The Regulation of Personal Health Record Systems in Canada

James Williams, Jens H. Weber-Jahnke[*]

INTRODUCTION

Health care systems in North America, Europe, and other parts of the world are being challenged by rising service costs and aging populations. In response to these concerns, governments and health care providers are seeking to improve the efficiency and efficacy of health care delivery. Among other initiatives, they have invested vast sums of money into information and communications technologies, including decision support systems, telemedicine, and electronic records. In Canada, the efficiency and quality gains expected from electronic health information systems have prompted the federal government to devote billions of dollars of funding towards the goal of a pan-Canadian electronic health record (EHR) system. On a provincial level, governments have launched several initiatives to increase the utilization of medical records systems by physicians and other health practitioners.

Despite the growing prevalence of health information software, it is not clear that patients have benefited from the accessibility that these systems allegedly provide. This situation is somewhat disconcerting, given that the jurisprudence in Canada indicates that patients have a right to access their personal health information (PHI) stored in medical records systems.[1] While legislation also provides for a right of access in many provinces,[2] actually obtaining access to PHI in the custody and

---

* James Williams, BA, BSc, JD, MSc is a privacy/security consultant with Ontario's "Community Care Information Management" program. Jens Weber-Jahnke, Dipl. Inform., Dr. rer. nat., PEng, is Director of Software Engineering and associate professor at the University of Victoria.

1 The right of a patient to access their own health records has been considered by the Supreme Court of Canada. In *McInerney v. MacDonald*, [1992] 2 S.C.R. 138, 93 D.L.R. (4th) 415 (S.C.C.), the Court decided that patients had a right to access their health records. The Court based this right of access not on property rights, but on the fiduciary duty owed by the physician to the patient. In making this distinction, the Court affirmed the principle in *Lamothe v. Mokleby* (1979), 4 Sask. R. 352, 106 D.L.R. (3d) 233 (Sask. Q.B.), that the physician owns the records themselves, along with the system that the records are stored in. In addition, various provincial statutes also make it clear that health care providers own health records. For instance, the Ontario *Public Hospitals Act*, s. 14(1) states that "the record of personal health information compiled in a hospital for a patient is the property of the hospital". a discussion of the interplay between common law and privacy law surrounding rights of access, see *Rousseau v. Wyndowe*, 2008 FCA 39, 71 Admin. L.R. (4th) 58 (F.C.A.).

2 For example, the *Personal Health Information Protection Act*, S.O. 2004, c.3, Sch. A, [PHIPA] s. 52(1) provides a right of access to one's own personal health information, (barring a few exceptions).

control of a health care provider can be a costly and time-consuming process. Not only must a patient make a request to the custodian, whose staff members may be overtaxed with routine operational duties, but also there are often issues with respect to composing records from disparate sources and severing the contents of records. The presence of case notes, comments, and other work product artefacts can complicate the process, as health care providers are generally reluctant to share this type of information with patients.[3]

The personal health record (PHR) has the potential to solve the problem of access by fundamentally altering the manner in which patients interact with health care providers. As opposed to EHR systems, the patient manages the information in a PHR, giving them access to their information on demand. In terms of recent trends, many health care organizations in the United States have developed bridges by which information generated by health care professionals (e.g., diagnostic reports) can be transferred to a PHR system without labour-intensive manual intervention. The vision of the PHR is that of a patient-managed repository that contains an entire history of care, including prescriptions, care episodes, and billing information. The question of how to provide patient-access to health information effectively disappears, since the health record becomes inherently patient-centric.

Online tools that provide patients with instant access to a longitudinal, patient-managed repository of PHI also have ramifications for the degree to which patients can participate in the management of their own health. The PHR may serve as a tool by which health care providers can encourage patients to become active partners in their health — a strategy that has been cited in the research literature as offering major advantages to the health care system on both a micro and macro level.[4] Some researchers have suggested that participation in their own health care management can make patients more health conscious.[5]

In addition to encouraging self-management, PHR systems also have the potential to support online communities devoted to health care. Although these systems are still in their infancy, the marketplace evidences a noticeable trend towards the inclusion of features from the social networking domain. PHR systems such as PatientsLikeMe are explicitly built around the concept of an online network of patients who share personal health information, recommend practitioners, voluntarily report metrics on pharmaceutical usage, and provide support and encouragement to one another.

The advent of social networking applications has provided users with a new array of tools to facilitate collaboration and communication. However, the flexibility inherent to the design of these applications has given rise to significant concerns

---

3 See S.B. Frampton, S. Horowitz, and B.J. Stumpo, "Open medical records" (2009) 109:8 American Journal of Nursing 59.

4 See B. Fisher, V. Bhavnani, and M. Winfield, "How patients use access to their full health records: a qualitative study of patients in general practice" (2009) 102:12 Journal of the Royal Society of Medicine 539.

5 See V. Franklin *et al.*, "Patients' Engagement With 'Sweet Talk' — A Text Messaging Support System for Young People With Diabetes" (2008) 10:2 Journal of Medical Internet Research 20.

about privacy, security, and data quality.[6] Regulatory authorities in Canada have taken increasing interest in social networking, as evidenced by the Privacy Commissioner's recent report on Facebook.[7] Given that PHI is one of the most sensitive types of personal information, the use of online social networking techniques in the health care domain is a matter of no small interest to regulators, health care providers, and patients.

This paper analyzes the regulatory regime for PHR systems in Canada. The first part of the paper consists of an introduction to some of the major issues associated with these applications, with a focus on privacy, security, data quality, and interoperability. Following this preliminary discussion, the bulk of the analysis deals with the legal instruments that apply to PHR products developed by private sector organizations. Due to space constraints, the paper concentrates on legislative and regulatory instruments, deferring a discussion of the possible impacts of tort, product liability, and contract law on PHR systems.[8] Despite this omission, it is clear that the current regulatory regime is not well suited to handling some of the challenges arising from this type of application. Given the market indicators on the popularity of PHR systems, there is need for future work in this area, both by the research community and by regulatory agencies.

I. PERSONAL HEALTH RECORD SYSTEMS

(a) Background

The difficulty involved in accessing one's own medical information is not a recent phenomenon. In the traditional physician-patient relationship, the physician has had exclusive access to information on diagnoses and treatment; patients could take little initiative, due to their relative lack of knowledge, and the paucity of resources at their disposal.

This situation began to change in the late twentieth century. In addition to the advent of direct-to-consumer advertising, the appearance of the Internet allowed patients to access current and peer-reviewed health information resources directly.[9] The first generation of websites devoted to health care consisted of *health portals* — online catalogues of information on health care. At the time of writing, patients can access a wide variety of online resources, reducing the traditional information asymmetry with respect to conditions and treatments.

Although the introduction of online health portals greatly improved the availability of information, patients still face major hurdles in accessing their own health information. Given that many experts in the field of health care have extolled the

---

6 See J. Williams, "Social Networking Applications in Health Care: Threats to the Privacy and Security of Health Information" (2010) Proceedings of 2nd Intl. ICSE Workshop on Software Engineering in Health Care 39.

7 PIPEDA Case Summary #2009-008.

8 A discussion of the interface between PHR systems and tort, product liability and contract law would be highly interesting. However, it would also be a significant undertaking that is well beyond the scope of this paper.

9 See P. Bleicher, "Health 2.0: Do it yourself doctoring" (2008) 17 Applied Clinical Trials 38.

benefits arising from preventative medicine and patient empowerment, this state of affairs does not have positive implications for the sustainability of health care systems in Canada and abroad.

The answer to the question of accessibility may come in the form of a new breed of health information management application. *Personal health record* (PHR) systems are patient-managed repositories of PHI that allow users to store longitudinal and comprehensive records of their health data. Individuals can use these applications to manage their personal health information, including medication histories, immunizations, past procedures, allergies, and insurance plans. Information in the PHR can also be shared with family members, friends, and health care providers at the owner's discretion, through the use of social networking features or role based access controls. The ability to grant access to other individuals supports a variety of usage scenarios, such as legal guardianship and substitute decision-making.

The inclusion of social networking mechanisms in PHR systems is a significant recent development, as it expands the scope of the application beyond simply providing access to information, namely towards a platform for *collaboration* in health care. The term "Medicine 2.0" has been used to denote the use of social computing for purposes of promoting collaboration between patients, caregivers, and health care providers.[10] As an example, HealthyCircles (www.healthycircles.com) allows users to access provider registries, diet plans, telemedicine, and interactive health-monitoring applications; health care practitioners may collaborate with patients by joining a patient's care team. The power of collaboration is significant, and even outside of the PHR domain, there are rapidly growing online communities devoted to particular health ailments.[11]

(b) The PHR

A PHR is a health record that is controlled by a patient, rather than by a health care provider.[12] In the words of one researcher, patients decide what is included, where it comes from and who can see it.[13] Although some PHRs have been created for mobile devices such as USB keys and smartphones, the most salient and popular examples of PHRs consist of online health records management systems such as HealthVault, Google Health, and Dossia. In the latter case, the PHR is managed by a *site operator* — an organization that develops, deploys, and maintains the software. In addition, the site operator furnishes the infrastructure (typically servers hosting relational database management systems) on which the information resides. The servers involved may be located at the site operator's various facilities, or they may be distributed in a "cloud".

---

10 See G. Eysenbach, "Medicine 2.0: social networking, collaboration, participation, apomediation, and openness" (2008) 10:3 Journal of Medical Internet Research e22.

11 See *supra* note 10.

12 See T. Van Deursen, P. Koster, and M. Pektovic, "Reliable Personal Health Records" (2008) Proceedings of eHealth Beyond the Horizon — Get IT There 484.

13 D. Stewart, "Socialized Medicine: How Personalized Health Records and Social Networks are changing Health Care" online: (2009) 32:7 EContent 30 <http://www.econtentmag.com>.

One of the main functions of a PHR is to serve as a repository for both patient-generated data (i.e., self-reported metrics such as blood pressure) and data that has been created by health care providers. In order to provide some clarity, we introduce four usage scenarios that take account of the different ways in which information may be exchanged between a PHR and health care providers:

In the *Isolated PHR* usage scenario, the patient is responsible for loading information into the PHR, granting other individuals access, and extracting data in a form that is readable by a health care provider. Patients may load information that has been produced by professionals, such as diagnostic reports or prescriptions, but the process is entirely driven by the patient.

The *Data Sink* usage scenario extends the isolated PHR approach by allowing health care providers to upload information to the PHR. As an example, Health Management Organizations in the United States have automated the process of uploading diagnostic reports and billing information to PHRs such as Dossia. Mainstream services such as Google Health allow patients to upload the results of laboratory tests or other diagnostic procedures, but the process is simplified greatly if the provider has control over the upload process.

In the *Data Source* scenario, the isolated PHR approach is modified by allowing health care providers to download information from the PHR. For instance, the patient may have used a monitoring device to load daily blood pressure readings into her PHR record. By downloading this data, a physician would be provided with self-reported health metrics by which she may formulate a care plan for the patient.

Lastly, the *Interoperable PHR* combines the data sink and data source scenarios, allowing health care providers to upload and download information from the PHR. Since multiple providers may be involved in exchanging data with a PHR, the participating information systems should conform to interoperability standards that allow data to be drawn from multiple sources and reconciled within the PHR's data model.[14]

(c) Social Computing

As mentioned above, PHR systems are moving towards incorporating features from social computing systems — web-enabled applications that put an emphasis on online social networking and collaboration. Although the original World Wide Web was intended to support collaboration through the use of email, hyperlinks, and bulletin boards, information on first generation websites generally flowed in one direction. The second generation of websites placed a high degree of emphasis on participation, including collaboration and content generation by users. Although wikis and blogs are common examples of second-generation websites, the most feature-laden applications consist of *social networking platforms*. Users of these systems construct online social networks through the use of voluntarily initiated social ties. As opposed to bulletin boards and chat rooms, online social networking sites make the relationships between users explicit, visible, and computable.

Current PHR offerings such as Google Health and Microsoft HealthVault al-

14 See J.S. Kahn, V. Aulakh, and A. Bosworth, "What it Takes: Characteristics of the Ideal Personal Health Record" (2009) 28:2 Health Affairs 369.

low consumers to grant access permissions to health care providers and family members, typically by sending an "invite" to an email address. As a result, the first generation of PHR systems can be said to have rudimentary social networking capabilities. However, some websites (e.g., PatientsLikeMe) go far beyond the basics, by providing a full suite of collaboration and networking tools. From descriptions of products on the horizon, it seems safe to assume that PHR systems will generally incorporate features from the social networking domain. Although this trend promises to enrich the user experience, it comes with a price; as discussed below, PHR systems that incorporate social networking features also inherit the privacy and security risks associated with them.

Lastly, social networking does not merely provide benefits for patients. Health care providers can also take advantage of the collaborative nature of social networking approaches, establishing virtual communities in which practitioners can share advice, research results, and best practices.[15] For example, *Medting.com* is an application that permits physicians to share medical images and videos, get advice from peers, discuss cases, rate and recommend cases and retrieve relevant professional publications from sources such as pubmed. Another example is the *DocPatients* network at *Doctations.com*, which provides an online community to facilitate participation of patients in provider eHealth processes.

(d) PHR versus EHR systems

In order to clarify the regulatory environment governing patient management systems, it is important to distinguish EHR from PHR systems. This section introduces some basic concepts from the academic and industrial literature.

In an influential document, the Canadian Medical Association (CMA) defined an EHR as:

> . . . a longitudinal collection of personal health information of a single individual, entered or accepted by health care providers, and stored electronically. The record may be made available at any time to providers, who have been authorized by the individual, as a tool in the provision of health services. The individual has access to the record and can request changes to its content. The transmission and storage of the content is under strict security.[16]

The CMA definition coheres well with those offered by the academic community. According to various researchers, EHR systems are typically (1) complete, integrating information from all health providers that treat the individual; (2) lifelong, storing information over the course of an individual's life; (3) accessible,

---

15 See M.N. Kamel Boulos and S. Wheeler, "The emerging Web 2.0 social software: an enabling suite of sociable technologies in health and health care education" (2007) 24 Health Information and Libraries Journal 2.

16 Canadian Medical Association, "Advancing Electronic Health Records in Canada" CMA Working Principles and Recommendations Discussion Paper (2002). Although not present in the CMA's definition, Canadian EHRs are managed by governmental ministries or agencies. Access to these systems is typically tightly controlled through the use of access permissions and rigorous contractual arrangements.

available to a variety of professionals in various geographical areas, and; (4) secure, protected against unauthorized access.[17]

Although PHR systems are designed to meet these same conditions, there are some important differences. *First*, EHR systems (and EMR systems in clinics or hospitals) are typically used for a variety of functions; health information in these systems may be used for clinical work, teaching, research, and process improvement. In addition to health care providers, individuals conducting audits, accreditation, and qualification reviews may access data in the EHR.[18] In contrast, data residing in a PHR may not be available for these purposes, since access requires explicit consent from the record owner.[19] *Second*, EHRs contain various institutional work products, such as physician's notes and administrative data. The release of this information to patients is generally resisted by health care practitioners. *Third*, health data in an EHR is supplied by professionals, whereas health data in a PHR can come from non-professional sources, including the patient herself. *Fourth*, an EHR is typically managed by a government agency or health authority, whereas PHR systems can be provided by Internet service providers or software vendors such as Microsoft or Google. *Fifth*, access to patient information in a PHR is granted not through the use of organizational level agreements, but by the explicit consent of the patient.

On account of these differences, it is clear that PHR and EHR systems are not synonymous. The main consequence of this conclusion is regulations and standards for EHRs may not be relevant to PHR systems.

II. ISSUES WITH PHR SYSTEMS

PHR systems raise a number of interesting issues concerning privacy, security, trust, integration, and interoperability. This section introduces some of the risks that arise under each of these headings, in order to provide background for the discussion to follow.

As a preliminary matter, it is useful to review some of the unique aspects of information management in the health care domain. *First*, PHI is arguably among the most sensitive types of information. In contrast to other types of sensitive information (e.g., financial information) individuals cannot easily be indemnified with respect to unauthorized disclosure of their personal health information. This type of information also has high value to many third parties, including insurers, employers, pharmaceutical companies, researchers, and public health agencies. *Second*, in contrast to many other application domains, the relationships of actors participating

---

17 See N. Terry and L. Francis, "Ensuring the Privacy and Confidentiality of Electronic Health Records" (2007) 2007 U. Ill. L. Rev. 681. Of course, real-world systems may fail to satisfy one or more of these conditions at any given time.

18 See L.E. Rozovsky and N.J. Inions, *Canadian Health Information*, 3d ed. (Toronto: Butterworths, 2002) at 7.

19 This constraint prevents PHRs from serving as a source of information for reporting to governments and other public bodies tasked with managing the health care system. However, some current PHR service providers reserve the right to use the data for other purposes. As an example, PatientsLikeMe shares information with corporate partners.

in the health care of an individual are ephemeral, since health care teams coalesce around episodes of care. *Third*, the inquiries that an individual makes about health conditions can give outsiders information about that individual's health status. *Fourth*, since health conditions are often hereditary, information about a patient's ailments or health concerns can facilitate the inference of information about their family members.

(a) Privacy and Security

From one perspective, privacy and confidentiality issues may actually be less intense in PHR systems than in the traditional medical records settings. For instance, a major hospital may hold records on hundreds of thousands of patients, each of which is accessible to a wide variety of health care professionals and administrators. In the absence of strong access control mechanisms (to prevent unauthorized users accessing data) and auditing (to prevent authorized users from misusing their privileges), PHI in a medical records system is readily available to hospital employees. In contrast, within the PHR context a patient must explicitly grant permission to allow another actor to view a portion of her health record; the information in the record is ostensibly within the full control of the patient.

Despite this initial impression, significant privacy and security concerns arise within the PHR context. While health care providers are typically bound by various legal instruments that impose constraints on the collection, use and disclosure of PHI, an operator of a PHR may not have the same obligations. Given the value of health information to third parties, most vendors will be faced with an incentive to disclose the information, either by bulk data extracts or by allowing access to the data repository. PHR operators may release personal information to a variety of data recipients, including marketers, employers and insurance companies.[20]

Since many online PHR systems are delivered as hosted services, the physical location of the site's servers is not always clear. Site operators may sell, transfer, or sub-contract their operations, sometimes resulting in a change in the legal jurisdiction where the data resides.[21] Even more ominously, *cloud computing* approaches can result in data being scattered and duplicated across numerous jurisdictions.[22] This state of affairs raises a number of issues. *First*, in some of these regions, privacy protections may be lacking. For instance, the provisions of the United States

---

20 As an example of third party access, there is recent evidence of increased data requests from social networking sites by government agencies. For an example, see R. Lardner, "Break the law and your new 'friend' may be the FBI" *Associated Press*, (16 March 2010).

21 Another interesting issue that arises with respect to the PHR concerns the legal status of the PHR's contents from the standpoint of documentary evidence. A discussion of this topic is beyond the scope of this paper, but see Ken Chasse, "Electronic Records as Documentary Evidence", (2007) 6 C.J.L.T. 141 for a relatively recent treatment of the general difficulties surrounding Canada's approach to electronic documents in this context.

22 See Brian Hayes, "Cloud computing" (2008) 51:7 Communications of the ACM 9.

Patriot Act[23] raise particular risks for the confidentiality of PHI, as that statute prohibits a vendor from telling users that their data has been accessed by governmental agencies. *Second*, cloud computing approaches have a number of security implications. Not only do virtualized cloud environments raise the risks of security issues, but the fact that the infrastructure is dynamic and distributed makes it difficult for vendors or health care providers to perform assurance, risk assessment, or testing activities. *Third*, users typically have no control over retention periods for PHI or associated metadata. Even if deleted from the repository, duplicate images and backups can exist in any of the multiple jurisdictions in which the data was stored.

While governments and health care providers are typically subject to obligations concerning the accuracy of PHI stored in their medical record systems, PHR vendors may not be faced with similar responsibilities. In some sense, the fact that patients manage their own information in the PHR vitiates the relevance of the accuracy obligations that frequently are assigned to health care providers. However, the presence of defects in the PHR software may result in a loss of data integrity — a situation that could prove onerous should the data be relied upon for the provisioning of health services.

If social networking features are included in a PHR system, additional security and privacy issues arise. *First*, social computing applications allow for complex usage scenarios. This complexity can create problems for users who are trying to assess the risks associated with sharing data. In addition, the added complexity makes it difficult to draft accurate and comprehensive privacy policies.[24] *Second*, the ease with which network formation is accomplished means that social networks are often more expansive than one might expect, leading users to misjudge their actual exposure.[25] *Third*, there is evidence that leakage of personal information to third party servers and applications occurs in many social networking applications.[26] In particular, social networking systems often make use of third party advertising servers, which receive personal information about users in order to provide targeted advertising. Since a small group of companies has captured a large share of the market, the providers of these services are often in a position to aggregate data drawn from multiple websites.

Lastly, the use of PHR to store personal information leads to a problem regarding legal recourse in the case of misuse, unauthorized disclosure or loss of integrity. Unlike financial losses, incidents involving PHI are difficult to value; the lack of even vague estimates on the value of misused PHI means that it is difficult

---

23 *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001*, Pub. L. 107-56, 115 Stat. 272 (2001).

24 See H.M. Kienle, A. Lober, and H.A. Muller, "Policy and Legal Challenges of Virtual Worlds and Social Network Sites" *eprint arXiv:0808.1343* (9 August 2008) online: <http://arxiv.org/PS_cache/arxiv/pdf/0808/0808.1343v1.pdf>.

25 See R. Gross, A. Acquisti, and H.J. Heinz, "Information revelation and privacy in online social networks" (2005) Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society WPES '05 71.

26 See B. Krishnamurthy and C. Wills, "On the leakage of Personally Identifiable Information Via Online Social Networks" (2009) WOSN, online: <http://www2.research.att.com/~bala/papers/wosn09.pdf>.

to assess damages. The same difficulties in valuation make privacy breaches difficult to indemnify, as evidenced by the general lack of insurance products for this type of loss.

(b) Trust

In addition to issues concerning privacy and security, PHR systems demonstrate some notable challenges in the area of trust. First, and most obviously, there are several issues that arise with respect to trust from a user perspective. For instance, if a user adds a care provider such as a physician or occupational therapist to her care team, she trusts that the user account corresponding to the care provider is actually owned by someone licensed to practise medicine. Indeed, there is a possibility for duplicitous individuals or companies to create fake accounts on PHR systems, in order to eavesdrop, obtain data from patients, or provide suggestions on treatments. Current policies to verify the authenticity and credentials of professional caregivers range from simply clicking a button in order to "attest" to be a licenced physician (e.g., Medting.com) up to requiring a licence registration number, which is then cross-checked with the medical association that issued it (e.g., the CMA's Asklepios.ca).

Moreover, users need to trust that the recommendations provided by online care providers are unbiased by commercial interests or, at the very least, that any potential bias has been disclosed to them. The Health on the Net (HON) foundation has developed a code of ethical conduct and a certification process for addressing this issue (HONcode). Online care providers can apply for an HONcode certificate, which they can publish on their profiles.

In addition to these issues, there is a larger concern about the *trustworthiness of the information* contained in a PHR. A recent survey of Chief Executive Officers of Canadian acute care hospitals indicated that patient literacy was considered a very important barrier for the introduction of patient-accessible electronic health records.[27] There is a widespread perception that health data entered by patients cannot be relied upon. Kim *et al.* conclude that this is of particular concern in those target demographics that would most benefit from Internet-based health services, e.g., elderly patients with low income.[28] Empirical studies have shown that the accuracy of patient-entered data varies based on the type of the information provided, and the format it is provided in.[29]

Moreover, the *provenance* of the information entered has shown to be an important indicator for its trustworthiness. For example, patients entering laboratory information from a primary source (printed lab report, hand written note, or mem-

---

27 S. Urowitz *et al.* "Is Canada ready for patient accessible electronic health records? A national scan" (2008) 8:33 BMC Medical Informatics and Decision Making.

28 E. H. Kim *et al.* "Challenges to using an electronic personal health record by a low-income elderly population" (2009) 11:4 Journal of Medical Internet Research e44.

29 See M. I. Kim and K. B. Johnson, "Patient entry of information: evaluation of user interfaces" (2004) 6:2 Journal of Medical Internet Research e13. For example, information about diagnoses provided in text form proved to be quite accurate, while information about therapy goals (free text or selected from a predefined list) proved to be less accurate.

ory recollections) generate information with different levels of trustworthiness. The PHR may also require the user to "translate" or "abstract" the raw laboratory data contained on the lab report in order to fit it in the patient record. The level of guidance on these abstraction steps provided by the PHR influences the trustworthiness of the entered data.

Finally, PHRs may contain data that was uploaded directly from a laboratory of a professional care provider. However, without information about the provenance of this information, this data may be indistinguishable from patient-provided information. The inclusion and maintenance of "meta health data" (i.e., data about the context of the actual health data) in PHR applications may be a partial answer to this problem. Standards for representing such meta data have been developed by organizations such as Health Level 7 and OpenEHR. However, few current PHR systems make use of them.

(c) Integration and Interchange

If a PHR system is used merely as a patient-managed record of health information, (as in the isolated PHR scenario), integration with health care provider business processes and information systems is straightforward. In this case, the patient can print out information, upload diagnostic reports, and grant access to physicians via a hosted, online interface. Issues of trust and provenance apply, but the health care provider does not need to worry about integrating their technical systems with the PHR.

In contrast, a range of issues arise when a PHR is used as a data sink or data source. In the data source scenario, health authorities and hospitals may have standards or guidelines concerning minimum thresholds for data quality. In the data sink scenario, most health care providers in Canada manage the risks involved in sharing PHI with other entities through the use of information sharing agreements.[30] Since many PHR vendors are a) not health care providers, and b) likely located in other legal jurisdictions, drafting agreements for data sharing with PHR systems is likely to be more complicated. Some health authorities may also be concerned about the workload involved in accommodating PHR systems within their business practices.

Even if the appropriate contractual provisions are in place, interchange of data requires that the health care provider's information systems communicate with the PHR. In the almost certain absence of a shared data model, the two systems require a means of exchanging information that allows transformation of the data, while preserving the semantics. Such messaging middleware exists, but is not particularly widespread in Canada.

Putting aside concerns about interoperability between the information systems of health care providers and the PHR, there is an additional interoperability issue — namely, the ease with which information may be transferred between competing PHRs. If PHRs are analogous to social networking applications, the costs of switching providers are quite high. A user who is thinking of switching to a competing PHR system is faced with the daunting task of migrating their personal information. If this is a manual process, the effort could be substantial, yielding a

30 Also known as "personal information transfer agreements."

disincentive for patients to change, even in the face of questionable security and privacy practices.

III. THE REGULATORY LANDSCAPE IN CANADA

(a) Overview

The provision of health care in Canada is generally a joint responsibility between the federal and provincial governments, as it is not an enumerated category within the division of powers listed in sections 91 and 92 of the *Constitution Act, 1867*.[31] As a result, both levels of government may pass legislation concerning health. In the words of the Supreme Court of Canada, "Health is not a matter which is subject to specific constitutional assignment but instead is an amorphous topic which can be addressed by valid federal or provincial legislation, depending in the circumstances of each case on the nature and scope of the health problem in question."[32] In practice, the precise boundary of federal and provincial authority over health care has been contested, and is not capable of being summarized in the present work.[33]

In terms of the practical distribution of responsibilities, the provincial governments generally have authority over the administration of health care organizations, including hospitals, laboratories and long-term care facilities. In addition to providing (partial) funding for provincial health care, the federal government takes responsibility for a number of programs and legislative instruments. Several federal statutes relate to public health concerns, including the *Quarantine Act*[34], the *Hazardous Products Act*[35] and the *Food and Drugs Act*.[36] The federal government also has authority over First Nations groups, under subsection 91(24) of the *Constitution Act, 1867*. While Health Canada provides primary health care to hundreds of First Nations communities, the federal government also provides transfer payments as a means of fulfilling its responsibilities.

At the provincial level, Legislatures have passed statutes aimed at regulating health care providers, including hospitals, self-regulating professions, mental health facilities, ambulance services, and provincial insurance programs. Many of these organizations have also promulgated bylaws or codes of conduct that are binding upon their employees or members. Lastly, common law judgments have not only created non-statutory law, but have provided interpretations of key provisions and terms in the various instruments.

The following subsections introduce a subset of the instruments that are relevant to health information management — namely, privacy statutes, health infor-

---

31 (U.K.), 30 and 31 Vict., c. 3, reprinted in R.S.C. 1985, App. II, No.5.

32 *Schneider v. British Columbia*, [1982] 2 S.C.R. 112 at 142 (S.C.C.).

33 For a discussion, see Martha Jackman, "Constitutional Jurisdiction over Health in Canada" (2000) 8 Health L.J. 95.

34 R.S.C. 1985 c. Q-1 / S.C. 2005, c. 20.

35 R.S.C. 1985, c. H-3.

36 R.S.C. 1985, c. F-27. For a discussion of various federal statutes, see Tracy M. Bailey, Timothy Caulfield, and Nola M. Ries, *Public Health Law and Policy in Canada* (Toronto: LexisNexis Butterworths, 2005) at 12.

mation statutes, medical device regulations, and industry-promulgated standards.

(b) Privacy Statutes

(i) Background

The protection of privacy in Canada arises from a patchwork of statutes, regulations, bylaws, judicial/administrative decisions, codes of conduct, and industry standards. With respect to data protection law, the most relevant instruments are the various privacy statutes; there are no less than 23 privacy statutes in Canada, some of which are devoted exclusively to the protection of health information. In general, the Canadian statutes take their inspiration from a set of "fair information practices" first developed by the Organization for Economic Cooperation and Development (OECD). In response to Canada becoming a signatory to the *OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*,[37] the Canadian Standards Association (CSA) promulgated the *Model Code for the Protection of Personal Information* in 1996.[38] While the federal government had already passed a privacy statute binding on federal public bodies,[39] the development of a statute for the private sector was given impetus by a directive of the European Union[40] that prohibited member states from transferring data to jurisdictions with inadequate privacy protection.

The *Personal Information Protection and Electronic Documents Act*[41] (PIPEDA) is a federal statute that applies to private sector organizations. PIPEDA was originally described as a means for enhancing consumer confidence in electronic commerce applications, by means of protecting the personal information involved in transactions. Despite the focus on electronic commerce, the scope of the legislation is much more expansive than this narrow description implies. PIPEDA contains provisions that regulate the collection, use and disclosure of personal information in a wide variety of additional contexts. Lastly the statute explicitly incorporates the CSA *Model Code* in the form of a schedule (Schedule 1) that lays out 10 fair information principles.

(ii) Applicability

In terms of applicability, subsection 4(1) of PIPEDA makes it clear that the statute applies to every organization in respect of personal information that (a) "the organization collects, uses or discloses in the course of commercial activities", or; (b) "is about an employee of the organization and that the organization collects, uses or discloses in connection with the operation of a federal work, undertaking or

37 (23 September 1980) Organization for Economic Co-operation and Development.

38 Standards Council of Canada, CAN/CSA-Q830-96 [Model Code].

39 The federal *Privacy Act* came into force on July 1, 1983.

40 Directives E.C., "On the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data" [24 October 1995] O.J. L. 95/46.

41 S.C. 2000, c.5.

business".[42] Since PHR systems like HealthVault and Google Health are not related to federal works, undertakings or businesses,[43] applying PIPEDA to these services involves an examination of whether the vendor organization qualifies as an "organization that collects, uses or discloses personal information in the course of conducting commercial activities." The following subsections explicate some of the concepts that appear in this provision.

(A) Personal Information

Subsection 2(1) of PIPEDA states that the term "personal information" means "information about an identifiable individual."[44] The key concept at work in this definition is that information is personal if it can be traced back to an individual by a third party. The definition is expansive, in that it allows a wide variety of information to count as personal; in particular, third parties may be possessed of *background knowledge* — information that provides enough context to make the identification of the individual feasible.[45]

Information contained within PHR systems typically includes demographic information, as well as different types of health information. Due to the presence of the former, it would be quite likely than a third party coming into possession of the

---

42 In addition, Section 4(2)b of PIPEDA states that the privacy regulations contained in its first Part do not apply to "any individual in respect of personal information that the individual collects, uses or discloses for personal or domestic purposes and does not collect, use or disclose for any other purpose". At first glance, condition (a) of Subsection 4(1) may appear to be ultra vires, as the *Constitution Act, 1867* assigned to provincial governments the ability to pass laws related to property and civil rights. However, the federal government was assigned the power to regulate trade and commerce. A detailed analysis of these issues is found in W. Charnetsky, P. Flaherty, and J. Robinson, *The Personal Information Protection and Electronic Documents Act: A Comprehensive Guide*, (Aurora: Canada Law Book, 2001). At present, it suffices to remark that the federal government has some authority to regulate interprovincial and international trade and commerce, as well as trade which affects the whole nation. It is those powers which ground the federal government's claim that PIPEDA applies to transactions across international or provincial borders.

43 The question as to whether pan-Canadian health records systems could conceivably qualify as federal works, undertakings, or businesses for the purpose of PIPEDA is not considered in this paper.

44 The name, title, business address, and telephone number of an employee of an organization are expressly excluded from this category, thereby providing employers with the ability to disseminate workplace contact information freely.

45 As an example, a patient's provincial medical insurance number readily allows a third party to identify an individual, since there is a one-to-one mapping between it and the set of Canadian citizens. On the other hand, a patient's date of birth and surname may only give a third party a probabilistic inference as to the identity of the individual, since more than one person may have the same surname and birth date. If the third party comes into possession of a second database that includes dates of birth, surnames and postal codes, the probability of identifying the patient is increased.

contents of a PHR record could identify the individual to whom it belongs.[46] As a result, the contents of the PHR will generally count as personal information under PIPEDA. There are ways, however, for vendors to avoid this conclusion. If the data in the PHR is encrypted, a third party (lacking the decryption key) would be unable to make any sense of the contents.[47] PHR architectures that provide encryption against the platform are a subject of current research; given the existing literature, it would not be surprising to see reference architectures emerge within the next five years.[48]

(B) Organization

Subsection 2(1) of PIPEDA defines an "organization" to include "an association, a partnership, a person and a trade union." Given the interpretative strictures contained in subsections 33(1) and 35(1) of the *Interpretation Act*,[49] the definition of an organization therefore covers corporate entities, including non-profit societies. This is a fortuitous development from a regulatory perspective, as many vendors of PHR applications are corporations (e.g., Google) and non-profits (e.g., PatientsLikeMe).[50] On this front, the Privacy Commissioner has stated that the legal nature of an organization is not determinative of whether it is bound by PIPEDA. In particular, a non-profit organization may still be caught, as the following excerpt

---

46 Unfortunately, the type of binary distinction between "identifiability" and "non-identifiability" endorsed by modern privacy law has major deficiencies when applied to datasets. One of the problems is that the background knowledge of a third party is not restricted in any way. As a simple example, I may happen upon a piece of paper which gives blood pressure readings for a particular date (yesterday). In the absence of other knowledge, I cannot locate the patient based on the blood pressure reading alone. However, imagine that I live in a small town. While in a coffee shop I overheard someone describe the results of yesterday's blood pressure check at the local clinic. Assuming the results match those that I found on the piece of paper, I am certainly justified in inferring that I have found the owner of the record. However, absent that serendipity, I would have a hard time making any inferences. The fact that PIPEDA allows the "identifiability" of the record to be determined by such slim possibilities is a deficiency in the law.

47 Technically, the third party could conduct one of several forms of attacks, one of which would involve attempting to ascertain the key. In general, it is not possible to guarantee that the attacker cannot succeed.

48 Partial solutions to this issue have been provided in the context of social networking applications by a number of authors, including M. M. Lucas and N. Borisov, "FlyByNight: mitigating the privacy risks of social networking" (2008) Proceedings of the 7th ACM Workshop on Privacy in the Electronic Society WPES 08 1.

49 R.S.C. 1985 c. I-21. For instance, subsection 35(1) states that the word "person", or any word or expression descriptive of a person, includes a corporation.

50 Even if a vendor is a private sector corporation, the rationale for offering PHR services can vary. For instance, Google and Microsoft have different financial strategies underlying their offerings. For a discussion, see P.C. Tang and T.H. Lee, "Your doctor's office or the Internet? Two paths to personal health records" (2009) 360:13 The New England Journal of Medicine 1276.

demonstrates:

> The first matter to address is that of jurisdiction. [The Law School Admission Council] contends that it is not engaged in any commercial activities for the purpose of [PIPEDA]. In support of this position, LSAC relies on "its status as a non-profit, non-stock organization, its membership and governance structure and the public policy aspect in providing an education-related mechanism to assess individuals seeking to enter a regulated profession to practice law."[51]
>
> LSAC's status as a non-profit, non-stock, membership-based organization is not determinative. [PIPEDA] applies to organizations, defined in section 2 as including "an association, a partnership, a person and a trade union." There is no exemption for non-profit or member-oriented organizations. To the contrary, the definition of "commercial activity," namely, "any particular transaction, act or conduct or any regular course of conduct that is of a commercial character, including the selling, bartering or leasing of donor, membership or other fundraising lists," makes clear Parliament's intention that the *Act* apply to commercial transactions that non-profit, membership-based organizations might engage in.

As a result of this reasoning, both corporate and non-profit providers of PHR services can qualify as organizations within the context of PIPEDA. Subsection 4(1) makes it clear, however, that not every organization collecting personal information is caught by the statute; only organizations that collect, use, or disclose personal information in the course of conducting commercial activities are subject to PIPEDA.

(C) Collection, Use, Disclosure

It is not clear that PHR vendors will necessarily collect, use, or disclose personal information. Recalling the four PHR scenarios outlined above, an isolated PHR system is a mere repository of information, where data exchange is performed manually by the account holder. Patients upload information, and have exclusive control over what is subsequently accessed. In such a case, the basic processes of data management are completely different from organizations such as hospitals, marketing agencies or worker's compensation boards. In the words of the Privacy Commissioner, commenting on a similar issue with respect to social networking sites:

> The purpose of the *Act* is to balance an organization's need to collect, use and disclose personal information for appropriate purposes with the individual's right to privacy vis-à-vis their personal information. In the off-line world, organizations may collect particular personal information, and use and disclose such personal information, in order to provide a specific service. On Facebook, users decide what information they provide in order to meet their own needs for social networking.[52]

From a user perspective, entry of data into a PHR system is either accomplished by the patient herself, or (in a data sink approach) by a health care provider.

---

51 PIPEDA Case Summary #2008-389 (Report of Findings).

52 *Supra* note 7.

The vendor of the PHR system does not play a role in actually collecting data. In addition, it is not clear that every PHR vendor will use or disclose data. While it is true that some websites (e.g., PatientsLikeMe) disclose information to commercial partners, it is not necessarily the case that PHR vendors intend to use or disclose PHI in such a manner.[53] The determination of whether a PHR vendor is "using" or "disclosing" for purposes of PIPEDA seems to be contingent, and impossible to specify a priori.

(D) Commercial Activities

The last task remaining in our application of clause 4.1(a) to PHR vendors involves a determination of whether they are engaged in "commercial activities". Subsection 2(1) of PIPEDA defines this term (perhaps unhelpfully) as "any particular transaction, act or conduct or any regular course of conduct that is of a commercial character, including the selling, bartering or leasing of donor, membership or other fundraising lists". As stated by the Commissioner in a recent speech, the moment a PHR or social networking application vendor uses information for commercial purposes, the law applies and the organization becomes responsible for safeguarding the data.[54]

As detailed above, a non-profit agency can engage in commercial activities. Conversely, one might wonder about the implications of for-profit business entities engaging in non-profit activities, such as hosting PHR systems. A recent report by the Commissioner on Facebook reveals a surprisingly expansive view of the activities that count as commercial:

> [P]ersonal information posted by individuals for purely personal purposes that would otherwise be exempted under the *Act* does fall under the *Act* and imposes obligations on Facebook to the extent that Facebook uses such personal information in the course of commercial activities. There is no conflict between the same information being both for personal purposes and commercial purposes.
>
> . . .
>
> It is reasonable to assume that those features of the site that do not have an obvious link to its business model are included to enhance the user's experience on Facebook. Enhancing the experience likely encourages existing members to continue to use the site and presumably encourages others to join as well — thereby indirectly contributing to the success of Facebook as a commercial enterprise. In that sense, collection, use and disclosure of personal information in relation to a feature without an apparent direct commercial link can still be characterized as occurring "in the course of com-

53 As we noted in the section on privacy and security issues, the temptation to use or disclose PHI may be quite strong. Despite the bona fide intentions of an organization, unauthorized use and disclosure remains a security and privacy risk.

54 "Facebook users themselves are the ones who decide what information they are willing to post on the site to carry out their social networking. That information in itself does not fall under PIPEDA". J. Stoddart, "When Everyone and Their Mother is a Content Provider: The Principle of Privacsy at the Heart of the Social Revolution" (2010) Remarks at the CRIM Crystal Ball Conference.

mercial activity" in the sense required under the *Act*.[55]

Given this decision, as well as the purposive approach to statutory interpretation urged by the Supreme Court,[56] it does not seem far-fetched to assume that the Commissioner would likely view a non-profit PHR initiative from a for-profit vendor as constituting "commercial activity" within the sense required by PIPEDA.

(E) Jurisdiction and Online Services

It is likely that Canadians using PHR systems will be transmitting data across jurisdictional boundaries. As mentioned above, the division of powers can be invoked to argue that PIPEDA should apply to interprovincial and international flows of information. Both administrative decisions and federal court jurisprudence are in consonance with this approach.

Canadian jurisprudence on the jurisdictional reach of the provincial courts is typically attributed to *Morguard Investments Ltd. v. De Savoye*,[57] in which the Supreme Court was tasked with adjudicating a dispute over whether a court in British Columbia could recognize and enforce decisions from a court in Alberta. The majority decided that courts in a province may recognize and enforce judicial decisions made by courts in a different province, provided the latter properly (or appropriately) exercised jurisdiction. In order to aid with this determination, the court introduced a test for the appropriate exercise of jurisdiction, by which there must be a "real and substantial connection" between the jurisdiction and the issue in question.

Subsequent cases have extended the decision in Morguard. In *Beals v. Saldanha*,[58] the court concluded that the Morguard principles should be extended beyond interprovincial scenarios, so that the "real and substantial connection" test should also apply to the enforcement of foreign judgments. In *Disney Enterprises Inc. v. Click Enterprises Inc.*,[59] the court considered the case of an Ontario-based online content provider taken to court in New York. In the course of deciding that the Ontario courts could enforce the damage award set by the US court, (which had exercised proper jurisdiction), Justice Lax stated that the determination of the proper exercise of jurisdiction by a court depends on two principles: the need for order and fairness and the existence of a real and substantial connection to either the cause of action or the defendant. The first principle is met in a case involving multiple jurisdictions when there are "reasonable grounds for assuming jurisdiction". In particular, Justice Lax noted that the jurisprudence in Canada supports the view that there is sufficient connection for a foreign court to take jurisdiction where Canada is the "country of transmission or origin."

Lastly, the federal court has explicitly considered the issue of whether the fed-

---

55 *Supra* note 7.

56 See, for example, *Bell ExpressVu Ltd. Partnership v. Rex*, 2002 SCC 42, [2002] 2 S.C.R. 559 (S.C.C.).

57 [1990] 3 S.C.R. 1077, 76 D.L.R. (4th) 256, [1991] 2 W.W.R. 217, 52 B.C.L.R. (2d) 160 (S.C.C.).

58 2003 SCC 72, [2003] 3 S.C.R. 416 (S.C.C.).

59 (2006), 267 D.L.R. (4th) 291, 49 C.P.R. (4th) 87 (Ont. S.C.J.).

eral privacy commissioner has jurisdiction to investigate complaints concerning privacy issues arising from cross-border information flows. *Lawson v. Accussearch Inc.*[60] was an application for judicial review of a decision by the commissioner to the effect that she did not have jurisdiction to investigate issues pertaining to cross-border information flows, as any investigation would require the use of her powers extra-territorially. The court held that although Parliament had not intended for the commissioner to act extraterritorially, PIPEDA could apply where the dispute was "sufficiently connected to Canada to ground the exercise of Canadian jurisdiction".

Simply put, the fact that a given vendor or service provider is located in a foreign jurisdiction will not exempt it from the scope of the law. In *Lawson*, the federal court held that PIPEDA could still apply to foreign entities that either receive or transmit communications to or from Canada, and that collect or disclose information about individuals in Canada. The success of the Commissioner's investigation of Facebook was ample demonstration that PIPEDA can apply to the commercial collection, use and disclosure of personal information by foreign entities operating in cyberspace.

Despite the decision in *Lawson*, Canadian regulatory authorities can only bring their weight to bear on threats that they are made aware of. In addition to issues of monitoring, whistleblower protection and feedback mechanisms, a major issue in the design of regulatory systems consists of statutes that prevent data custodians from alerting their stakeholders about access requests by government agencies. For example, Information and Privacy Commissioner of British Columbia conducted an extensive investigation into the *Patriot Act*, in response to concerns that Canadian subsidiaries of US companies could be compelled to (silently) hand over the personal information of British Columbians.[61] The final report states that in the absence of appropriate (American) safeguards concerning requests for information by US authorities, it is prudent to assume that a) US authorities are unfettered in their ability to seek an order for disclosure of records pertaining to Canadians, and; b) they may do so in circumstances that are not consistent with Canadian law and policy. While the report contained 16 concrete recommendations for the British Columbia government, it mentioned that the *Patriot Act* is "also an issue for the private sector and will have to be addressed by all jurisdictions across Canada and at an international level."[62]

(iii) Implications

The analysis above leads us to conclude that many PHR vendors will be subject to PIPEDA. Despite this result, there are some challenges in applying that statute to PHR systems. PIPEDA was clearly not designed to cover information systems in which individuals manage their own information, engaging in selective and

60 2007 FC 125, [2007] 4 F.C.R. 314 (F.C.).

61 Information and Privacy Commissioner of British Columbia, *Privacy and the USA Patriot Act: Implications for British Columbia Public Sector Outsourcing* (2004), online: <http://oipc.bc.ca/sector_public/archives/usa_patriot_act/pdfs/report/privacy-final%20summary.pdf>.

62 *Supra* note 61 at 18.

voluntary disclosure to third parties.[63]

First, PIPEDA contains a host of provisions and guidelines surrounding the collection of personal information (PI). Both subsection 7(1) and the Schedule 1 "Consent" principle impose restrictions on the ability of organizations to collect PI without knowledge and consent. The "Identifying Purposes" principle states that the purposes for which PI is collected shall be identified at or before the time of collection. Lastly, the "Limiting Collection" principle dictates that organizations may only collect the minimal amount of PI necessary to fulfill these explicitly stated purposes. Given that PHR systems involve patients voluntarily contributing PI and PHI, the constraints enumerated above are largely irrelevant.[64]

Second, many of the remaining PIPEDA principles are of questionable utility when applied to PHR systems. The "Access" and "Accuracy" principles do not appear to be relevant, while the "Openness" and "Challenging Compliance" principles impose easily discharged burdens on vendors. Retention periods are mentioned in the model code, but the organization is allowed to determine guidelines and procedures (and presumably any retention periods not mandated by other legal instruments). Lastly, the fact that PIPEDA lacks breach notification requirements means that vendors are not under a general duty to warn users of privacy breaches.

Despite these difficulties, PHR systems do not evade PIPEDA's reach entirely. First, the "Safeguards" principle holds that information shall be protected by "security safeguards appropriate to the sensitivity of the information." In particular, the safeguards must protect against loss or theft, as well as unauthorized access, disclosure, copying, use or modification. The nature of the protection should include (a) physical measures, (b) organizational measures, and (c) technological measures. The principle also dictates that employees of an organization receive training concerning confidentiality, and that care shall be used in the disposal or destruction of data.

Second, PIPEDA does contain provisions that could be used to limit *the use and disclosure of information* stored in PHR systems:

- The "Limiting Use, Disclosure and Retention" principle specifies that personal information shall not be used or disclosed for purposes other than those for which it was collected, except with consent or where re-

63 PIPEDA, s. 3 states that the aim of the statute is to establish

> rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.

It is by no means clear that PHR vendors have a need to collect, use or disclose any personal information at all.

64 As noted in S. Perrin *et al., The Personal Information Protection and Electronic Documents Act: An Annotated Guide*, (Toronto: Irwin Law Inc. 2001), data protection legislation aims at providing individuals with a legal right to control the collection, use, and disclosure of their personal information. The most important stage in a business process is therefore the collection of information, as it becomes more difficult to exert control once the data have been collected.

quired by law. Information may only be retained as long as necessary for the fulfillment of those purposes; information that is no longer required to fulfill these purposes should be destroyed, erased or made anonymous.

- The "Identifying Purposes" principle's clause 4.2.4 states "when personal information that has been collected is to be used for a purpose not previously identified, the new purpose shall be identified prior to use. Unless the new purpose is required by law, the consent of the individual is required before information can be used for that purpose."

Although one could argue that information in a PHR has not been "collected," a purposive interpretation would likely accommodate PHR vendors within the scope of these principles. Subsection 5(3) of PIPEDA also provides a purposive limitation, as it states that "[a]n organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances." The test for appropriate purposes is therefore contextual and objective, providing some impartiality for claimants wishing to dispute information management practices.[65]

In addition, the "Consent" principle states that "[t]he knowledge and consent of the individual are required for the collection, use or disclosure of personal information, except where inappropriate." As pointed out by Perrin *et al.*[66], the phrase "except where inappropriate" does not lend itself well to statutory interpretation. As a result, the drafters of PIPEDA introduced three lists in subsections 7(1), 7(2) and 7(3) that are intended to provide an exhaustive list of cases where it would be inappropriate to obtain knowledge and consent. Of these exceptions, the most salient consist of use and disclosure for research purposes. However, such use or disclosure is only permitted if certain conditions are met, providing patients with some assurance that their information will not be accessed by researchers in an ad hoc fashion.[67]

Third, the PIPEDA principles impose certain *administrative obligations* on PHR vendors. Clause 4.9.1 of the "Individual Access" principles provides individuals with a right to request an account of the uses that have been made their information, as well as an account of the third parties to which it has been disclosed. Clause 4.1.3 of the "Accountability" principle mandates that PHR vendors use "contractual or other means" to provide a comparable level of protection when information is

---

65 From the Commissioner's findings, it appears as though the test for appropriate purposes is evolving to include a series of questions similar to those involved in *R. v. Oakes*, [1986] 1 S.C.R. 103 (S.C.C.). As an example, in PIPEDA Case Summary #2006-351 the Assistant Commissioner considered the following questions in determining the appropriateness issue:

1. Is the measure demonstrably necessary to meet a specific need?
2. Is it likely to be effective in meeting that need?
3. Is the loss of privacy proportional to the benefit gained?
4. Is there a less privacy-invasive way of achieving the same end?

66 *Supra* note 64.

67 A full discussion of this exception is beyond the scope of this paper.

sent to third parties for processing. Clause 4.1.4 of the same principle obligates vendors to implement procedures to protect personal information.

The most unique provision from the standpoint of PHR systems is subsection 9(1), which states that an organization must not give an individual access to personal information if doing so would likely reveal personal information about a *third party*. The same provision goes on to state that if the information about the third party is severable from the record containing the information about the individual, the organization must sever the information about the third party before giving the individual access. As mentioned above, the hereditary nature of many conditions entails that third parties can often receive information on individuals by obtaining knowledge of health conditions of their family members.

(c) Health Information Statutes

(i) Background

Certain provinces have devised statutes and regulations specific to health information. Typically, these instruments seek to maintain coherence with fair information practices, while accounting for the unique demands of the health care domain. Since Ontario's *Personal Health Information Protection Act*[68] (PHIPA) is a well-known example of a health information statute, it will ground the discussion below.

PHIPA is designed to protect patients by imposing constraints on the collection, use, and disclosure of PHI. In large part, the development of the statute was prompted by a desire on the part of health care providers to create a regulatory regime that was tailored to the unique needs of the health care industry. As a result, health providers in Ontario that are subject to PHIPA have received an explicit exemption from the applicability of PIPEDA.[69]

PHIPA provides for a number of fair information practices. *First*, a patient has a right to access their PHI, and to correct any information that is inaccurate. *Second*, organizations subject to PHIPA must be open about their information practices, and must inform patients of their ability to make complaints to both the organization itself, and to the Ontario Privacy Commissioner. *Third*, the statute includes special procedures for consent, tailored to match the reality of health care as an industry that relies upon relatively fluid and unpredictable exchanges of information between specialists. Fourth, the statute contains breach notification provisions that require organizations to inform a patient at the first reasonable opportunity if the patient's information is compromised. Fifth, PHIPA requires organizations to take reasonable steps to ensure the accuracy of PHI, and to ensure that it is retained, transferred and disposed of in a secure manner.[70]

In terms of application, the weight of PHIPA generally falls on a set of health care providers, referred to in the legislation as "health information custodians", as well as their agents. However, PHIPA also contains provisions for "providers," per-

68 S.O. 2004, c.3, Sch. A and its accompanying regulations O. Reg. 329/04.

69 S.O.R./2005-399, made under PIPEDA.

70 The five aforementioned principles are, of course, not the only ones enshrined in the statute, and we will discuss additional issues in the sections to follow.

sons who provide "goods or services for the purpose of enabling a health information custodian to use electronic means to collect, use, modify, disclose, retain or dispose of [PHI]".[71] A refinement of a provider is a "health information network provider," a "person who provides services to two or more health information custodians where the services are provided primarily to custodians to enable the custodians to use electronic means to disclose [PHI] to one another . . ."[72]

(ii) Applicability

Addressing the status of *private sector PHR vendors* under PHIPA involves characterizing the role that vendors play in the management of health care information.[73] As a starting point, subsection 7(1) states that PHIPA applies to the collection of PHI by a health information custodian, as well as the use or disclosure of PHI by i) a health information custodian, or ii) a person who is not a health information custodian and to whom a health information custodian disclosed the information. A private sector organization that provided PHR services to residents of Ontario would not qualify as a "health information custodian" under PHIPA, as neither section 3 of PHIPA nor its accompanying regulations seem to support such a claim. This is unfortunate for regulators, as many of the key provisions in PHIPA attach exclusively to health information custodians.[74]

Despite the conclusion that PHR vendors do not appear to qualify as health information custodians, they will be caught by subsection 7(1) if they are a person to whom a health information custodian has disclosed PHI.[75] Section 49 imposes two obligations on such recipients of PHI. *First*, the recipient must not use or disclose the information for any purpose other than (a) the purpose for which the custodian was authorized to disclose the information under PHIPA, and (b) the purpose of carrying out a statutory or legal duty. *Second*, the recipient must not use or disclose more of the information than is "reasonably necessary to meet the purpose of the use or disclosure," unless the use or disclosure is required by law.

In addition to treating a PHR vendor as a data recipient, a regulator attempting to bring a PHR system within the ambit of PHIPA could attempt to characterize the vendor as a person who provides "goods or services for the purpose of enabling a health information custodian to use electronic means to collect, use, modify, dis-

71 PHIPA, s. 10(4).

72 O. Reg. 329/04, s. 6(2).

73 Due to space constraints, a discussion of public sector PHR initiatives is beyond the scope of this paper.

74 For instance, section 10 requires health information custodians to follow PHIPA-compliant information practices. Subsection 11(1) requires a custodian to take reasonable steps to ensure that PHI is accurate, complete and up-to-date as is necessary for the purposes for which it uses the information. Subsection 12(1) requires custodians to take steps that are reasonable in the circumstances to ensure that PHI in the custodian's custody or control is protected against theft, loss and unauthorized use or disclosure. Under that provision, the custodian must also ensure that records containing the information are protected against unauthorized copying, modification, or disposal.

75 In our terminology, a PHR vendor will be caught by subsection 7(1) if the PHR is following either the data sink or interoperable PHR models.

close, retain or dispose of [PHI]". Despite the initial appeal, it is not clear that PHR vendors are providing a service by which custodians may store PHI in electronic form, as opposed to providing a service by which patients may manage their own health information.[76] Even less promising is the claim that a PHR vendor is a "health information network provider" under PHIPA — a person who provides "services to two or more health information custodians where the services are provided primarily to custodians to enable the custodians to use electronic means to disclose [PHI] to one another." The primary purpose of a PHR product (even one used as a data sink and data source by custodians) is not to transfer PHI between health care providers, but to empower patients to manage their own information.[77]

Lastly, PHIPA is a provincial statute that regulates the collection, use, and disclosure of personal health information by a specific class of entities within the province of Ontario. Since many online PHR systems furnished by private sector vendors will serve multiple jurisdictions, it is not clear that PHIPA will apply to the majority of PHR offerings.

(iii) Implications

As demonstrated above, private sector PHR vendors are caught in a fairly minimal fashion by PHIPA. If a PHR system obtains information directly from a health information custodian, the vendor of the system is under an obligation not to use or disclose that information for any purpose other than to facilitate the patient's management of her own health information. Nor should the vendor use or disclose more information than necessary to meet this purpose. However, if the patient uploads information into the PHR system, then PHIPA is silent.

The fact that PHR systems fall outside the ambit of Ontario's health information legislation is not unique. Indeed, PHR systems do not appear to qualify under British Columbia's new e-health law, as vendors of these systems do not appear to be a "health care body" within the meaning of the BC *Freedom of Information and Protection of Privacy Act*.[78] In the United States, such vendors are also outside the scope of the *Health Insurance Portability and Accountability Act*.[79]

---

76 In a PHR system, control over the content of a patient record rests with the patient. The fact that health care providers may have access to a patient's records through the vendor's product is not determinative, since such access permitted on the basis of the patient's express consent alone.

77 This is unfortunate for regulators, as subsection 6(3) of PHIPA regulation 329/04 contains a strong set of information management requirements, including provisions that mandate audit logging, impact assessments, security assessments, and agreements with third parties.

78 R.S.B.C. 1996, c. 165.

79 Pub. L. 104-191, 110 Stat. 1936 (1996). See, e.g., E. Rakestraw, "One Size Doesn't Fit All" (2009) 30 J. Legal Med. 269. Recent legislation in the United States of America may have changed this situation.

(d) Medical Device Law

(i) Background

The government of Canada has promulgated regulations[80] concerning medical devices, under the auspices of the *Food and Drugs Act*. Any organization that intends to import or sell a medical device in Canada is subject to a mandatory licensure regime. The requirements for licences, and the obligations accruing to the organization, depend upon the risk category of the device, and whether the organization is a manufacturer, retailer, distributor, or importer.

Section 2 of the *Food and Drugs Act* defines a "device" as any article, instrument, apparatus, or contrivance, including any component, part or accessory thereof, manufactured, sold or represented for use in (a) the diagnosis, treatment, mitigation or prevention of a disease, disorder or abnormal physical state, or its symptoms, in human beings or animals; (b) restoring, correcting or modifying a body function or the body structure of human beings or animals; (c) the diagnosis of pregnancy in human beings or animals, or; (d) the care of human beings or animals during pregnancy and at and after birth of the offspring, including care of the offspring.[81]

Schedule 1 of the *Medical Devices Regulations* (the "Regulations") provides rules for four types of medical devices: invasive, non-invasive, active, and special cases. The Regulations also provides four risk levels, known as Classes I, II, III, and IV; the risk level increases with integer value. Class II medical devices (and higher) must be licensed with Health Canada. As part of the licensure process, vendors have to provide objective evidence for the safety and effectiveness of their devices. Class I products do not need to be licensed. However, vendors importing or selling Class I products are required to hold a Medical Device Establishment Licence. Vendors that have acquired product-based licences for all the medical devices they deal with do not have to acquire a separate Establishment Licence.

Different licences also exist for *components* of systems. This is particularly important from a software perspective, as today's software systems are highly interconnected, which causes practical difficulties in defining concrete system borderlines. Medical devices licensed as *components* must be packaged and sold separately from the rest of the system. Class III and higher licences must be renewed in case of a significant change to the medical device. Class II licences are renewed only if the vendor proposes to make a change to the name of the vendor, the name of the device, the device identifier or the medical conditions, purposes or uses for which the device is manufactured, sold, or represented.

(ii) Applicability

Software has long been an embedded component within hardware-based medical devices, (e.g., pacemakers, CT-scanners, drug infusion pumps, etc.). However, there has been a degree of uncertainty in the manufacturing community about the

---

80 The *Medical Devices Regulations*, S.O.R./98-282.

81 The term includes a contraceptive medical device, but does not include a drug. The *Medical Device Regulations* state that the term "medical device" means a "device," as above, but not one intended for use in relation to animals.

role of *purely* software-based products in the regulatory framework. Health Canada has recently issued a notice that explicitly includes any kind of *patient management software* (PMS) as an "active device" under the act. Risk level II is associated with PMS that perform any function above basic data storage and retrieval, e.g., data manipulation, visualization, decision support, etc.[82] In a clarifying note, Health Canada has indicated that PHR systems are indeed patient management software in this regard. Health Canada has announced that it will start enforcing regulatory compliance of Class I patient management software by February 1, 2011, and Class II software by September 1, 2011.

(iii) Implications

Under the regulatory regime for medical devices, organizations that import, sell, or distribute patient management software must hold an *establishment licence*. In order to obtain such a licence, a vendor must provide evidence that documented procedures are in place in respect of distribution records, complaint handling, recalls, and mandatory problem reporting. If an organization sells Class II devices, they must also provide evidence that documented procedures are in place for storage, handling, delivery, installation and servicing of the software product.

In addition to an establishment licence, a *medical device licence* must be obtained for each Class II patient management software product released into the marketplace. These licences require a manufacturer to obtain a certificate showing that its quality management system is compliant with the ISO 13485:2003 standard. In the licence application, the company will provide the product name/identifier, the purpose or intended use of the product, and an attestation that it meets the safety and effectiveness and labelling requirements. The vendor's Quality Management System (QMS) must be documented, and the vendor must provide evidence that it complies with both ISO 13485:2003 and applicable sections of Part I of the Regulations. The vendor must prepare a description of the medical conditions, purposes, and uses for which the patient management software is manufactured, sold, or represented.

In addition to these requirements, the vendor must list any standards applied in the manufacture of the software product, in order to meet the *safety and effectiveness requirements*, found in sections 10 to 20 of the Regulations. Somewhat discordantly, many of the requirements involve concepts foreign to software systems, such as sterilization, flammability, and robustness in the face of transport/storage. Despite this incongruity, the requirements do contain several provisions that apply to software. First, section 20 states that if "a medical device consists of or contains software, the software shall be designed to perform as intended by the manufacturer, and the performance of the software shall be validated." Second, section 12 states that a medical device shall "perform as intended by the manufacturer." Lastly, section 10 confers a duty to ensure that medical devices are designed and manufactured to be "safe." Manufacturers must take reasonable steps to identify the

82 Health Canada, Notice, "Classification of Medical Devices Class I or Class II Patient Management Software" (31 August 2009), online: <http://www.hc-sc.gc.ca/dhp-mps/md-im/activit/announce-annonce/md_notice_software_im_avis_logicels-eng.php>.

risks inherent in the device, and to either eliminate or reduce them.

(e) Standards, Certifications and Industry Guidelines

(i) Background

Canada Health Infoway (Infoway), a federally funded not-for-profit organization tasked with promoting the adoption of eHealth technologies, has recently begun to offer a certification program for "client registries, consumer health application and platforms, immunization registries, and provider registries."[83] Infoway's certification focuses on privacy, security and interoperability; at the time of writing, only general information on the assessment criteria has been made available to the public. They have been based on relatively large set of Canadian, international and US industry standards, codes, and legislation. Interoperability and functionality criteria of eHealth systems applying for certification are assessed based on Infoway's published EHR architecture requirements and technical standards. Infoway intends to generate revenue from their certification services; the organization gives paying companies a time window of 90 days to complete the certification process, starting from the day they receive the assessment criteria package.[84]

In addition to Infoway's efforts, several provinces have initiated certification programs. The main focus of these certifications is on eHealth systems for health care providers (rather than consumer applications). Certifications are typically voluntary but often motivated by significant business incentives. For example, British Columbia subsidizes doctors who install EMR systems that are approved by the Physician Information Technology Office (PITO).

By way of comparison, certification standards for eHealth systems have been introduced in other jurisdictions.[85] As an example, the Certification Commission for Health Information Technology (CCHIT) has been offering a variety of certification programs since 2006. Currently offerings target ambulatory EHRs, inpatient EHRs, emergency department EHRs, and ePrescribing systems. While PHRs are not currently targeted by the official CCHIT certification programs, a PHR certification program is under development and draft criteria have been published. Many of the current EHR certification criteria apply to the PHR context, in particular

---

83 Information on the consumer health application certification process is available online: <http://internet.infoway-inforoute.ca/working-with-ehr/ solution-providers/ certification/what-infoway-certifies/consumer-health-application>.

84 In contrast to other industrial certification programs in other countries (e.g., programs of the U.S. Certification Commission for Health Information Technology), no evidence on existing Infoway-certified products has been published to date. After asking Infoway for details on their assessment criteria for research purposes, we were told that detailed assessment criteria were released only to "bona fide" customers, i.e., paying customers with the intent to use their certification services. This position remained unchanged even after offering to pay for the assessment package, i.e., Infoway did not accept us as a "bona fide" customer.

85 Due to space concerns, we restrict our discussion to the United States. In the European context, EuroRec has a similar mandate for developing certification programs for health information technologies. EuroRec's programs are still under development and currently focus primarily on EHR systems.

those criteria pertaining to authentication, access control, auditing, integrity, and recovery. Additional criteria have been added to require certified PHR systems to notify users of changes to usage policies and give them a means to seek redress from the PHR operators in case they fail to meet performance expectations. The draft standard also includes requirements on how to handle patient consent, proxies (e.g., legal guardians, family members), and third party access to personal health information in PHRs.[86]

(ii) Applicability

At the current time, PHRs and EHRs are sufficiently distinct concepts, offering different functionality, centred on different types of users. Therefore, industry standards pertaining to EHRs do not readily apply to PHRs. Nevertheless, data interoperability between PHRs and EHRs has become an increasingly important objective. As a result, EHR data standards have gained influence over PHR standards and vice-versa. For example, Infoway's EHR architecture (data, security, and privacy requirements) is used as a basis for their certification of consumer health products. As mentioned above, details on Infoway's certification regime are currently unavailable to the public, making it difficult to assess the state-of-the-art with respect to standardization in the Canadian context.

(f) Other Instruments

Health provider organizations such as hospitals and social agencies are subject to confidentiality obligations contained in a variety of statutes, including the *Public Hospitals Act* [87] and the *Home Care and Community Services Act*.[88] While a detailed analysis is beyond the scope of this paper, it is possible that provisions in these instruments may have implications for the dissemination of data contained in PHR systems.[89]

In addition, health care professionals are typically bound by professional codes of conduct, which typically include provisions relating to confidentiality. As an example, the College of Physicians and Surgeons of Ontario is a professional body that has been granted certain powers under the *Regulated Health Professions*

---

86 The draft standard holds that any release of information to third parties requires the express consent of the patient; the PHR service must maintain a proof of contractual Chain of Custody with its third party entities, which includes a) terms by which it shares or exchanges personally identifiable, partially identifiable, or de-identified data with third party entities, b) prohibitions against re-identification of de- identified data without consent of the consumer, c) explicit documentation of agreements with third party entities that involves transfer or sale of consumer information, and e) the process by which the consumer will be contacted in the event of a violation of the Chain of Custody Agreement.

87 R.S.O. 1990, c. p.40.

88 S.O. 1994, c. 26.

89 As an example, the Ontario *Regulated Health Professions Act*, S.O. 1991, c.18 [RHPA] contains a *Health Professions Procedural Code* whose confidentiality requirements take precedence over PHIPA.

Act[90] and the *Medicine Act*.[91] Regulations made under the latter statute have a direct bearing on the ability of physicians to maintain PHI in electronic records. In particular, section 20 of the *Medicine Act*'s O. Reg.114/94 permits physicians to create and maintain patient medical records in an electronic computer system only if the system meets certain criteria. As an example, the system must collect audit trails, showing the date/time a patient's record was accessed, any changes made at the time of access, and the original data before the access. The system must "include a password or otherwise provide reasonable protection against unauthorized access." The regulations require that a system used by a physician "automatically backs up files and allows the recovery of backed-up files or otherwise provides reasonable protection against loss of, damage to, and inaccessibility of, information."

IV. ANALYSIS

This section addresses the obligations incumbent on private sector PHR vendors, from the perspective of a regulator wishing to address the three categories of issues mentioned above. While there are significant gaps, at least some of the relevant issues have been covered by legal requirements found in the various instruments mentioned above.

(a) Strengths

The various legal instruments outlined above have some positive effects on the issues involved in commercializing PHR systems. First, the current regulatory framework imposes constraints on the ability of vendors to use or disclose PHI. Subsections 5(3), 7(2), and 7(3) of PIPEDA (as well as several clauses in Schedule 1) place limits on the ability of a vendor to use or disclose personal information. In addition, one of the provisions in the "Individual Access" principle obligates vendors to provide an audit trail of all uses to which personal information has been put, and the third parties to which it has been disclosed.[92] If applicable in the circumstances, subsections 49(1) and 49(2) of PHIPA also impose constraints on the ability of vendors to use or disclose information that has been uploaded by health information custodians.[93] In the event that a vendor wishes to engage third parties to perform processing or archiving of personal information, the "Accountability" principle in PIPEDA's Schedule 1 dictates that the vendor must use "contractual or other means" to provide a comparable level of protection while the information is being processed.

Second, the various instruments contain guidance on security measures. For instance, the "Safeguards" principle in PIPEDA confers upon vendors an obligation

90 RHPA, *supra* note 89.

91 S.O. 1991, c. 30.

92 PIPEDA, *supra* note 41, Sch. 1 s. 4.9.1.

93 Similar to the case of disclosure to outside organizations, the leakage of personal information to third party applications is an eventuality that should be anticipated by PHR vendors. These vendors are therefore under an obligation (through PIPEDA and/or PHIPA) to prevent such leakage.

to protect personal information in a PHR from loss and theft, as well as unauthorized access, disclosure, copying, use, or modification.[94] The "Safeguards" principle provides space for organizations to vary the nature of the safeguards in response to the sensitivity of the information, and presumably the nature and likelihood of the salient risks.[95] If physicians are uploading information to the PHR, the Ontario *Medicine Act* also requires the use of safeguards, including audit trails and reasonable protection against unauthorized access, loss, damage, or inaccessibility of information.

Third, the integrity dimension of security is at least partially addressed in the instruments that were surveyed above. Unauthorized modification of personal information is covered by the "Safeguards" principle of PIPEDA.[96] While the PIPEDA principle of "Accuracy" appears to operate at a higher level of granularity than the traditional notion of data integrity, the *Medical Devices Regulations* could provide some guidance on reducing risks. Section 20 of the Regulations states that if "a medical device consists of or contains software, the software shall be designed to perform as intended by the manufacturer, and the performance of the software shall be validated." According to IEEE Standard 610, software validation is "the process of evaluating software during or at the end of the development process to determine whether it satisfies specified requirements." Applying this definition to the section 20 of the Regulations implies that the vendors need to keep an explicit specification of the intended performance for their software — a specification that should include functional requirements, as well as non-functional properties (e.g., data security, integrity, etc.). Furthermore, section 10 of the Regulations confers upon vendors a duty to identify the risks inherent in PHR software, and to either eliminate or reduce them.

Fourth, the various instruments force PHR vendors to put in place administrative mechanisms to support the protection of privacy. The "Accountability" principle forces a vendor to designate an individual who is accountable for the organization's compliance with PIPEDA; it also mandates that the vendor implement various policies and practices, including a) procedures to protect personal information; b) procedures to receive and respond to complaints and inquiries; c) staff training; and d) developing information to explain these and other policies and procedures. Furthermore, an Establishment Licence forces a vendor to provide evidence that documented procedures are in place in respect of distribution records, complaint handling, recalls, and mandatory problem reporting.

(b) Weaknesses

Although the various instruments cover some of the issues with PHR systems, it is clear that there are many outstanding issues worthy of further investigation by academics, industry groups, and regulators.[97] First, it is not clear that the safeguards mandated by PIPEDA are sufficient for addressing the main security risks

94 PIPEDA, *supra* note 41, Sch. 1 s. 4.7.1.

95 *Ibid.* Sch. 1 s. 4.7.2.

96 *Supra* note 92.

97 Due to space constraints, we will only discuss a few major issues in the remainder of this article.

of PHR systems. Much of the guidance in PIPEDA concerns basic security precautions, such as passwords and locked filing cabinets. It is not clear that the major security risks of PHR systems (particularly those using social networking architectures) are thoroughly addressed using these methods, as many of the issues involved are novel.[98] Schedule 1 of PIPEDA does state that personal information must be protected by security safeguards "appropriate to the sensitivity of the information," creating an obligation for organizations to customize their security procedures. However, it is not clear that this is coextensive with an obligation to address security issues that are unique or novel to the domain, as opposed to merely applying sufficient traditional safeguards. The main issue with respect to PIPEDA is that there are no settled "best practices" to determine what standards vendors would have to meet to safeguard data in social networks or PHR systems.[99]

While the *Medical Devices Regulations* is much more specific, the bulk of the obligations concern quality, with an emphasis on the nature of the manufacturing process. Although quality is undoubtedly an important topic for PHR products, a focus on quality does not address the privacy and security concerns outlined above. As an example, the Regulations use the concept of "safety," which does not prima facie subsume privacy and security issues. The most promising aspect of the medical device regime is the requirement to identify and eliminate "risks" in the software. As in the case of PIPEDA, it is not clear that best practices have been established in the social networking and PHR domain; nor is it clear whether the word "risk," in the context of the Regulations, covers all of the privacy and security concerns associated with these products.[100]

Second, there are many unanswered questions concerning the suitability of medical device law as a framework for regulating patient management software. To take but one example, interoperable PHR products will likely be categorized as Class II patient management systems, requiring product-focused licences. However, the current licensing regime does not require renewal of the licence when the

98 For instance, signalling and secondary disclosure issues in PHR systems are not completely addressed by standard security measures. In addition, some attacks on social networking systems are actually compatible with the presence of traditional safeguards; some only require an attacker to analyze the network using authorized methods, such as search functionality. For a technical example, see J. Staddon, "Finding 'hidden' connections on LinkedIn: an argument for more pragmatic social network privacy" (2009) Proceedings of the 2nd ACM Workshop on Security and Artificial intelligence AISec '09.

99 Of course, the Commissioner can investigate the use of safeguards in the course of making a decision, as occurred in PIPEDA Case Summary #2006-356. (Customer's banking personal information found in a recycling bin). In order to provide objectivity, recommendations for those security and privacy risks unique to PHR or social networking applications should be based on a body of best practices.

100 The issue of whether the term "risk" as used in the *Medical Device Regulations* would capture privacy and security vulnerabilities in patient management software is a topic beyond the scope of this paper. At an intuitive level, one might ask whether the term "risk", used a statute initially devised for medical devices such as pacemakers, would cover scenarios that involve administrative or usage-level vulnerabilities, as opposed to issues with the device itself.

software changes. This is a grave problem, since software problems may emerge in subsequent major releases and revisions of the products. A product-focused certification regime that does not take into account the evolutionary nature of software will not be effective.

Another problem is that the "software as a product" paradigm is currently shifting to a "software as a service" (SaaS) paradigm. Many PHRs are provided as services, rather than shipped products. The *Medical Devices Regulations* do not sufficiently address this notion of medical devices as a service. Another problem pertains to the unclear notion of what constitutes "custom developed" software. Health Canada explicitly excludes "custom developed" software from the licensure requirement. However, a sufficiently precise definition of this term is missing. It can be argued that virtually all patient management software developed today makes some use of pre-existing software components (e.g., libraries), while it can also be argued that most patient management software can customized in one form or another to a particular customer context.

Third, it seems that none of the instruments above contain provisions mandating that a vendor notify either users or regulators in the case of a *privacy breach*. While breach notification provisions are found in PHIPA, our analysis showed that this statute has limited application to private sector PHR vendors.[101]

Fourth, there is a fair bit of uncertainty concerning *retention periods* for personal information. The "Limiting Use, Disclosure and Retention" principle of PIPEDA urges organizations to develop guidelines and implement procedures with respect to the retention of personal information, including minimum and maximum periods.[102] It further recommends that personal information that is no longer required to "fulfill the identified purposes" should be destroyed, erased, or made anonymous.[103] Apart from this restriction, the choice of retention period seems (in the absence of other relevant legislation) to be at the discretion of the vendor.[104] Additional pieces of legislation like the Ontario *Medicine Act* may specify retention periods[105] for patient medical records in the custody and control of a physician, but these are of questionable applicability in the case of a private sector PHR vendor. This state of affairs does not provide PHR users with a high degree of control over the longevity of their data.

Fifth, a major issue exists with respect to subsection 9(1) of PIPEDA, which prohibits secondary disclosures of information. In particular, PIPEDA states that an organization "shall not give an individual access to personal information if doing so would likely reveal personal information about a third party."[106] Given the heredi-

---

101 Although breach notification may be included in a forthcoming revision to PIPEDA, the lack of such an obligation is a serious issue at present.

102 PIPEDA, *supra* note 41, Sch. 1 s. 4.5.2.

103 *Ibid.* Sch. 1 s. 4.5.3.

104 The Model Code states that personal information used to make a decision should be retained long enough to allow an individual to access the information after the decision has been made. Section 8(8) of PIPEDA is also relevant.

105 Specifically, Subsection 19(1) of O. Reg.114/94 under the *Medicine Act*, *supra* note 91.

106 If the information about the third party is severable from the record, the organization may sever the information.

tary nature of many diseases, subsection 9(1) may prohibit PHR vendors from offering their systems as a data source for health care practitioners, even if the patient has provided the health practitioner with access rights to the PHR.

Sixth, none of the instruments mentioned above deal with the issues of *trust* that were introduced above. The issue of duplicitous users posing as patients or physicians is likely better addressed through registration procedures and industry-sponsored certification regimes, rather than legislation. Bias by commercial interests remains a residual risk, and an effort to address the quality of information in a PHR with respect to provenance involves multi-jurisdictional and multi-party negotiations and agreements.

Seventh, the PHR landscape lacks standards for *interoperability*. As mentioned above, the high costs of switching PHR vendors may provide a disincentive for users to abandon a vendor whose services are lacking. In the absence of messaging middleware that allows exchange of data between disparate data models, it is likely that data interoperability will remain a key issue in the near future.

Eighth, many of the issues associated with *social networking* techniques are unaddressed by the various instruments outlined above. The complexity of interactions in these systems typically makes it difficult for users to assess risk, and to understand privacy policies. The ease of forming online networks can make it difficult to judge one's exposure. Furthermore, social networks are subject to attacks that are not possible in traditional applications, such as the inference of an individual's characteristics from facts about her friends.[107] These issues seem to lie outside the scope of traditional security safeguards, leaving them unaddressed apart from a small amount of work occurring in the research community.

V. CONCLUSION

This paper has served as a brief introduction to the status of private sector PHR vendors in the Canadian legal context. Eschewing the common law for reasons of brevity, the paper covered the impact of statutes, regulations, certification regimes, and industry standards on the nascent PHR landscape. While the current legal framework addresses some of the major issues with PHR systems, other risks and vulnerabilities remain unaddressed.

In particular, we have seen that major issues remain with respect to interoperability, trust, social networking, secondary disclosures, safeguards, and retention periods. The most significant issues from our perspective are (a) the lack of emphasis on interoperability; (b) issues with using medical device law to regulate software systems, and; (c) the residual risk concerning the scope of the security obligations contained in the various instruments. Lastly, the health care domain has unique features that are not well served by standard approaches to privacy, as we demonstrated in our brief discussion of genetic diseases and secondary disclosures.

Given the efforts of the federal commissioner to regulate the use of social networks, it appears that Canada is not entirely unprepared for the emergence of PHR

---

107 For an example of this sort of inference, see T. Bradley, "What You Don't Know about Your Online Reputation Can Hurt You" (28 May 2010), online: PC World <http://www.pcworld.com/businesscenter/article/197529/what_you_dont_know_about_your_online_reputation_can_hurt_you.html>.

systems. However, much work remains to be done in understanding the legal implications of these applications. It is our hope that this paper will serve as a useful introduction for policy makers, regulators, vendors, and academics. However well-equipped our regulatory system, it appears that the personal health record is here to stay.