Social Networks for Health Care: Addressing Regulatory Gaps with Privacy-by-Design

James B. Williams, Jens H. Weber-Jahnke, Senior Member, IEEE

Abstract—Social computing is a relatively new approach to systems design that emphasizes the importance of facilitating collaboration and communication between users. Although social networking is now part of mainstream culture, the use of these applications in the health care space is still in its infancy in Canada. As major vendors are preparing to enter the marketplace, it is important for a wide variety of stakeholders to discern the ramifications of this next wave of technological innovation. This paper discusses social networking applications for health care, and the challenges of dealing with this new type of information management system under current Canadian law. While regulatory authorities have considered the privacy and security implications of social networking in the course of investigating complaints, this paper contains the first explicit analysis of the legal difficulties surrounding the use of social networking for health care applications in Canada. Those risks not covered by the current regulatory framework are assessed from the standpoint of privacy-by-design, as we discuss how software developers can build privacy protection into social networking applications.

Index Terms—legal factors, privacy, data security, regulatory compliance, personal health information, social computing.

I. INTRODUCTION

The advent of social networking applications has provided Internet users with a new array of tools to facilitate collaboration and communication within virtual communities. However, the flexibility inherent in the design of these applications has given rise to significant concerns about privacy, security and data quality. Regulatory authorities in Canada have taken an increasing interest in social networking, as evidenced by the Privacy Commissioner’s recent report on Facebook [29].

The concerns surrounding the privacy and security implications of social networking applications become even more significant when considered in the context of health care. Given that personal health information (PHI) is one of the most sensitive types of personal information, the recent release of the first generation of social networking applications for health care (SNAHCs) is a matter of no small interest to regulators, health care providers and patients.

In this paper, we will situate social networking applications for health care within the context of Canada’s regulatory regime. After reviewing some of the major security and privacy concerns associated with these applications, we will discuss some of the key legislative instruments governing the collection, use and disclosure of personal information. As our contribution towards research in this domain, we will evaluate private sector social networking applications within the context of representative privacy and health information statutes. We will close the paper with a discussion of ‘privacy-by-design’, and how its major principles can aid vendors of social networking software in mitigating some of the risks that arise in the health care space.

Due to space constraints, we will defer any discussion of recent common law jurisprudence, including tort, product liability and contract law. 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 impending deployment of social networking software in the health care domain, there is a pressing need for future work in this area, both by the research community and by regulatory agencies.

II. SOCIAL COMPUTING

A. The Social Web

Social computing is a recent and increasingly popular approach to application design. Although not restricted to the Internet, most social computing platforms are web-enabled applications that focus on online social networking and collaboration. The term ‘Web 2.0’ was introduced to denote internet architectures that permit content to be easily generated and published by users. Although the original World Wide Web was intended to support collaboration through the use of email, hyperlinks and bulletin boards, the first generation of internet applications tended to contain static content. Information generally flowed in one direction – from the site author to the user.

In contrast to the largely unidirectional nature of first-generation websites, Web 2.0 applications are designed to encourage high degrees of participation. Users are typically encouraged to act as producers, through the use of facilities that allow them to create persistent content on the website. In contrast to first generation websites, Web 2.0 applications are not mere purveyors of static content; they are often rich in
user-generated content, and may feature revealing, visible histories of user activity. According to Abram, the new web architectures emphasize “conversations, interpersonal networking, personalization and individualism” [1].

B. Social Networking

There are many different types of Web 2.0 applications, including wikis and blogs. The most feature-laden Web 2.0 architectures, however, are to be found in the area of online social networking. This popular style of application allows users to network within a virtual community, through the use of various mechanisms that promote social interaction. Users of a social networking site like Facebook begin by creating a profile containing personal information. The user can then begin to construct a virtual social network, by adding other users as friends, colleagues, or family members. Sites may also include automatic recommender systems suggesting potential social links based on profile information (e.g., same employer, same school graduation year, same friends). As opposed to other types of web architecture, online social networking sites make the relationships between users explicit and visible.

III. SOCIAL NETWORKING IN HEALTH CARE

A. Health Information in Canada

The health care system in Canada is under an increasing amount of stress, faced by rising service costs and an aging population. As part of their response to these pressures, governments and health care providers have invested vast sums of money into electronic health (e-health) systems. Examples of these information technologies include electronic medical records (EMRs), decision support systems, telemedicine networks, and regional electronic health records (EHRs). The growing prevalence of electronic medical records has led the federal government to spur efforts to integrate systems into a pan-Canadian EHR.

Despite the growing uptake of electronic health information systems, patients have not necessarily benefited from the accessibility that these new systems were intended to provide. Although the Supreme Court of Canada (SCC) decided in McInenery v. MacDonald that patients had a right to access their health records, the court did not base that right on a notion of ownership. While legislation also provides for a right of access in many provinces, obtaining access to a health record, even where guaranteed by law, can be costly and time consuming.

B. Empowering Patients with Web Technologies

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

This situation began to change in the late 20th century. In addition to the advent of direct-to-consumer advertising, the appearance of the Internet allowed patients to access up-to-date health information resources directly [5]. The first generation of online websites devoted to health care consisted of health portals, which catalogued information. Even today, sites such as WebMD (www.webmd.com) provide information that has been at least partially researched by practitioners. As a result, patients in the Internet era have a wide array of online applications to help them in their search for information on medical conditions and treatments.

Although these advances greatly improved the availability of information, patients were no closer to being able to access the most important health information – namely, their own. Given that many experts in the field of health care have extolled the benefits arising from preventative medicine and patient empowerment, the inability for patients to access their own medical information does not bode well for the sustainability of the health care system.

A new generation of social networking applications promises to overcome this omission. Personal health record (PHR) systems from vendors such as Microsoft and Google allow individuals to keep a longitudinal and comprehensive record of their health data, which can be shared with family members, friends and health care providers at the owner’s discretion. Users of these services can keep track of their personal health information, including medication histories, immunizations, past procedures, allergies and insurance plans.

Despite these advances, social networking applications promise to do more than just provide access to personal health information. 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 [8]. Patients may also collaborate with one another, as evidenced by growing online communities devoted to particular health ailments [5]. Some researchers have suggested that participation in their own health care management can make patients more health conscious [10]. This observation is in keeping with applications such as HealthyCircles (www.healthycircles.com), which builds upon the basic technology of Microsoft HealthVault by adding provider registries, diet plans, telemedicine and interactive health-monitoring applications.

C. Enabling Providers

Social networking technologies also have potential benefits to health care providers. First, they may support professional development, by serving as a virtual space in which online communities of practitioners can share advice, expertise and the results of the latest research. Second, they may function as a mechanism for keeping up to date with current best practices—a service that is highly useful for practitioners in remote communities [13].

D. Basic Model of a Social Network in Health Care

A social networking application for health care (SNAHC) involves: a) a set of patients, who store personal information in their health profile; b) a set of providers, representing health
care professionals; c) a set of mechanisms for exchanging information, such as message boards, groups, email and profile posts; d) a set of relationship types which patients and providers can choose to participate in; d) a set of search functions by which users can locate information. e) a site operator who controls the site, and f) a set of third parties who may exchange data with the site.

E. Features of the Health Care Domain

The complex nature of health care delivery means that SNAHCs have some unique challenges [27]. First, the information involved is highly sensitive. Second, aggregated personal health information has high value to certain data recipients, such as pharmaceutical companies and marketers. Third, unlike financial information, there is no easy way to indemnify an individual with respect to the unauthorized use and disclosure of personal health information. Fourth, since health teams coalesce around episodes of care, the networks formed in health care settings are usually quite ephemeral. Fifth, the inquiries that a patient makes, or the friends that they keep, could be a signal as to what sort of ailment they suffer from. Sixth, there is a high possibility of secondary disclosure, as inferences can be drawn about a patient from the information that has been revealed by her family members.

F. Security and Privacy Issues

As summarized in [27], social networking applications exhibit a number of security and privacy issues. 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 [14]. 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. Third, trust is a major issue for social computing. To take but one example, duplicitous individuals may create fake accounts in order to obtain information from unsuspecting users. Fourth, the accumulated personal information may be used for other purposes. Site operators may release personal information to a variety of data recipients, including marketers, employers and insurance companies. Indeed, there is recent evidence of increased use of social networking sites by government agencies [16]. Fifth, users typically have no control over retention periods for personal information or associated metadata. Sixth, there is evidence that leakage of personal information to third party servers and applications occurs in many social networking applications [15]. Seventh, the 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. Even more ominously, cloud computing [11] approaches can result in data being scattered and duplicated across numerous jurisdictions. Lastly, the costs of switching from one social networking provider to another are exceedingly high, in comparison to e-commerce applications. A user who is thinking of switching platforms is faced with the daunting task of migrating their personal information, as well as recreating their social network in the new environment.

IV. THE REGULATORY LANDSCAPE IN CANADA

A. Governance of Health Care in Canada

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. As a result, both levels of government may pass legislation concerning health. 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, the Hazardous Products Act and the Food and Drugs Act [3].

Each province has passed a set of statutes aimed at regulating the behaviour of health care providers, which include hospitals, self-regulating professions, mental health facilities, ambulance services, long-term care facilities, and provincial insurance programs. Many of these organizations have also promulgated bylaws or codes of conduct that are binding upon their employees or members. In addition, various common law judgments have not only created non-statutory law, but have provided interpretations of key provisions and terms in the various instruments.

B. Privacy Law in Canada

The protection of privacy in Canada arises from a patchwork of statutes, regulations, bylaws, common law decisions, professional codes of conduct and voluntary industry standards. Despite this diversity, the protection of personal information in Canada is generally a result of statutory law. Since a full discussion of the various legislative and regulatory instruments is beyond the scope of this paper, we will largely concentrate on the legal situation in the province of Ontario.

The Canadian privacy 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, the Canadian Standards Association (CSA) promulgated the Model Code for the Protection of Personal Information in 1996. In the next section, we will examine representative statutes governing privacy in Canada, both of which are based on the principles in the CSA Model Code.
C. PIPEDA

The Personal Information Protection and Electronic Documents Act (“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 that lays out ten fair information principles.

In terms of applicability, Section 4 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 business. Although the issue is beyond the scope of this paper, PIPEDA generally applies to transmissions of personal information across borders.

D. PHIPA

As our representative example of a health information statute, we have chosen Ontario’s Personal Health Information Protection Act, 2004, (PHIPA) and its accompanying regulations. PHIPA is designed to protect patients by imposing constraints on the collection, use and disclosure of personal health information (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 healthcare industry. As a result, health providers in Ontario that are subject to PHIPA have received an explicit exemption from the applicability of PIPEDA, courtesy of an order (SOR/2005-399).

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. 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.

In terms of application, the weight of PHIPA generally falls on health care providers, referred to in the legislation as ‘health information custodians’, and their agents. However, PHIPA also contains regulations for ‘providers’, persons 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]”. 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”.

E. Medical Devices Regulation

The Government of Canada has promulgated regulations 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 must hold a Medical Device Establishment License. The requirements for licenses, 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 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. The term includes a contraceptive medical device, but does not include a drug.

The Medical Device Regulations (SOR/98-282) state that the term ‘medical device’ means a ‘device’, as above, but not one intended for use in relation to animals. Schedule 1 of the regulations provides rules for four types of medical devices: “invasive, non-invasive, active, and special cases”. The regulations also provide four risk levels, known as Classes I, II, III and IV; the risk level increases with integer value.

F. Standards and Industry Codes

Voluntary industry standards, codes and certifications exist in addition to mandatory regulations. Canada Health Infoway (Infoway), a federally funded not-for-profit organization tasked with promoting the adoption of eHealth technologies, has recently (2009) begun to offer a certification program for ‘client registries, consumer health application & platforms, Immunization registries, and provider registries’. Infoway’s certification focuses on privacy, security and interoperability. 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 U.S. industry standards, codes and legislations, including some of the aforementioned statutes, but also foreign acts, e.g., HIPAA.
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; 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” (paying) customers of their certification services. (This position remained unchanged even after offering to pay for the assessment package). Infoway gives paying companies a time window of 90 days to complete the certification process, starting from the day they receive the assessment criteria package. In contrast to other industrial certification programs in other countries (e.g., programs of the U.S. Certification Commission for Health Information Technology), no roster of Infoway-certified products has been published to date.

Additional standards and certifications have been developed at the regional level under provincial jurisdictions. 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).

V. SCOPE OF COMPLIANCE

In this section, we consider whether vendors of social networking software are caught by the various regulatory instruments outlined above. As a preliminary matter, it is important to be aware of the difference between a social networking application for health care (SNAHC), and a personal health record (PHR). The former is explicitly designed around a model of collaboration and communication, based on the formation of explicit ties between users. In contrast, a PHR is a health record that is controlled by a patient, and not by a health care provider [25]; in the words of one researcher, patients decide what is included, where it comes from and who can see it [22]. Ideally, PHRs should conform to interoperability standards that allow data to be drawn from multiple sources [12].

Several modern PHR offerings such as Google Health and Microsoft HealthVault allow consumers to give access permissions to arbitrary individuals, 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. While additional social networking features are undoubtedly going to become common features in the PHR space, there is nothing in the definition of a PHR that requires these features.

A. PHIPA

Subsection 7(1) of PHIPA declares that the statute applies to the collection of PHI by a health information custodian, as well as the use or disclosure of PHI by either i) a health information custodian, or ii) a person to whom a health information custodian disclosed the information. A private sector organization furnishing social networking or PHR services to residents of Ontario would not qualify as a ‘health information custodian’. This is unfortunate for regulators, as it is only this type of entity that is required, in Sections 10-12, to a) utilize compliant information practices, b) ensure that PHI is accurate, and c) provide reasonable safeguards.

The next step for a legislator wishing to bring a PHR or SNAHC vendor within the ambit of PHIPA is to characterize the vendor as a ‘provider’. Unfortunately, it is not clear that private sector PHR vendors are providing a service by which custodians may store PHI in electronic form. Instead, they appear to be providing a service for patients to manage their own health information. 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.

Even less promising is the claim that a PHR or SNAHC vendor is a ‘health information network provider’ under PHIPA, since the primary purpose of their product is not to transfer PHI between health care providers, but to facilitate management of a patient’s own health information.

Vendors of patient management software may qualify as a data recipient – a person to whom a health information custodian has disclosed PHI. Section 49 of PHIPA imposes two obligations on data recipients: 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.

The fact that PHR and SNAHC systems fall outside the ambit of Ontario’s health information legislation is not unique. Indeed, PHR and SNAHC 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. In the United States, such vendors are also outside the scope of the Health Information Protection and Accountability Act [18].

B. PIPEDA

Unlike PHIPA, PIPEDA does regulate the private sector. Since vendors or SNAHC and PHR systems are unlikely to be in the category of federal work, undertaking or business, the main issue concerns whether they qualify as an “organization that collects, uses or discloses personal information in the course of conducting commercial activities”. As mentioned above, the operator of a PHR or SNAHC may be a corporation like Google, or a non-profit entity. The definition of ‘organization’ in PIPEDA encompasses associations, sole proprietorships, partnerships, non-profit organizations and corporate entities. In addition, the information contained within PHR and SNAHC systems will
count as personal health information, under PIPEDA, unless the vendor uses some method for completely anonymizing the information stored.

As a result, the main issue turns on whether SNAHC and PHR vendors are using their systems to conduct ‘commercial activities’, defined in PIPEDA as “any particular transaction, act or conduct or any regular course of conduct that is of a commercial character”. In considering whether an organization is engaging in a commercial activity, the nature of the organization is not determinative. As examples, Google and Microsoft have different financial strategies underlying their offerings [23]. It is likely, given a purposive approach to statutory interpretation, that the Commissioner or the federal court would be amenable to expanding the reach of PIPEDA to fill in the gaps that arise from the failure of PHIPA to cover PHR and SNAHC applications.

PIPEDA generally applies to interprovincial and international flows of information. 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 v Accusearch the federal court held that PIPEDA can 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.

C. Medical Device Regulations

While there has been a degree of uncertainty in the manufacturing community about the role of software with respect this regulation, 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.

D. Industry Standards

Given that most of the emerging standards in Canada are for EHR systems, the question of whether a PHR or SNAHC is a type of EHR is central to an analysis of whether industry standards apply to PHR and SNAHC systems. The Canadian Medical Association (“CMA”) defines 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.” (CMA) Other commentators have suggested that EHR systems are typically: 1) complete, integrating information from all health providers that treat the individual; 2) life-long, storing information over the course of an individual’s life; 3) accessible, available to a variety of professionals in various geographical areas, and; 4) secure, protected against unauthorized access [24].

From an empirical standpoint, many EHR initiatives may fail to meet all of these conditions, so they are not necessarily determinative. Even if PHR and social computing applications were to meet the criteria, there are clearly significant differences. First, EHR systems (and EMR systems in clinics or hospitals) typically store a variety of work products, serving a variety of functions. Health information in these systems may be used for clinical work, teaching, research, and process improvement. The information may be viewed (perhaps in aggregate form) in the context of audits, accreditation, and qualification reviews [20]. The patient’s medical records are certainly treated in a different manner than the contents of a PHR or social networking application, since the patient does not give explicit permission for many of these other functions.

Second, EHRs may also contain practitioner’s notes and work products, the ownership of which clearly belongs to the EHR owner, and the release of which may be contested. Third, health data in an EHR is supplied by professionals, whereas health data in a PHR or SNAHC can come from non-professional sources. As a result, data quality determination is much more difficult [25].

We conclude that, at the current time, PHRs and EHRs are sufficiently distinct concepts, offering different functionality, centered 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 and increasingly important objective in order to avoid duplicate data entry. 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. Details are currently unavailable to the public, as indicated earlier.

E. 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. 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 and SNAHC systems.

In addition, health care professionals are typically subject to both specialized statutes and professional codes of conduct. These instruments may impose duties on health care professionals, including obligations to respect confidentiality. For example, the Ontario Medicine Act contains provisions relating to patient medical records. The impact of these codes of conduct on participation in SNAHC systems has yet to be addressed in a systematic way.

VI. SUMMARY OF OBLIGATIONS

In this section, we will provide more detail on the obligations arising from the sources of law considered above.

A. Privacy Laws

Although PIPEDA will likely catch many PHR and
SNAHC vendors, there are some challenges in applying it to this type of service. PIPEDA was not designed to cover patient-managed repositories in which individuals manage their own information, selectively and voluntarily disclosing it to others. The principles of Consent, Limiting Collection, Identifying Purposes, Access and Accuracy would seem to be of limited use in such circumstances. In addition, the principles of Openness, Accountability and Challenging Compliance do not impose significant burdens on vendors, as administrative solutions are easy to implement. Lastly, in contrast to PHIPA, PIPEDA lacks breach notification requirements, so vendors are not under a general duty to warn users of privacy breaches.

Despite the difficulties mentioned above, the principles entitled Safeguards and Limiting Use/Disclosure/Retention appear to impose more substantial obligations on PHR and SNAHC vendors. First, the principle of Safeguards provides both obligations (‘shall’) and recommendations (‘should’) on vendors. PIPEDA holds that personal information shall be protected by “security safeguards appropriate to the sensitivity of the information”. These safeguards shall 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. PIPEDA dictates that employees of an organization shall receive training concerning confidentiality, and that care shall be used in the disposal or destruction of data.

PIPEDA also contains provisions that could limit secondary uses of data stored in a PHR. 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 required 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 reinforces constraints on secondary uses by forcing organizations to seek consent from the patient in advance of using collected information for new purposes. Although one could argue that information in a PHR has not been ‘collected’, a purposive interpretation of the term 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 “an organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances.” Reinforcing this point is the ‘Consent’ principle, which states that “[t]he knowledge and consent of the individual are required for the collection, use or disclosure of personal information, except where inappropriate.”

The most unique provision in PIPEDA from the perspective of health care 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. Given the genetic/hereditary nature of many diseases, information about an individual’s health can occasionally reveal information about the health of their relatives.

B. Medical Device Regulations

Under the regulatory regime for medical devices, organizations that import, sell or distribute Class I or Class II patient management software must hold an establishment license. In order to obtain such a license, 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 license, a medical device license must be obtained for each patient management software product released into the marketplace. These licenses require a manufacturer to obtain a certificate showing that its quality management system is compliant with the ISO 13485:2003 standard. In the license 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 labeling 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 risks inherent in the device, and to either eliminate or reduce them.

C. Gaps

Unfortunately, the obligations accruing under PIPEDA and the Medical Device Regulations only catch a small number of the privacy and security issues we mentioned above. PIPEDA
does contain provisions constraining secondary uses and disclosure of PHI. While the provisions concerning safeguards impose duties on vendors, the general tone of the legislation suggests that the safeguards concern basic security practices, and not the sorts of unique concerns that affect PHR and SNAHC systems. The main concern with the impact of PIPEDA is that there are no settled ‘best practices’ to determine what standards vendors would have to meet to safeguard PHR and SNAHC systems. Additionally, the lack of breach reporting and the prohibition in Subsection 9(1) may cause problems for both regulators and vendors.

While the Medical Device Regulations are 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 and SNAHC 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 regulations 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 domain; nor is it clear whether the word ‘risk’, in the context of the regulation, captures all of our privacy and security concerns.

Given that the existing regulatory framework imposes a duty on vendors to provide safeguards, and to eliminate risks, it is worth asking whether regulators would be best served by encouraging vendors to shift from a compliance mindset to a preventative approach. In the last section, we show that there are several design choices which promise to yield a reduced risk profile in PHR and SNAHC systems.

VII. PRIVACY BY DESIGN

Privacy by Design (PbD) is based on the idea that privacy cannot be effectively guaranteed in modern information and communication technologies (ICTs) if it is treated as an afterthought. While Privacy Enhancing Technologies (PETs) have their role to play in increasing the protection of personal information, organizations must adopt certain privacy principles guiding their development, implementation, operation and evolution of any ICT.

A. Proactive not Reactive; Preventative not Remedial

The traditional approach in the ICT industry has been to remedy privacy issues after they have manifested themselves. Given the sensitivity of PHI, privacy breaches may not be easy to remedy. Moreover, regulatory challenges can have a lasting impact on a company’s public image. Although taking a proactive stance may entail a greater short term cost, the downstream benefits can be significant.

For example, PHR and SNAHC vendors can try to prevent privacy and security risks arising from the use of their systems by duplicitous users. First, automated queries can be run to detect fake user accounts, based on the structure of a user’s local network. For instance, an account managed by a marketing company might have a very different local network structure than an account managed by a bona fide user, whose profile would likely be linked to the profiles of users who were themselves well connected. By identifying vertices or cliques of vertices with low connectivity, vendors could generate lists of suspected duplicitous users for further scrutiny.

Second, business processes can be developed to verify if users claiming to be health care providers are actually credentialed. An example of such a process consists of checking a physician’s information against a provincial registry maintained by the College of Physicians and Surgeons. Third, search functionality can be restricted to prevent users from extracting ‘hidden’ data about the network [21]. This would make it more difficult for third parties in possession of a user account to bypass the privacy and security controls provided by the site.

B. Privacy as the Default

Many ICT services provide users with mechanisms to keep their data private. The essence of the “privacy by default” principle is that these mechanisms should be switched on by default, without requiring user action. While service providers may allow users to opt out of new features, the “privacy by default” principle seeks to ensure that the privacy of users is not weakened if they remain inactive, i.e., it mandates an ‘opt in’ approach.

Violations against the “privacy by default” principle have created significant media attention in social networks in the past. The Facebook Beacon affair is an example that has caused a large public outcry and a class action law suit, resulting in Facebook having to spend $9.5M on a settlement. In this case, the popular social networking site Facebook introduced a service that would track their users’ activities on other Web sites and send reports to third parties. On its introduction, this functionality was initially switched on by default [26].

While the avoidance of cases like the above is straightforward, the —privacy by default— principle has more subtle implications on social networks for health care. In contrast to general social networks that are used to “stay in touch”, health care is inherently episodic. Network connections may be determined in the context of transient health conditions, behaviours, geospatial locations and other factors at the time of a particular episode or sequence of episodes. Few users may take action to purposefully sever these connections after they have become obsolete.

As a result of these difficulties, SNAHC systems should be aware of the transient nature of circles of care and provide safeguards to protect the user’s privacy by default. One possible approach would be to automatically abstract and generalize health information accessible to “inactive” long-term connections after some time. Another would be to introduce a temporal decay into a user’s network, so that connections between a user and a health care provider would degrade over time, effectively hiding the user profile from the provider.
C. Privacy Embedded into Design

This principle requires application developers to consider privacy as an integral part of their design rather than something that can be “bolted on” retroactively. Experience has shown that privacy mechanisms that reside at an interface-level only are prone to be circumvented. Moreover, it may be impossible to implement certain privacy preserving behaviour as an “add-on” without the necessary support in the core system design. For example the above-mentioned feature of transient connections in SNAHCs may be difficult to bolt-on to an existing general purpose social networking platform.

Fortunately, as summarized in [27], various research groups have provided mechanisms by which privacy may be embedded into the design of social networking applications. First, vendors can adopt architectures that allow for anonymity, including anonymous opinion exchange. Of particular interest are architectures in which the user is anonymous from the perspective of not just other users, but the platform itself [17]. These methods would guard against the signaling, leakage to third parties, and data mining problems, as well as eavesdropping by duplicitous users.

Second, vendors should provide interfaces for third party applications that respect the privacy of users, while still allowing for customized content to be delivered. The use of such interfaces may be a best practice in the future; current approaches include “privacy by proxy” mechanisms [9].

D. Full Functionality – Positive-Sum, not Zero-Sum

Although privacy is often portrayed as being in conflict with other business objectives, devoting effort to privacy protection can be win-win proposition. For example, information privacy is often seen as being in tension with patient safety; some practitioners believe that health care providers should always be able to gain access to patient records, even without express consent. Based on such a position, most Canadian provinces do not require patient consent for centrally collecting their health data for the purpose of provider access. Despite the frequency with which the claim is asserted, it is not clear that privacy mechanisms are in conflict with patient safety – in fact, the opposite may be true. Formal studies have shown the value of unbiased second opinions for patient safety [19]. Once shared EHRs have become widely available, such unbiased consultations will not be possible without proper privacy mechanisms. This example indicates that augmenting PHRs and SNAHCs with privacy features could serve to benefit the health care system in other respects.

E. End-to-End Lifecycle Protection

This principle advocates privacy protection from the moment of data collection until the time the data is safely destroyed. The data collected in SNAHCs comprises not only patient health records but also the network connections themselves, data disclosed to third party (3P) applications and other data recipients (cf. Fig.1). Social networks have not commonly been offering end-to-end lifecycle protection to users. As Aspan reported, Facebook made it almost impossible for users to delete their data [2]. Apart from the issue that social network providers have an interest in keeping data for secondary purposes, the technical problem of completing eliminating all traces of a user in a social network is not trivial. Evidence about a user may be meshed up in other user data, e.g., comments on their data or blogs. The lack of end-to-end lifecycle privacy protection in current social networks has given rise to much frustration and created third party services with the whole purpose of advising users on how to delete their data from such sites, e.g., deleteyouraccount.com. An even more difficult problem is the deletion of data from 3P applications, which are not under the control of the SNAHC provider. Nevertheless, there are opportunities to improve current practice.

First, there is a growing literature on anonymization techniques for the type of data stored in a SNAHC [28]. Vendors of these systems can choose from a variety of approaches for anonymizing network data, if bulk extracts are requested by governments, researchers or advertising agencies.

Second, vendors should protect user privacy by constraining 3Ps who may have access to the information in their PHR or SNAHC system. Access control mechanisms can be created for applications, allowing users to have fine grained control over what an application can access. In addition, privacy policies of SNAHCs typically do not extend to 3P applications (cf. Fig. 1), which are normally governed by their own policies that users must accept separately. While it is rare enough that users critically review privacy policies of Internet services, the practice of disparate policies for each 3P application and the SNAHC creates a patchwork of policies that can quickly become incomprehensible to users. Therefore, SNAHC providers adhering to PbD principles should ensure that 3P application providers connecting to their systems should a) sign a contract that binds the 3P to obey strict information management practices, and b) adhere to PbD as well.

F. Visibility and Transparency

The objective of this principle is to provide a means of independently verifying that an organization operates according to set of understandable and comprehensive privacy policies. Visibility has not been a strong point of social networks. Data mash-ups and the combination of multiple networking services create unexpected information flow through ‘back channels’, impeding a user’s ability to get a clear view of the way their data is propagating. There have been allegations and supporting evidence that some social networking sites are not following the policies that claim to adhere to [4]. Recognizing the sensitivity of health information, SNAHCs should provide their users with clear ways to verify adherence to privacy policies. Given the complexity of interactions on social networking sites, vendors may be forced to find alternatives ways of representing privacy policies, including diagrams and interactive user guides.

G. Respect for User Privacy

Privacy-enabling solutions respect a user’s interest in
controlling access to. Sadly, dismissing privacy concerns as being important only for users “who do things that they shouldn't be doing in the first place” are unfortunately still common in the ICT corporate world [7]. Thankfully, there are several ways in which vendors can empower users. First, platforms can provide mechanisms that afford users fine-grained control over their data. In addition to covering profile data, these mechanisms will allow users to set privacy policies for shared content, applications, groups, searches and other social networking features. In order to ease the burden on users, vendors must provide intuitive user interfaces for controlling privacy settings.

As a second example, vendors could provide a means by which users can visualize their current exposure on the network. As mentioned above, users often underestimate the scope of their online social networks. Graphical displays of these networks would help a user to appreciate the potential risks arising from a disclosure.

VIII. CONCLUSION

This paper has discussed the regulatory environment for PHR and SNAHC systems in Canada. We have seen that these software applications are treated lightly by health information statutes. The applicability of general purpose privacy statutes is also somewhat limited. While the medical device regulations will apply to these products, it focuses largely on quality.

Those legal provisions that do stick to PHR and SNAHC systems obligate vendors to implement safeguards, and to identify and eliminate risks. Without a standard, a body of best practices, or a set of judicial or administrative decisions, vendors have little guidance on what efforts are required under either of these obligations.

Instead of viewing the situation from a compliance perspective, vendors may wish to adopt a Privacy by Design approach. There are several obvious ways in which PHR and SNAHC systems can be engineered with privacy in mind, as evidenced by products in industry, as well as research projects in academia. The discussion in this paper of these issues is, of course, preliminary. It is our hope that our brief analysis of the challenges of regulating SNAHC and PHR systems will spur researchers, industry groups and vendors to undertake future efforts in this field.

REFERENCES

[29] E. Denham, PIPEDA Case Summary #2009-008: Report of findings into the complaint filed by the Canadian Internet Policy and Public Interest Clinic (CIPPC) against Facebook Inc under [PIPEDA], Privacy Commissioner of Canada, 2009.