Street, 55000, Kiryat Ono, Israel

A R T I C L E   I N F O

Article history:
Received 9 March 2017
Received in revised form 19 March 2018
Accepted 7 May 2018

Keywords:
Personal health records
Regulation
Privacy
Security

A B S T R A C T

Personal health records (PHR) have been endorsed as a promising tool for the self-management of an individual’s medical information, affording benefits to both the individual patient and the healthcare system as a whole. Nevertheless, adoption rates have been relatively slow and widespread acceptance has yet to be achieved. A significant obstacle often cited as delaying the implementation of these systems has been concern regarding the ability to properly ensure the security and privacy of this sensitive information. This article reviews the current legislative landscape in various countries, examining the degree to which they address these issues and support the implementation of PHR’s. This review compares in particular a number of prominent components of health data security and privacy across five different legislative jurisdictions in order to allow for a closer examination of regulatory approaches and measures. Of the legislation reviewed the EU’s GDPR stands out as seemingly providing the most comprehensive and stringent protection measures, yet nonetheless appears to leave significant room for interpretation and a degree of ambiguity in key areas. The results of this comparison, demonstrate considerable variances with regards to legal terminology and the degree of compliance required from entities offering PHR services across various jurisdictions. The paper ends with a discussion of specific policy implications and recommendations stemming from the current legislative state of affairs.

© 2018 Elsevier B.V. All rights reserved.

1. Introduction

The ever-growing wealth of personal medical information, often derived from various dispersed sources, has driven the development of digitized platforms as a means for efficiently maintaining, organizing and properly utilizing this abundant data [1,2]. The emerging platforms can be broadly divided into two categories, the electronic medical/health record (EHR/EMR) and the personal health record (PHR) [3]. The EHR is most commonly defined as a repository of patient data stored in a digital format. An EHR contains retrospective, current and in some cases prospective information regarding the patient’s medical condition [4]. The information may include demographic characteristics, documentation of encounters with healthcare providers (family doctor, community clinic, hospital, etc.), regular medications, drug sensitivity, previous operations, previous hospitalizations, laboratory results, and others [5].

Although distinctions have been made between EMR’s and EHR’s as far as the ability to be used across multiple healthcare providers [6], the common feature distinguishing both from the PHR is that they are systems intended for the use of health care professionals. This as opposed to the PHR whose primary purpose is to grant individual patients access and control of their personal health information [7].

The PHR is meant to be a patient centered tool for promoting engagement, involvement and the self-management of their ongoing healthcare [2,8]. The information contained in the PHR may include medical history, medication use and patient generated health information such as weight, glucose levels [9] and blood pressure. In addition it may include information to support wellness management, health and lifestyle habits such as diet, exercise, activity logs, and stress levels as well as alerts and reminders for assisting in disease management [10,11]. These various implementations are continuously being bolstered by a growing stream of smartphone applications entering the market, which are providing additional services, ranging from vital sign monitoring to mental health management [12]. The PHR may further incorporate decision-support tools to aid users in healthcare and life style management [1,13]. PHR’s have the potential to transform healthcare management, shifting the focus to a truly patient-centric model. PHR users have been shown to take an active interest in their healthcare, engaging with healthcare professionals and taking action to better their health [14]. Studies have shown that increased patient engagement, particularly for those managing chronic illnesses [15], leads to better outcomes, increases the likelihood of

* Corresponding author.
E-mail address: ofir@ono.ac.il (O. Ben-Assuli)

https://doi.org/10.1016/j.healthpol.2018.05.002
0168-8510/© 2018 Elsevier B.V. All rights reserved.
participation in preventive and healthy practices and reduces medical errors and hospital readmissions [16, 17]. The use of PHR’s has been shown to be associated with improved clinical outcomes [12]. For example in a study examining the association of parental use of integrated personal health records (PHRs) in relation to children’s adherence to immunization and well-child care (WCC) visit recommendations, researchers found that parents who used a PHR were more likely to adhere to the recommended WCC visits [18]. In another study researches demonstrated that the use of a PHR medication review tool, linked to the provider’s medical record, can improve the accuracy and safety of medication regimens adherence [19]. Additional benefits stem to be gained in the public health arena, assuming proper security and confidentiality measures can be established, aggregated data could be used to support health monitoring, outbreak management and research initiatives [20].

Although the concept of a PHR is not new [2,11], there is a lack of a clear consensus regarding its exact definition [15,21–23]. Various definitions can be found in the literature, for instance, according to the Office of the National Coordinator for Health Information Technology (ONC) a PHR is defined as a “an electronic record of health related information on an individual that conforms to nationally recognized interoperability standards and that can be drawn from multiple sources while being managed, shared and controlled by the individual” [24]. This as compared to the European standard EN13606-1 definition for a PHR which is “a health record for which the subject of care or a legal representative of the subject of care is the data controller” [25]. Another variation is provided by the Markle Foundation which defines a PHR as “An Internet-based set of tools that allows people to access and coordinate their lifelong health information and make appropriate parts of it available to those who need it”. There are various other definitions, with each emphasizing different aspects of the system [26].

2. Background to PHR spread around the world, security issues and challenges

When reviewing the global PHR landscape we found various systems being offered, whereas in some countries these offerings were made by corporate PHR vendors, in others they were part of statewide-backed initiatives.

Although dependent to a degree by how they are defined, In the US, which is a major focal point for corporate PHR vendors there have been estimated to be between 100 and 200 different PHR systems being offered [3,23,27]. The different systems provide varying degrees of connectivity and functionality, ranging from standalone software programs to cloud-based web portals which may be fully or partially integrated (‘tethered’) with other systems such as institutional EHR’s [1,11,15]. The systems are offered in various settings by institutional and commercial providers [28]. Multiple commercial PHR’s have emerged over the years differing in their designs, approaches, business models and licensing conditions. Two of the major initiatives in this field have been Microsoft’s ‘HealthVault’ launched in 2007 and Google’s ‘Google Health’ launched in 2008. ‘Google health’ provided a medium for storing, managing and sharing personal medical information as well as a directory of online services relevant to the specific data uploaded by the patient. Microsoft’s ‘HealthVault’ was intended as a medical information sharing platform to be used by both patients and health professionals, supplemented by a specialized search engine for health information [29]. Nevertheless, although being backed by a major conglomerate with significant technological prowess, ‘Google Health’ did not fare well and in 2011 Google announced the discontinuation of the service [2].

There are various other PHR systems being offered in different countries around the world, of which many are state-backed initiatives, although overall these are still relatively few. In 2003, Denmark launched a government-run PHR portal service known as Sundhed.dk which allows patients, among other things, to view treatments and diagnoses from their own patient record, book appointments with their doctor, renew prescription drugs, monitor medication compliance, and more [26]. Australia launched in 2012 a nationally run PHR, known as ‘My Health Record (formerly known as Personally Controlled Electronic Health Records)’ [30]. The system comprises two main components, the first is a website containing consumer-facing information supporting the use of the system. The second one is the PHR component, to which information can be uploaded from a number of sources which include, registered health providers, government related health agencies and registered users [31]. In Austria, ‘Elektronische Gesundheitsakte (ELGA)’ is a nationwide, patient –centered EHR/PHR system. Health records created at various health facilities are networked and made available electronically providing easy access to the patient’s health records [32]. In Finland ‘My Kanta’ is national patient portal which provides access to patient information archived in the Kanta Patient Data Repository, ‘My Kanta’ is set to be complemented with a new PHR platform for the management of patients’ personal health information (Omataietovaranto). Patients, through various PHR applications developed by national and regional projects or by software vendors, will be able to enter their personal data such as results of online health risk tests or measurements performed at home [32]. The Netherlands offers a PHR initiative under the MedMij program, which is intended to provide patients with a secure online environment for collecting and using health information from various sources [32,33].

Widespread PHR acceptance and implementation has the potential to produce significant benefits by reducing healthcare costs, improving quality of care and providing better health outcomes [11]. However, despite the promise held by PHR’s, adoption rates have been relatively slow [34]. One of the reasons cited for this has been patients’ concerns regarding the ability of such systems to properly protect the privacy and security of their medical information [35]. The chain of information at the base of PHR’s presents multiple points of vulnerability, potentially compromising the privacy of the information and the safety of those to whom it belongs. Beginning from the mobile and medical devices which collect personal health information and which have been demonstrated to be susceptible to interception and manipulation. Continuing with the various forms of electronic data transmission, through internet and wireless connections, and ending with the storage and retrieval of the collected information [13].

Attitudes among patients regarding the need and the ability to safeguard their personal information may vary according to their cultural, ethnic and socioeconomic background, personal inclinations, technological savviness and awareness to the potential dangers and threats [6,36]. Nonetheless it seems clear that these concerns are quite prominent among patients [37] as reflected in multiple surveys on the matter [6].

There appears to be just cause for these concerns [38], as an estimated 2.3 million Americans were victims of medical information identity theft during or before 2014 and nearly one third of the US population having been subject to some form of health information security breach during 2015 [39]. Medical information identity theft has been shown to be a costly and complicated matter to resolve, potentially leading to serious damage to its victims [40]. Thus, despite the significant benefits that have been demonstrated to be associated with the incorporation of PHR’s into the healthcare system, the above issues have been undermining the adoption of PHR systems [41,42]. Nonetheless, there still seems to be a keen interest on behalf of patients in having the ability to access and manage their personal health information [43]. These different attitudes seem to reflect the observation that concerns regarding
security are more characteristic of those not using the technology while those who adopt PHR, if they find they have benefited, are less disturbed by the matter [26].

As described above the advent of PHR’s is accompanied by a host of issues related to privacy, security and proper regulation [44]. In a world of growing interconnectedness we are already facing serious concerns regarding the safety of personal information, and the addition of medical information into the equation, perhaps the most sensitive of all personal data [45,46] further aggravates these concerns. Over the last few years the legislative, regulatory and technological arena has witnessed a number of developments and changes, including the demise of a major PHR vendor (i.e. Google Health) [2], new legislation [3] and obsolete certification initiatives (CCHIT) [47]. As such we believe there is importance in presenting an up-to-date review of the current regulatory framework in various countries around the world, as far as it applies to both internal and cross border PHR services.

As one of the main barriers to PHR adoption are concerns regarding security and safety, a review of different approaches taking by various countries to regulate and answer this need can provide insights into the best practices for remedying this situation as well as identify issues and obstacles that should be considered when addressing the matter.

Accordingly, the goal of this paper is to provide a basis for researchers and policy makers to examine and compare the merits of different approaches and further the development and implementation of required measures necessary to ensure that private health information is adequately protected, ultimately paving the way to increased PHR adoption.

In the following sections we will present an overview of the regulatory framework currently employed in several countries around the world as it relates to safeguarding PHR data, followed by a discussion regarding the implications of the current regulatory status and possible remedies to issues that arise.

3. Methodology

An in-depth literature survey was conducted using Google Scholar, via the authors’ academic institutions’ subscriptions to the vast majority of academic publication databases. Furthermore in order to be comprehensive as possible we performed an extensive search using the general Google search engine, as many papers, specifically regarding regulation, are not necessarily published in academic journals but may be published through government and private publications and websites, such as the Markle foundation and the US government.

The literature review was conducted using the following search strings/key words: PHR; personal health records; personal and sensitive data; Data Protection Directive; legislation; regulation; privacy; laws; market; privacy shield; EU directives; general data protection regulation; GDPR; legal; privacy; legislation; guidelines; policy; personal health record company; DMP; privacy act; certification; patient privacy and data security. We continued by reviewing the publications to identify relevant data concerning background issues and regulatory and policy frameworks applicable to PHR systems in different countries around the world.

The inclusion criteria for the references were as follows. For technology related issues, only review papers published after the year 2000 were examined. For evidence based practice, policy making, and intervention of technology in policy making topics, there was no restriction on date to allow for a broader historical and theoretical view. Additionally only information available in English was reviewed.

4. Current state of PHR regulation worldwide

In the initial stage of the review we sought to identify various legislative frameworks in countries around the world with applicable PHR security and privacy regulation.

In the US, one of the central markets for PHR system development [26], the relevant legislation pertaining to PHR’s are the ‘Health Insurance Portability and Accountability Act of 1996 (HIPAA)’ and the ‘Health Information Technology for Economic and Clinical Health (HITECH)’ which was introduced in 2009. These serve as the legal mechanisms governing privacy and security of protected health information. The initial security requirements for the exchange of certain health information and its disclosure were established by the HIPAA. These requirements were further expanded upon by the HITECH, which includes the requirement to notify individuals regarding breaches concerning their protected health information.

The HIPAA’s regulations and safeguards, issued by the ‘National Institute of Standards and Technology (NIST)’, are intended to govern the proper fulfillment of privacy and security requirements by entities offering PHR services. Additional provisions are provided in the ‘IT Infrastructure Library (ITIL)’, which includes security management guidelines based on ‘International Organization for Standardization (ISO)’ standards [48]. Among the issues addressed by these acts are the components of a facility’s privacy program, requirement for training, measures that must be implemented for the protection of data security and de-identification of data.

However, when discussing US regulation, a very important aspect that needs to be emphasized is that HIPAA regulations only apply to ‘covered entities’ i.e. traditional health care providers and their business associates or contractors, this in contrast to private PHR vendors who are not bound by this act [42].

Due to ambiguity following the HIPAA enactment regarding what constituted ‘business associates’ as well as to their precise legal standing, further legislation was enacted to clarify these matters. The HITECH act served to elucidate the status of business associates which process the information as a conduit, but do not use the information for other purposes. According to the act these entities would be subject to the same privacy requirements as covered entities [38,49,50].

These provisions were further clarified in 2013 by the Omnibus Final Rule which stated that business associates of covered entities include any business that “creates, receives, maintains or transmits personal health information”. Accordingly businesses which provide services such as data transmission and cloud servers would be obliged to comply with all of the HIPAA security rules and some of the HIPAA privacy rules [51].

Additional relevant legislation applicable to PHR service providers in the US, which in this case would apply to private vendors as well, is the ‘Federal Trade Commission (FTC) Act’. Under Section 5 of the act, violation of assurances, regarding privacy and security, as delineated in a privacy policy is prohibited. Accordingly PHR vendors, that do not uphold the security measures to which they committed, can be held accountable [52,53]. Additionally, in 2009, as directed by the the HITECH act, the FTC issued the Breach Notification Rule, applying breach notification regulation to non-HIPAA covered entities.

In addition to the above law-mandated regulations there are also non-governmental initiatives such as The ‘Markle Common Framework’. The framework is a set of policies and guidelines for the proper managing of personal health information, first published in 2006 by the Markle foundation [54]. The framework was further supplemented and updated in 2012 to address technological and legal developments, including the HITECH Act. The framework includes policy guides, technology guides, and model contract
language, outlining a set of ideal attributes for PHR’s and the corresponding best practices required to achieve them [55].

In Canada, the applicable legislation includes, the Canadian ‘Personal Information Protection and Electronic Documents Act’ (PIPEDA), which is part of federal legislation relating to private sector organizations, and the successive ‘Amendment to the PIPEDA by the Digital Privacy Act’ [56]. Although originally geared towards electronic commerce, the PIPEDA regulatory scope covers issues regarding the collection, use and disclosure of personal information in diverse contexts. In addition, assuming that PHR systems fall under the category of medical devices they must meet the licensing requirements of the ‘Medical Devices Regulations’ included in the ‘Food and Drugs Act’. Some of the provinces have also passed specific legislation relating to entities managing health information, such as Ontario’s ‘Personal Health Information Protection Act’ (PHIPA). Additional legislation that may apply includes the ‘Public Hospitals Act’, the ‘Home Care, Community Services Act’, ‘Regulated Health Professions act’ and the ‘Medicine Act’. Outside of the legislative realm there is a certification program for PHR providers offered by the non-governmental organization ‘Infoway’ [57,58].

The overall governing law applicable to PHR’s in the European Union (EU) thus far has been the Data Protection Directive (officially “Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data”), supplemented by the E-Privacy Directive ("Directive 2002/58/EC on Privacy and Electronic Communications") which were enacted in 1995 and 2002 respectively [59]. The directives concern the processing of personal data and the free movement of such data within the EU. The directives contained broad data protection and privacy policies as well as general categories of personal and sensitive data, but did not specifically detail the security and privacy measures which must be applied for the protection of health related data [60].

As a directive, EU member states were required to enact their own laws, which were to be based on the principals outlined by the directive. The independent drafting and implementation of the law as interpreted by each member state, led to legal variances which resulted in differing degrees of enforcement and additional related problems [61]. We hereby bring several examples from the EU, as they pertain to PHR’s to illustrate this situation.

In Germany the EU data protection directive was incorporated as part of the ‘Federal Data Protection Act (Bundesdatenschutzgesetz – BDSG)’, with the ‘Law for Medical Products (Gesetz über Medizinprodukte – MPG)’ also possibly being relevant to PHR’s [62].

The BDSG specifies the requirements regarding the safe communication and storage of personal health information. This includes the demand that the design and management of the entire system’s infrastructure meet current laws and standards. The system must afford restriction policies, auditing functionalities, backup strategies, firewalls, intrusion detection systems and a secure operating system [59].

The directives in Norway were implemented by the ‘Personal Data Act’, as well as the ‘Regulations on the processing of personal data’ which regulates all processing of health information necessary for providing, administrating or assuring the quality of healthcare to individuals. Additional relevant legislation includes the ‘Personal Health Data Filing System Act’. Organizations in Norway wishing to process sensitive personal health data must obtain a license from the ‘Data Protection Authority’. The authority outlines the general security guidelines to be applied for planning and implementing the protection of personal data [60].

In a study examining the possible future integration of PHR systems with Austria’s national electronic healthcare record (ELGA), the authors indicate that guidelines for PHR security standards would be derived from the Health Level 7 (HL7) PHR working group’s standardization work [63]. ELGA which was launched in 2015, allows cross-domain exchange of health data between all authorized Austrian health care providers (HCP) and enables secure access to health data for any patient visiting a HCP. All documents used in the system are required by law to conform to the nationally harmonized HL7 CDA implementation guidelines [64].

The Health Level Seven International (HL7), is an international organization which develops standards for interoperability in healthcare information technology [65]. In 2014 the organization released the HL7 Personal Health Record System Functional Model (PHR-S FM). The PHR-S FM addresses the necessary requirements for various facets of the system including collecting patient-generated health data, interoperability with EHR systems, data provenance, and privacy [65,66].

In a final example, in the UK according to the ‘Data Protection Act 1998 (DPA)’ any professional entity which holds personal information such as PHR providers is considered a ‘Data controller’. Data controllers are obligated to report their business activities to the ‘Information Commissioner’s Office (ICO)’ and must adhere to the data protection principles in relation to all personal data. These principals include the requirement to secure and guard the data against breaches and limitations on moving the data outside the EU [67].

As EU member states differed in the way they developed and implemented laws stemming from the directive, various inconsistencies emerged leading to legal uncertainty and administrative costs, which affected both the trust and confidence of individuals as well as companies’ ability to operate. In an attempt to remedy this situation the EU put forth and adopted in April 2016 a new set of regulations known as the ‘General Data Protection Regulation (GDPR)’ (Regulation (EU) 2016/679). The new regulation taking effect in May 2018, replaced the aforementioned ‘Personal Data Protection Directive’.

The new set of regulations introduced in the GDPR aims to resolve previous issues by standardizing data protection regulations throughout the EU. Additionally it seeks to better address emerging and globalized technologies and ensure the protection of individual rights and their control over personal information. A significant emphasis is given to provisions that promote accountability and governance, requiring relevant bodies to demonstrate their compliance with the principles outlined by the regulation. Among the changes introduced are provisions regarding the processing of data outside the borders of the EU, individual control over data portability and the ‘right to be forgotten’. The regulation also includes the requirement to provide transparent, clear and easily accessible policies. Additional measures stipulated include the appointment of a ‘data protection officer’, the requirement to conduct a ‘privacy impact assessment’ and obligations regarding ‘data breaches’ as well as specific requirements of national data protection authorities [68]. Furthermore the regulation presents the concepts of ‘privacy by design and by default’. The essence of these principals is that data controllers must design and implement mechanisms for protecting data which uphold the standards specified by regulation. Additionally they must ensure that by default only personal data which is necessary for a particular purpose is processed. This refers to the volume of data collected, the extent of processing, the duration of data storage and its degree of accessibility [70]. An overview of some of these guidelines is provided in Table 1. As a side note it should be mentioned that the UK’s vote by referendum to leave the EU has led to some uncertainty regarding future data protection and transfer policies [71]. Nonetheless, although acknowledging that certain aspects of the exit’s effects still remain unclear, the UK government previously assured that its decision to leave the EU would not affect its adoption of the GDPR [72].

When reviewing additional countries, we found one example from the Far East. In 2010 the Japanese Government launched
the ‘My Hospital Everywhere’ initiative, a national Personal Health Record program. The objective was to create a means for individuals to receive, provide, maintain and manage their own personal health information. According to a task force report, the relevant regulations pertaining to the system would be the ‘Act on the Protection of Personal Information (PPI Act)’ and the ‘Guidelines for the Protection of Personal Information’ [73]. The PPI Act is a central piece of legislation which outlines the basic principles for the protection of personal information and applies to both the public and private sectors. Article 6 of the PPI Act states that the government shall take special measures to protect especially sensitive information. Accordingly, legislation regulating businesses which manage sensitive data such as the healthcare industry, entail stronger confidentiality provisions. There are also more detailed guidelines which were established by different ministries for specific industry subsectors. Although these guidelines are not binding, most companies seem to abide by these rules, fearing reputational damage. The Ministry of Economy, Trade and Industry (METI) and Financial Services Agency (FSA) guidelines have provisions on the special treatment of sensitive information which includes healthcare. These guidelines provide an information security scheme which comprises four areas: ‘Organization’, ‘Person’, ‘Resources’, and ‘Information Technology’. These guidelines also specify the measures to be taken in case of a data leak or other breach of the PPI Act. As far as accreditation, companies can voluntarily join the ‘PrivacyMark system’ operated by a joint public–private agency established by METI. The mark is granted to companies who demonstrate their compliance with the law and the establishment of a personal information management system with a high level of protection [74].

In Australia the government launched in 2012, the ‘My Health Record’ system (formerly known as Personally Controlled Electronic Health Records) which allows individuals to create and manage their personal health record online. Corresponding legislation known as the ‘My Health Records act and privacy act (the My Health Records Rules and Regulation)’ [75] was introduced to support the system. The legislation covers the governance of the system, registration of relevant entities, the collection, use and disclosure of the contained personal health information as well as penalties and enforcement measures [76]. Additional relevant legislation includes the ‘Australian Privacy Principles (APPs)’ under the federal Privacy Act 1988’, the ‘Healthcare Identifiers Act (HI Act)’ [75] and the ‘Data Privacy Amendment, Notifiable Data Breaches Act 2017’ [77].

There are also several sets of international non-binding standards which have been introduced that are applicable to PHR’s. The ISO 27799, is a standard issued by the International Standards Organization, concerning the protection of personal health information. The standard provides guidance to holders of personal health information on the applicable implementation of ISO/IEC 2700, the general standard for the protection of electronic information. The organization also offers a certification process, allowing PHR holders to become ISO certified [48].

<table>
<thead>
<tr>
<th>Table 1</th>
<th>Examples of GDPR guidelines [72].</th>
</tr>
</thead>
<tbody>
<tr>
<td>Records of processing activities (documentation)</td>
<td>• Maintaining internal records of processing activities</td>
</tr>
<tr>
<td>Data protection by design and by default</td>
<td>• Obligation to integrate technical and organizational data protection measures into processing activities</td>
</tr>
<tr>
<td>Data protection/Privacy impact assessments (DIA s/PIA’s)</td>
<td>• A tool to assist in identifying the most effective way to comply with data protection obligations and meet individuals’ expectations of privacy</td>
</tr>
<tr>
<td>Appointment of a data protection officer (DPO)</td>
<td>• Duties include:</td>
</tr>
<tr>
<td>Breach notification</td>
<td>• Obligation to report certain types of data breach to the relevant supervisory authority (within 72 h), and in some cases to the individuals affected</td>
</tr>
<tr>
<td>Transfer of data</td>
<td>• Restrictions on the transfer of personal data outside the European Union</td>
</tr>
<tr>
<td></td>
<td>• Records will include:</td>
</tr>
<tr>
<td></td>
<td>• Organization’s details</td>
</tr>
<tr>
<td></td>
<td>• Purposes of the processing</td>
</tr>
<tr>
<td></td>
<td>• Description of the categories of individuals and categories of personal data</td>
</tr>
<tr>
<td></td>
<td>• Categories of recipients of personal data</td>
</tr>
<tr>
<td></td>
<td>• Details of transfers to third countries including documentation of the transfer mechanism safeguards</td>
</tr>
<tr>
<td></td>
<td>• Retention schedules.</td>
</tr>
<tr>
<td></td>
<td>• Description of technical and organizational security measures.</td>
</tr>
<tr>
<td></td>
<td>• Designing and implementing mechanisms for protecting data according to regulation.</td>
</tr>
<tr>
<td></td>
<td>• Ensuring that by default only personal data which is necessary for the each particular purpose is processed (amount collected, extent of processing, storage duration and degree of accessibility)</td>
</tr>
<tr>
<td></td>
<td>• Assessments will include:</td>
</tr>
<tr>
<td></td>
<td>• A description of the processing operations and the purposes</td>
</tr>
<tr>
<td></td>
<td>• An assessment of the necessity and proportionality of the processing in relation to the purpose</td>
</tr>
<tr>
<td></td>
<td>• An assessment of the risks to individuals</td>
</tr>
<tr>
<td></td>
<td>• The measures in place to address risk</td>
</tr>
<tr>
<td></td>
<td>• Report will include:</td>
</tr>
<tr>
<td></td>
<td>• The nature of the personal data breach</td>
</tr>
<tr>
<td></td>
<td>• The contact details of the data protection officer</td>
</tr>
<tr>
<td></td>
<td>• A description of the likely consequences of the personal data breach</td>
</tr>
<tr>
<td></td>
<td>• A description of the measures taken, or proposed to be taken</td>
</tr>
<tr>
<td></td>
<td>• Transfers are to be made only according to the conditions detailed in Chapter V of the GDPR</td>
</tr>
<tr>
<td></td>
<td>• Transfers may be made if the Commission has decided that the destination of the data ensures an adequate level of protection</td>
</tr>
</tbody>
</table>
Additionally, as mentioned above, there is the ‘HL7 Personal Health Record System Functional Model (PHR-S FM)’ which received accreditation by the American National Standards Institute [65,66]. The model serves to support certification initiatives and the need for international guidance on principals for the development, certification, procurement and implementation of PHR systems [78]. In a Table 2 we present a summary of the relevant legislation as reviewed here.

In an effort to provide an in-depth comparison of the various components characteristic of legislative applicability to PHR development and adoption, we present in Table 3 a comparison of a number of key components of personal health information protection measures as manifested in the regulatory frameworks of various countries possessing comparable and PHR relevant laws and policies. Although as discussed earlier, the GDPR is set to take effect and override current EU legislation, we nonetheless believe there is value in presenting previous legislative initiatives and as such we bring one pre-GDPR example for comparative purposes.

The components selected for comparison include areas identified by International standard organizations as necessary for ensuring information security. Among these are information security policies; human resources security; asset management; access control; cryptography; physical and environmental security, information security incidence management and compliance [81].

As previously mentioned some distinction should be made with regards to private vendor offering as opposed to government or state-backed systems. In countries with state-backed initiatives, such as Australia, one can find legislation pertaining specifically to these systems. In other countries such as the US, legislation has a broader reference, covering general health data management systems, applicable to, but not limited to PHR’s.

The results of this comparison contain some of the following findings:

1. Safety and security measures

In relation to the overall measures required from entities a common feature observed is the general obligation to implement what the legislators refer to as “reasonable” or “appropriate” steps and measures. Of these the GDPR seems to provide more specific and stringent requirements as to what would be deemed appropriate, although here too terms such as “data protection by design and default” can be somewhat ambiguous as to their full implications.

2. User authentication, Encryption, Identification, and access

There exists an overall demand for user authentication across the various legislative frameworks, however these do not seem to require specific advanced means of identification. Regarding encryption the HIPAA Security Rule does not mandate such measures, however encryption can serve to exempt a covered entity from complying with breach notification requirements. Similarly, it has been suggested that Canada’s PIPEDA may exclude vendors of PHR’s that have employed data encryption. Seeing that it defines “personal information” as “information about an identifiable individual” in light of encryption it could be argued that such information cannot serve to identify an individual [57].

3. Data Controller, Data Processor and data ownership

Although the terms Data controller and Data processor are used in various jurisdictions in which a clear distinction is made between them, accompanied by legal implications [90]. Nonetheless, as seen here, three out of the five jurisdictions reviewed do not employ this specific terminology.

4. Data breach notification

The different legislations vary as regard to the time frame in which the regulator must be notified with two of them specifying a minimum requirement (72 h under the GDPR and 10 days in the US). As regards to notifying individuals, three of the legislative frameworks leave room for the discretion of the responsible enti-
<table>
<thead>
<tr>
<th>Country</th>
<th>US</th>
<th>Canada</th>
<th>Australia</th>
<th>The EU (GDPR)</th>
<th>Norway (Pre-GDPR)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applicable data protection laws or guidelines (Federal laws only)</td>
<td>• Federal Health Insurance Portability and Accountability Act of 1996, (&quot;HIPAA&quot;)&lt;br&gt;• Health Information Technology for Economic and Clinical Health (&quot;HITECH&quot;)&lt;br&gt;• Federal Trade Commission (the &quot;FTC&quot;) Health Breach Notification Rule&lt;br&gt;• Federal Trade Commission Act (&quot;FTC Act&quot;) [52,53]</td>
<td>• Personal Information Protection and Electronic Documents Act (&quot;PIPEDA&quot;) [56,57]&lt;br&gt;• Amendment to the PIPEDA by the Digital Privacy Act [56]&lt;br&gt;• Possibly also: the Public Hospitals Act, the Home Care, Community Services Act, Regulated Health Professions act and the Medicine Act [57]</td>
<td>• The Australian Privacy Principles (APPs) under the federal Privacy Act 1988.&lt;br&gt;• My Health Records act and privacy act (the My Health Records Rules and Regulation) [75]&lt;br&gt;• Healthcare Identifiers Act (HI Act) [75]&lt;br&gt;• The data privacy amendment, Notifiable Data Breaches Act 2017 [77]</td>
<td>• The EU General Data Protection Regulation (&quot;GDPR&quot;) Will replace the current European Data Protection Directive (and implementing national laws) [56].</td>
<td>• The Personal Data Act, Regulations on the processing of personal data [60]</td>
</tr>
<tr>
<td>Required Safety and security measures</td>
<td>• Reasonable administrative, physical and technical standards for security [49,82]&lt;br&gt;• No specific technical solutions are required [49,82]&lt;br&gt;• Safeguards include securing locations and equipment; technical solutions to mitigate risks; and workforce training [49,82]</td>
<td>• Safeguards which are appropriate to the sensitivity of the information [57]&lt;br&gt;• Protection includes physical, organizational, and technological measures, employee training, care in the disposal or destruction of data [57].&lt;br&gt;• System should include audit trails, a password or otherwise provide reasonable protection against unauthorized access. (as per the Medicine Act) [57]</td>
<td>• Reasonable steps to protect information which can deal with privacy inquiries or complaints [75]&lt;br&gt;• The 'My Health Record System' includes encryption, firewalls, secure login/authentication and audit logging [86]&lt;br&gt;• Access limited to registered healthcare providers delivering healthcare [86]</td>
<td>• Appointment of a data protection officer [83]&lt;br&gt;• Data protection by design and default [83]&lt;br&gt;• Mandatory Data protection impact assessments (‘DPIA’) [83]</td>
<td>• General security guidelines for planning and implementing protection [60]&lt;br&gt;• Physical and organizational mechanisms secure physical access to equipment [60]</td>
</tr>
<tr>
<td>User authentication, Encryption, Identification, and access by others</td>
<td>• Verification of the identity and authority of a person, if not known to the covered entity [82]&lt;br&gt;• Verification in either oral or written form [82]&lt;br&gt;• No specific or technical verification requirements [82]&lt;br&gt;• Participants can agree to provide a list of authorized persons [82]&lt;br&gt;• Encryption alone doesn’t satisfy HIPAA Security Rule standards [84]</td>
<td>• Reasonable technical, physical and administrative measures to protect personal information and unauthorized access [85]&lt;br&gt;• System should include audit trails, a password or otherwise provide reasonable protection against unauthorized access. (as per the Medicine Act) [57]</td>
<td>• Does not prohibit the use of simple username and static password system for accessing personal data, but it does state that access procedures need to be secure [87]</td>
<td>• Selection of authentication mechanisms in accordance with risk evaluation [60]&lt;br&gt;• Authorization register, procedures for granting and managing access privileges [60]&lt;br&gt;• Regular follow-up reviews of access control mechanisms [60]&lt;br&gt;• User authentication based on role in the organization [60]</td>
<td></td>
</tr>
<tr>
<td>Data Controller, Data Processor and data ownership</td>
<td>• &quot;Data Controller” and “Data Processor,&quot; are not used in U.S. legal terminology&lt;br&gt;• Entity that owns, licenses, or maintains the Personal data usually held accountable [56]&lt;br&gt;• Providers traditionally seen as owning the medical records they maintain. [11,27]&lt;br&gt;• Patients have right to access, receive a copy, request corrections and receive assurance of confidentiality [11,27]</td>
<td>• &quot;Data Controller” and “Data Processor,&quot; are not defined under Canadian Privacy Statutes.&lt;br&gt;• Organizations are &quot;accountable&quot; for personal information in their custody or control processed by service providers on their behalf [88]&lt;br&gt;• PHR vendors must use &quot;contractual or other means&quot; to provide a comparable level of protection when sending data to third parties for processing [57]&lt;br&gt;• The support of the record belongs to the establishment or the ministry, but the content belongs to the patient&lt;br&gt;• The patient has the right at any time to access his health information [22,89]</td>
<td>• Australian regime does not distinguish between those who control or own personal information and those who process personal information [90]&lt;br&gt;• The Privacy Act applies to any APP entity that collects, uses or holds personal information [90]&lt;br&gt;• The Controller, determines the purposes and means of the data processing [91]&lt;br&gt;• The 'processor' processes personal data on behalf of the controller [91]&lt;br&gt;• The data controller is considered the principal responsible party and held accountable for employing processors that comply with GDPR standards [91]&lt;br&gt;• Processors are also subject to penalties and civil claims [91]</td>
<td>• The Controller, determines the purposes and means of the data processing [91]</td>
<td>• The data controller is the not the owner of the data, but will need to be in control of the data based on the guidelines defined through legislation [60]&lt;br&gt;• Joint controllers are allowed based on an agreement how they will secure the private information and deal with the data controllers responsibilities [60]</td>
</tr>
<tr>
<td>Country</td>
<td>US</td>
<td>Canada</td>
<td>Australia</td>
<td>The EU (GDPR)</td>
<td>Norway (Pre-GDPR)</td>
</tr>
<tr>
<td>---------</td>
<td>----</td>
<td>--------</td>
<td>-----------</td>
<td>---------------</td>
<td>------------------</td>
</tr>
<tr>
<td><strong>Disclosure of data</strong></td>
<td>• Covered entities may not use or disclose except as permitted or required by law, or with an individual’s written authorization [92]</td>
<td>• Cannot be used or disclosed for purposes other than those for which it was collected, except with consent or where required by law [57]</td>
<td>• Data no longer required it is to be destroyed, erased or made anonymous [57]</td>
<td>• Collection, use or disclosure must conform to what a reasonable person would consider appropriate under the circumstances [57]</td>
<td>• Disclosure of health information to health personnel from other organizations should be in accordance with rules regarding professional secrecy, and procedures must be defined to satisfy the requirements of confidentiality, integrity and availability [60]</td>
</tr>
<tr>
<td><strong>Data breach notification</strong></td>
<td>• If breach involves information of more than 500 people: Under the FTC breach rule: the FTC must be notified as soon as possible and within 10 business days [84]. Under the HIPAA breach rule: the Office for Civil Rights (OCR) must be notified “without unreasonable delay”, and within 60 days. A prominent media source must be alerted within 60 days. If more than 10 individuals cannot be contacted, notice must be posted on company website for 90 days or posted in print and major broadcast media.</td>
<td>• Any private-sector organization must notify an individual if it is reasonable to believe that the breach poses a significant risk to the individual [56]</td>
<td>• The notification must be conspicuous and given directly to the individual as soon as feasible [56]</td>
<td>• The notification to the individual must provide sufficient information for understanding the significance of the breach and to take steps, if possible, to mitigate its impact.</td>
<td>• Data breaches must be reported to the protection authorities and to affected individuals if is likely to result in a risk to individuals [83]</td>
</tr>
<tr>
<td><strong>Applicable Enforcement/Penalty measures</strong></td>
<td>• Under the HIPAA penalties can reach up to $50,000 per violation per day, up to a maximum total of $1.5 million per calendar year. Criminal charges can be filed against individuals responsible for a breach, with fines up to $250,000 and jail sentences reaching up to 10 years.</td>
<td>• Under the FTC Act penalties can reach up to $40,000 per offense and criminal penalties of up to 10 years imprisonment</td>
<td>• Failure to report a breach to the Privacy Commissioner or notify an individual would be guilty of an offence punishable on summary conviction and liable to a fine not exceeding CAD 100,000 [56]</td>
<td>• Non-compliance with the ‘My Health Records’ Rules can result in cancellation of participation and other penalties [75]</td>
<td>• Data breaches or serious breaches of the applicable legislation. Pursuant to Norwegian law, fines may reach USD 140,000 [56]</td>
</tr>
</tbody>
</table>
ties in terms of assessing the potential risk and the actual likelihood that a breach occurred.

5. Applicable Enforcement/Penalty measures

Of the measures reviewed the most straightforward and stringent are those defined by the GDPR, which can amount to as much as €20 m or 4% of a business’s global revenue.

5. Discussion and policy implications

The current policy and regulatory framework concerning PHR services, as presented in this review reveals a fragmented and country specific state of affairs which may stem from different conceptions of the underlying issues. For instance in a comparison of EU and US policies regarding health information privacy, Hiller et al. [49] found that the EU appears to have a more comprehensive and proactive approach to the matter which might be attributed to the divergent foundational approach towards patient privacy. Whereas in the US a dedicated statute was necessary to establish these rights, in the EU the underlying right was already in place in the form of a basic human right to privacy. In a similar vein Canada privacy laws have been observed to put more emphasis on objectives rather than on methods, using general terms to describe the applicable steps necessary for protection of data.

The differences in regulation between countries regarding acceptable practices of data transfer and storage have already resulted in conflicts, such as limitations regarding transfer of personal data outside the boardsers of the EU [57]. Overall regulatory bodies have been struggling to keep up with the fast pace technological advancements in the field of medical care and data sharing [12]. As a result current legislation is patchy at best, containing significant gaps and unaddressed matters [42].

Regulatory efforts are further stymied by public sensitivities regarding matters of personal data protection and a lack of consensus on the matter. Additional difficulty is due to a lack of accepted definitions and nomenclature for the various types of services that would fall under the definition of PHR services [23] and a lack of proper differentiation in regulatory frameworks between PHR and EHR systems.

Despite government efforts to modify and clarify regulatory frameworks the comparison of different legislation seems to indicate that there are still broad areas which lack specific guidance. Current legal frameworks appear to leave broad areas to the discretion of the organizations as far as the specific security measures to be adopted and implemented. While the intent behind this seems to be driven by a desire to allow a degree of flexibility for service providers and the difficulty in prescribing a ‘one size fits all’ guidance program, it nonetheless may lead to insufficient data protection measures, failing to address the growing threats presented by data handling malpractice, and properly ensuring public trust and confidence.

Patients and consumers around the world are faced with significant difficulty when attempting to understand the regulatory intricacies governing and protecting what can be considered the most private of personal data [57]. The lack of consistent privacy and security standards across the PHR market can increase confusion and lead to mistrust by the wider public.

In a review of the privacy and security characteristics of web based PHR services [79] it was found that HIPAA was the most widely referenced standard, however the majority of PHR systems did not conform to a specific set of standards and regulations. Out of the twenty four systems reviewed, six specified that they comply with HIPAA, while another four stated that they were not covered by HIPAA regulation although some of their processes were guided by its standards. Several systems such as Microsoft HealthVault and Healthy Circles were certified by TRUSTe and seven of the systems stated they followed the Health on the Net Foundation Code of Conduct (HONcode) principles for trustworthy health information. Of the systems reviewed only four stated that they used encryption both for communication and storage.

An additional review of more than a 100 PHR systems, demonstrated overall low levels of standard adoption, with only about a third found to follow some form of standard. The most prominent standards among those adopted according to this paper were the CCR and HL7 [23].

The current PHR landscape seems to suggest the need for the establishment of a common privacy and security criteria which would be able to be clearly understood by the ordinary consumer and allow for various PHR systems to be independently rated and compared. In order to protect the patient’s rights, providers of PHR services should be required to provide detailed information concerning the security measures being employed, their adherence to regulatory standards, intentions regarding data usage and degree of accountability and liability when the systems are breached or compromised [45,49,79].

This need was identified early on, as demonstrated in a summary of responses to an industry survey published in 2006 by the Centers for Medicare and Medicaid Services. Respondents stressed the need for using open standards, and collaborating with industry groups on the development of consensus standards for the exchange and storage of PHR data.

There is currently a lack of agreed-upon standards in areas such as data definitions, communication protocols and data analytics [10,53,53]. Additional issues that need to be addressed are data ownership and control, third party use of stored data for alternative purposes and the applicability of the legal framework [12,94]. Common industry standards would also provide for a greater deal of interoperability and enhanced service possibilities, allowing patients to safely share data across a variety of platforms and geographical regions [27].

When considering possible suggestions for enhancing the privacy and security levels of personal health information, it is necessary to reconcile between the need for an efficient health care system on the one hand and the requirement for proper protection measures on the other [49].

Several suggestions have been proposed in order to address these matters. In a paper comparing key features of the GDPR and the components of HL7, the authors found that HL7 security and privacy standards efficiently support the implementation of GDPR guidelines. These finding indicate that setting clear and specific minimum industry standards such as those detailed in HL7 could meet the objectives of regulators and more precisely define the measures organizations must take to protect information [95]. Rather than just using relatively vague and open to interpretation phrasing such as “reasonable” or “appropriate” steps, widespread and mandatory employment of a basic and comprehensive set of technology neutral standards such as HL7’s PHR-System Functional Model (PHR-S FM) could provide better protection to patients and increase their confidence in the safety of such systems, promoting greater levels of adoption.

One initiative for providing consumers with a better means for comparing and assessing various PHR offerings is the Model Privacy Notice (MPN). The MPN is a voluntary, openly available resource designed as a means for developers to convey in straightforward manner information about their privacy and security policies to their users. The MPN was intended to act as a form of ‘nutritional facts label’ providing an easily understood snapshot of the major aspects of the providers protection measures and provisions [16].

However as far as the voluntary certification initiatives are regarded in general, it has been argued that they should not be seen as sufficient policy measures. In a paper issued by the Center for Democracy and Technology (CDT) [42] the authors assert
that although certification initiatives can be useful in promoting the implementation of data protection measures, such programs within themselves cannot guarantee compliance and shouldn't be viewed as a substitute for a mandated policy and the accompanying enforcement mechanism. The regulatory framework supporting consumer protections, according to the authors should be instituted through legislation, serving as the basis for establishing industry best practices. In order to promote the adoption of such practices the center suggests establishing a safe harbor regime. The safe harbor would constitute a set of recommended best practices to be employed by PHR vendors, beyond those required by law. Providers who successfully demonstrate their compliance with these standards would be eligible for various benefits such as exemption from certain liabilities or penalties and perhaps a registered seal of approval. Additional recommendations put forth by the center regard the security safeguards that PHR providers should be required to implement.

Other researchers [96] stress that a rule-based regulatory approach defining fundamental requirements, coupled with industry norms and social contracts driven by market forces, would best serve to strike the right balance between consumer trust and the flexibility necessary for advancing PHR market and technology [96]. The establishment of a dedicated body responsible for regulating PHR's services could foster adoption and standardization, by promoting timely and appropriate legislation and providing guidance to both consumers and developers [12]. The stalled implementation of National health information systems due to public concerns over data security and privacy in Germany and the Netherlands highlights the need for engaging the public in matters of policy, to which end creating a joint committee comprised of commercial, private and public representatives and additional stakeholders such as non-governmental organizations can be recommended [97].

International standardization initiatives developed and adopted through treaties could also be very useful in bridging the gaps and enabling widespread adoption. In a report commissioned by the UN reviewing issues of cross border data transfer, it is suggested that in order to promote international data flow, data protection legislation should contain specific provisions on cross-border data transfers and provide alternative mechanisms which will allow businesses to comply with varying regulatory demands. These may include target jurisdictions ensuring equivalent levels of protection, concession by the companies transferring the data to be held accountable for any data breaches and binding corporate rules that apply across all of a company's activities [98]. In Table 4 we present a summary of potential remedies to issues raised in this discussion.

### 6. Limitations

The current review has several limitations. The fast pace development of new technologies and the varied and complex myriad of legal and regulatory systems present significant challenges when attempting to assess the relevant and applicable legislative statures [38,59,96]. Adding to the difficulty is the fact that most of the existing regulatory frameworks were established initially with reference to overall personal data protection or national EHR systems, and do not provide specific distinct provisions with regards to private and corporate PHR based initiatives [38,99]. The matter is further complicated by the absence of a clear and agreed upon definition for what constitutes a PHR. Accordingly despite our best efforts to elucidate the various mechanisms in place, the accuracy of our description of the specific regulatory frameworks may be found to be lacking.

Additionally, although we strived to be as comprehensive as possible and conducted a broad literature search using a variety of pertinent search terms, the scope of our review may be found to be limited and some relevant legislation overlooked, as certain policies were less accessible in detail due to not having been published in English. The different approaches towards health care management, stages of implementation, the various constitutional and institutional frameworks and varying attitudes regarding privacy and security concerns, as found in different countries, limited our ability to make policy suggestions that are all encompassing and which can fully address the specific needs of individual countries.

### 7. Conclusion and future research avenues

As described in this paper the international community has yet to fully come to terms with the realities of the fast pace developments in the field of health information technology and the accompanying challenges it presents to patient data privacy and security as it relates specifically to PHR's. Governments are still struggling to find the balance between the desire to promote such technology with the hopes of reaping its potential benefits and the need to provide adequate safeguards to protect the rights of its users. The correct formula for successfully achieving this balancing act has yet to be clearly established and future research could assist
by providing further insight and suggestions for specific regulatory models that would properly support these needs.

Differences in policies adopted by various countries present difficulties as digital globalization increases and patient data is no longer bound to geographically-based jurisdictional borders. The rise in the adoption and popularity of cloud computing services and associated PHR systems utilizing such infrastructure entails the reality of personal health data being distributed and stored across various jurisdictions and geographical regions, which include areas where privacy regulation may be insufficient to ensure adequate protection [57]. As the global community is increasingly facing widespread health issues and epidemics which transcend national borders such as influenza and AIDS, a world-standard PHR could support more efficient and speedy medical care and appropriate response measures both for travelers and immigrants as well as their host countries [100].

Furthermore, as presented in this review, PHR systems in different countries have been established by both governmental and private vendors, accordingly it will be necessary to examine how these systems relate to each other and whether they can support data transfer and migration. As different technological solutions have been suggested for coping with these issues, future research could explore the degree to which they indeed answer these needs. With the growing trend of interconnectedness and borderless data exchange, as exemplified by mobile PHR’s, the Internet of things and cloud computing, it will be necessary to explore how health information in particular can be protected across numerous interacting digital platforms and which parties can be held accountable for guaranteeing proper data protection.

References

[33] Draft report EU state of play on patient access on eHealth data. Joint Action to support the eHealth Network; 2018.
[38] Improvements and challenges in health privacy law. Center for Democracy & Technology; 2009.
[49] Hiller J, McMullen MS, Chumney WM, Baumber DL. Privacy and security in the implementation of health information technology (electronic health records):


[66] International HLS. HL7 Publishes Updated Personal Health Record System Functional Model as an Approved ANSI Standard; 2014.


[76] Daly A. The introduction of data breach notification legislation in Australia: a comparative view computer law & security review; 2018.

[77] Health Level Seven International.


[90] Who does the GDPR apply to?: Information Commissioners Office.


[98] Little R. D2. 3 Privacy and Security Analysis.