1 Introduction
Faced with rising service costs and aging populations, governments and health care organizations in North America and Europe have little choice but to improve the efficiency and efficacy of medical care delivery. While culprits abound, research has shown that many inefficiencies and quality problems arise from a lack of access to relevant information. Common examples include unnecessary duplication of laboratory work, cancellation of scheduled treatments on account of missing data, and prescription of unnecessary (or even harmful) drugs. As a result of these concerns, governments and health organizations are investing in the development and acquisition of information and communications technology (ICT), including decision support systems, electronic medical record (EMR) software, and telemedicine. While these initiatives promise benefits for health care delivery, the use of software systems in the health care domain raises new concerns about safety, effectiveness, privacy, and security. Of these issues, safety and effectiveness are perhaps the most important. Research studies have estimated that medical errors result in up to 98,000 deaths each year in the United States, with costs approximated to $30 billion.\(^1\) Unfortunately, experience has shown that software systems have the potential to generate life-threatening errors.\(^2\)


\(^2\) According to research by the Huffington Post Investigative Fund, The US Food and Drug Administration (FDA) Manufacturer and User Facility Device Experience (MAUDE) database contains 237 reports on such incidents between...
In a recent notice, Health Canada clarified that patient management software (PMS) is subject to Canada’s medical device regime; it further warned vendors that enforcement is pending. In this paper, we will consider the regulatory framework for PMS in Canada, including medical device, privacy, and health information law. Our claim is that submitting software systems to a medical device regime could be an ineffective and cumbersome means of fulfilling policy objectives. Although we use Canada as the jurisdiction for our analysis, other countries are poised to follow Canada’s lead in submitting PMS to medical device regulation.

The first part of this paper discusses ICT for health care in order to provide background for readers who are unfamiliar with this area. After this introductory section, we discuss the basic features of medical device regimes at an abstract level, remaining neutral on jurisdiction. We then cover the basics of the Canadian regulatory landscape for PMS, including medical device regulation, privacy law, and industry-promulgated certifications and standards. We end the paper with an analysis of the strengths and weaknesses of the current framework, followed by suggestions on how to correct some of the deficiencies.

2 Patient Management Software

2.1 Application Variants
There are many types of ICT for use in a health care setting, ranging from simple applications for scheduling appointments to the complex software that provides control and diagnostics for images generated by magnetic resonance imaging scanners. Standards organizations have developed detailed specifications about the functional requirements on particular types of PMS.³

---

In the interests of providing an overview of ICT in health care, the following subsections introduce four general types of PMS.

2.1.1 Scheduling and Billing Software
The most basic PMS applications provide a core set of administrative functions for operating a health care delivery location, namely: (a) tracking patient contact information; (b) scheduling appointments; (c) printing billing information, and; (d) tracking employee hours. These applications are usually deployed on a standard desktop computer. Depending on the jurisdiction in question, users may be able to send billing information directly to insurers or governmental agencies. Scheduling and billing applications are not intended to store personal health information (PHI) for clinical use. Consequently, patient safety is a lesser concern in these types of systems, while most issues relate to information security and privacy.

2.1.2 Electronic Medical Records
An EMR is intended to extend the functionality of scheduling software by giving health care providers the ability to manage and process medical information for use in clinical care. Medical clinics and other health care organizations can use EMRs to store a wide variety of PHI, including prescriptions, health history, allergies, lab results, and care plans. The ability to manage patient records in electronic form offers advantages over paper-based systems, although researchers have also noted disadvantages and risks.4 Advantages of EMR systems include the ability to offer automated alerts, reminders, diagnostic aids, and case-specific best practice guidelines. EMR systems can also facilitate the collection of (anonymized) health information for public health surveillance and evidence-based medical research. On the negative side, researchers found that EMRs may introduce new types of medical errors


that put patient safety at risk\textsuperscript{5}, counteract effective communication\textsuperscript{6}, and pose severe privacy risks\textsuperscript{7}. Sittig and Singh have recently addressed safety and EMRs, basing their analysis on Carayon \textit{et al.}'s "Systems Engineering Initiative for Patient Safety".\textsuperscript{8} The authors recommend that governments should “create a regulatory environment compatible with widespread use and interoperability [of EMR systems], thereby enabling systems to continue evolving while maintaining appropriate safety and privacy oversight.”\textsuperscript{9}

Although EMR systems typically support the exchange of information for billing purposes, they are not designed to exchange information with other EMR systems. The reason for this lack of electronic interoperability is the absence of a commonly accepted standard for representing health information. Consequently, EMRs often become information ‘silos’ that store only the information that is known about patients at a particular health care organization. This fragmentation of information is problematic, since patients often receive care at multiple locations.

\textbf{2.1.3 Electronic Health Records Systems}

An electronic health record (EHR) system (also called a \textit{shared health record} or \textit{summary care record}) is a ‘multi-tenant’ EMR that focuses on providing \textit{shared} access to many health care providers in a jurisdiction. The Canadian Medical Association defines an EHR as:

\begin{quote}
…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
\end{quote}

\begin{thebibliography}{9}
\bibitem{Ibid} \textit{Ibid.} at 1112.
\end{thebibliography}
record and can request changes to its content. The transmission and storage of the content is under strict security.\textsuperscript{10}

EHR systems are typically: (1) \textit{complete}, integrating information from all health providers that treat the individual; (2) \textit{life-long}, storing information over the course of an individual’s life; (3) \textit{accessible}, available to a variety of professionals in various geographical areas, and; (4) \textit{secure}, protected against unauthorized access.\textsuperscript{11} Only the fourth element in this set is shared with EMR systems, which are not intended to be comprehensive, longitudinal, or accessed by more than one organization.

\subsection*{2.1.4 Personal Health Records Systems}

A personal health record (PHR) is a health record that is controlled by a health care consumer, rather than by a provider.\textsuperscript{12} In contrast to EMRs and EHRs, patients decide what data is included and who can see it.\textsuperscript{13} Although some PHRs have been created for home computers and mobile devices, the most prevalent PHRs are Internet-based systems such as HealthVault and Google Health.\textsuperscript{14} PHR software of this sort is provided as a hosted service, instead of an application that manages health information locally at the user’s computer.

\begin{thebibliography}{9}
\bibitem{10} Canadian Medical Association, \textit{Advancing Electronic Health Records in Canada: CMA Working Principles and Recommendations} (Ottawa: Canadian Medical Association, 2002).
\end{thebibliography}
2.2 Issues with Patient Management Software

Researchers have raised multiple issues with respect to software-based medical devices and PMS, particularly in the areas of safety, privacy, and efficacy. Adverse events relating to software systems can arise from a number of sources, including: (a) human-computer interface difficulties; (b) system inflexibilities that prevent the integration of the system with existing workflows; (c) weak privacy and security safeguards; (d) failure to integrate information from all relevant information systems; (e) lack of interoperability mechanisms, and; (f) improper customization or configuration of features. In this section, we provide more detail on a few of the major issues that arise when software products are put to use in a health care environment.

2.2.1 Management of Information

PMS initiatives have been criticized on the grounds that they present major risks with respect to privacy, safety, and effectiveness. Experts have argued that EHRs have the potential to do more harm than good. Insufficiently controlled EHRs may become a serious safety and privacy hazard, since they constitute “multicontributor records for which no individual clinician is responsible.” Even for EHR designs that allow patients to opt-out of sharing their data, the consent management practices of existing systems have been criticized as ineffective and unworkable.

2.2.2 Human Computer Interaction

Some of the largest risks pertaining to PMS arise not from logical programming mistakes, but from the way the PMS is used. The classic example of misuse is the Therac-25 radiation therapy machine, whose software caused patients to receive massive radiation overdoses. Although the Therac-25 machine is not a PMS, it is a well-studied case study in software engineering, and can be used to introduce several issues that are directly applicable to PMS today. A more detailed analysis of Therac-25 has been published in N.G. Leveson & C.S. Turner, “An Investigation of the Therac-25 Accidents” (1993) 26:7 Computer 18.

---

16 To take but one criticism, even if patients are aware of their ability to opt-out, they may be unable to do so on account of their physical or mental condition.
17 Although the Therac-25 machine is not a PMS, it is a well-studied case study in software engineering, and can be used to introduce several issues that are directly applicable to PMS today. A more detailed analysis of Therac-25 has been published in N.G. Leveson & C.S. Turner, “An Investigation of the Therac-25 Accidents” (1993) 26:7 Computer 18.
effort. This contributed to several accidents in which the wrong data were used.\textsuperscript{18} Other accidents with the Therac-25 happened when human operators became faster and more proficient with entering data; unfortunately, the software was not tested with data entered at this speed. This hazard resulted in several deaths until it was identified. Similar hazards due to ‘race conditions’ have been found in modern software, particularly browser-based applications.

Other common hazards related with human data entry in PMS include juxtaposition hazards (e.g., erroneous clicks on the wrong element in a potentially long ‘drop down’ list of choices)\textsuperscript{19}, interruption hazards (i.e., hazards caused by interrupting the clinician’s workflow)\textsuperscript{20}, and hazards due to software desensitizing users with respect to alerts and exceptions (‘alert fatigue’). An empirical study of computerized physician order entry systems showed that physicians override drug safety alerts in 49-96\% of the cases\textsuperscript{21}, routinely ignoring potentially important advices on adverse drug interactions, overdoses, allergies, etc.

\textbf{2.2.3 Inadequate Development Processes}

While PMS products are typically not directly embedded in hardware devices for patient treatment, they share some of the same risks with embedded software devices, and many of the lessons learned from Therac-25 and related incidents are directly applicable to PMS. Investigations of the Therac-25

\textsuperscript{18} Studies of the cognitive tasks of clinicians using PMS have shown analogous hazards. The following quote from a clinician illustrate this analogy: “I use templates when I have no time to type in data, but I don’t like it. Pressing Enter, Enter, Enter is a prescription for errors”, Shachak \textit{et al.}, supra note 5 at 344.

\textsuperscript{19} There is evidence that juxtaposition errors have caused life-threatening injuries in patients. A voluntary report filed in 2008 to the FDA describes an incident in which a patient received four times the excess dosage of a medication due to a poorly designed user interface component. FDA, “MAUDE Adverse Event Report”, Report Number MW5014180, online: FDA <http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfmaude/detail.cfm?mdrofi__id=1570801>.

\textsuperscript{20} Example: A patient calls to check something, so the clinician opens his chart. When the clinician returns to the visiting patient she forgets to close the caller’s chart and continues writing about the visiting patient in the caller’s chart.

accidents determined that many of them could have been prevented if the device manufacturer had applied a more systematic, quality-oriented software development process. Current manufacturing processes for PMS are similarly immature.  

One possible explanation for the lack of best-practice engineering processes is the fact that software vendors have been able to: (a) disclaim liability for defects, and; (b) include ‘gag orders’ in license contracts, preventing users from disclosing software-related accidents.

2.2.4 Lack of Scrutiny

A related aspect is that software source code is often not made accessible to external scrutiny. The Therac-25 software code was never disclosed, even when the Food and Drug Agency specifically asked for it during an investigation of the accidents. While this situation has changed today, as regulatory bodies can request source code as part of the approval process, regulators are often overburdened with the task of evaluating potentially millions of lines of program code, particularly given time limitations due to market and economic pressures. The open source software model has been proposed as a solution and experts have argued that the source code for PMS should be required to be open to public scrutiny (e.g., by academics), or at least be available by request (e.g., through freedom of information legislation).

Still, the source code of most current PMS is not disclosed.


2.2.5 Interoperability and “Systems of Systems”

Another set of issues with PMS arises from the growing trend of integrating software systems into large-scale “systems of systems”.\(^ {25} \) The resulting infrastructure is heterogeneous, combining disparate products, technology platforms, and policy frameworks. There is a lack of centralized control of the emerging system; instead, components evolve asynchronously and out of step. Interoperability hazards have become an increasing risk in PMS. For example, in 2008 a patient received an operation on the wrong side of her head after CT sinus pictures were sent from a PMS to another system that inadvertently flipped their orientation. Investigations determined that both systems worked correctly on their own; the problem arose at their interoperability point.\(^ {26} \)

2.2.6 Dependability and Fallback Hazards

The introduction of PMS changes the way that health care organizations manage data. There are two types of risks associated with this change. First, there are risks associated with switching over from a ‘legacy’ information management system. Second, there are ongoing risks of system failure during day-to-day operation. Both types of risk have caused serious injury, hospital-wide breakdown, and even result in deaths where a fallback system was not provisioned.\(^ {27} \)

---

25 For example, the emerging pan-Canadian EHR is designed to integrate multiple legacy systems: <https://www.infoway-inforoute.ca/working-with-ehr/knowledgeway/knowledge-center/657>. For an overview of composing systems, see <http://www.infoed.com/Open/PAPERS/systems.htm>.


2.3 Conclusion
While we only summarized the most prominent current features and issues associated with PMS, it is clear that software will play a rapidly increasing role in modern health care systems. Many observers believe that regulatory oversight is required to balance benefits and risks of this development in order to protect the public and quality of care. In the next section, we examine the current regulatory framework in Canada. Given Health Canada’s recent announcement that PMS is covered under the Medical Devices Regulations of the Food and Drugs Act, we focus much of our attention on the regulation of software as a medical device.

3 Regulating Patient Management Systems in Canada
Responsibility for the provision of health care in Canada is shared between the federal and provincial governments, as health care is not explicitly listed in sections 91 and 92 of the Constitution Act, 1867.28 As a practical matter, provincial governments generally wield authority over health care facilities, including hospital and laboratories, as well as professional bodies, ambulance services, and health insurance programs. The federal government provides funding to the provinces through the use of transfer payments. In addition, several federal statutes hold sway over various public health concerns, including include the Quarantine Act, the Hazardous Products Act, and the Food and Drugs Act.29

---

28 Constitution Act, 1867 (U.K.), 30 & 31 Vict. c. 3. 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 or scope of the health problem in question”, Schneider v. R. [1982] 2 S.C.R. 112 at 142, 6 W.W.R. 673. For a thorough discussion of the responsibility for health care, see Martha Jackman, “Constitutional Jurisdiction over Health in Canada” (2000) 8 Health L.J. 96.

In the following sections, we will briefly outline the major Canadian sources of law pertaining to PMS. Although multiple sources of law exist, we have opted to concentrate on a select set of instruments: medical device regulations, privacy and health information statutes, and industry-promulgated standards.\(^30\) Our emphasis is on medical device regulation, since its application to PMS has been considered only relatively recently and with some controversy.

3.1 Medical Device Regulation – An overview

The term ‘medical device’ covers a wide range of products, ranging from tongue depressors to electronic pacemakers. Although early medical devices were generally unpowered, modern medical device products often contain sophisticated electronics, including computer processors. Drug pumps, implantable defibrillators, and glucose monitors are but a few examples of medical devices that are now designed with either onboard computing power or downloadable memories.\(^31\)

Although medical devices have historically been monolithic units that are developed, validated, and approved as stand-alone entities, an increasing number of devices have networking interfaces that allow them to interconnect. This capability allows a medical device to serve as a \textit{producer} of data that can be used for care planning and a variety of other clinical and administrative functions.

Some medical devices can also act as \textit{consumers} of data generated by other medical devices. For example, a patient-controlled analgesic pump can use data from pulse and respiratory monitors to prevent an overdose. Medical devices that are able to autonomously (without the intervention of a human caregiver) monitor patients (consume data) as well as decide on interventions (produce treatment data) are called ‘closed-loop’ devices. Traditionally, regulators have hesitated to approve closed-loop devices because of the complexities of validating the safety of such autonomous systems. However, this notion has increasingly been challenged by researchers who point out

\(^{30}\) Due to space constraints, we concentrate on statutory law, neglecting the issue of liability for software-based medical devices under tort or contract law.

the safety benefits of closed-loop systems. With the increasing sophistication and intelligence embedded in PMS, it is likely that more closed-loop architectures will emerge that incorporate PMS as the central hub (middleware) for coordinating other medical devices (monitors and actuators).

As one might expect, the growing complexity and criticality of medical devices has raised concerns about their safety and effectiveness. Devices are considered effective when they meet their functional requirements—that is, when they produce the effect intended by the manufacturer. They are considered safe if their benefits outweigh their risks. To this end, medical devices are typically treated within the context of a risk management framework. Risk management processes begin by: (a) identifying the hazards surrounding a device; (b) estimating and prioritizing the risks, and; (c) developing strategies to mitigate, transfer, or eliminate the risks. Organizations are making an effort to formalize this process in the medical device context.

Unfortunately, risk can rarely be eliminated entirely. Instead, it must be mitigated and balanced with other factors, such as economic considerations. Not only are some hazards difficult to avoid, but medical devices have a lifespan; instead of being static, the properties of the device may change over time. Parts may wear, batteries may lose their charge, and software quality may deteriorate over time. Failing to take into account the lifecycle and lifespan of the device may put patients at risk.

32 A simple example would be an x-ray/ventilator coordination system, in which the x-ray device would coordinate with the ventilator to pause ventilation for a few seconds to get a still image. This coordination, which is usually done manually by a clinician, has resulted in accidents and deaths due to the operator becoming distracted and forgetting to switch ventilation back on. See Ann S. Lofsky, “Turn Your Alarms On” (2004) 19 Anesthesia Patient Safety Foundation Newsletter 43. See also Andrew King et al., “Prototyping Closed Loop Physiologic Control with the Medical Device Coordination Framework” (2010) in Lori A. Clarke & Jens H. Weber-Jahnke, chairs, SEHC ’10: Proceedings of the 2010 ICSE Workshop on Software Engineering in Health Care (New York: ACM, 2010) 1.


34 Lehman’s well-established laws of software include: (1) the law of continuing change: systems must be continually adapted or they become progressively less satisfactory; (2) the law of increasing complexity: as a system evolves its
3.1.1 Key Concepts – Lifecycles and Modes of Use

The World Health Organization identified several major phases in the development of a medical device: (1) conception and development; (2) manufacturing; (3) packaging and labelling; (4) advertising; (5) sale; (6) use, and; (7) disposal. The manufacturer of the device is responsible for guiding the product through the creation process, including design, development, testing, manufacturing, packaging, and labelling. Since manufacturers typically do not sell their products on the market, a vendor is required to make the product available to end users, provide training, and engage in post-sales activities such as problem reporting. Users of medical devices are typically health care professionals, but may also be the patient herself, or a family member.

In the case of complex devices, users must receive extensive training that includes recommended operating procedures, indications, and contraindications. Proper use of a medical device is of the utmost importance. Even the most carefully crafted medical device can be harmful if used in a way that the manufacturer did not intend. Lack of calibration, inappropriate maintenance, reuse of disposable devices, substandard training, and poor technique can all result in high levels of risk with respect to devices that are normally safe and effective.

In addition to the quality of the product and the appropriateness of the uses to which it is put, there is a third element that is critical to ensuring patient safety – namely, the representation of the device to the user. In order to safely use the device, a user must not only be aware of the intended modes of operation, but also of the various constraints, risks, and limitations of the device. As a result, the advertising, packaging, and labelling of a medical device are of great importance to its safety, effectiveness, and performance.

---

complexity increases, unless work is done to maintain or reduce it, and; (3) the law of declining quality: the quality of systems will appear to be declining unless they are rigorously maintained and adapted to operational environment changes. See M.M. Lehman, “On Understanding Laws, Evolution, and Conservation in the Large-Program Life Cycle” (1980) 1 Journal of Systems and Software 213.

3.1.2 Regulatory Controls

In keeping with the observations above, regulatory regimes for medical devices must attend to each of the phases of the medical device lifecycle. First, *pre-market controls* attempt to reduce the risks inherent to the device itself, by focusing on the processes involved in bringing the device to market – namely, design, manufacture, packaging, and labelling. Second, *market controls* attempt to reduce the risks of misuse by concentrating on the advertising and sale of the device. Third, *post-market surveillance* aims at uncovering new information about a device by monitoring the performance of medical devices that are in use. In the following subsections, we will discuss these tools in more detail.

**Pre-Market Controls**

Pre-market controls are targeted at the safety and effectiveness of the medical device itself. Generally speaking, manufacturers follow a process that involves design, development, testing, manufacturing, packaging, and labelling. Regulatory regimes can attempt to influence each of these activities by the use of various tools. First, safety and effectiveness requirements can influence decisions made during the design phase. Second, quality system requirements can force manufacturers to meet international standards with respect to development, testing, and manufacturing. Third, labelling requirements may impose duties on manufacturers to provide accurate descriptions of the product, as well as its intended uses. Regulators may also require manufacturers to provide detailed instructions for the use of the device, including operating procedures and best practice guidelines.

Products that fail one or more of these tests may fail to obtain clearance to enter into the marketplace. In keeping with the risk management principles underlying medical device regulation, the degree of scrutiny generally increases with the risk profile of the device; devices that pose a greater risk of harm are subjected to greater levels of scrutiny. Devices with higher degrees of risk may also be subjected to a *device licensing* regime, whereby regulators refuse to allow a device into the marketplace until it has successfully cleared all of the relevant pre-market controls.

**Market Controls**

In contrast to pre-market controls, which concentrate on the process involved in producing the device, market controls focus on the process involved in supplying the device to the end user. There are two main mechanisms by which regulators assert control over the sales process. First, regulators can require vendors to register themselves. Typically referred to as *establishment control*, mandatory registration allows regulators to maintain a
database of information on vendors, including information on their administrative procedures with respect to complaints, monitoring, training, and education. Second, advertising controls impose restrictions on the ability of vendors to issue marketing materials regarding the device. Regulators can prohibit vendors from advertising a device before it has received clearance to enter into the market; they may also impose obligations on vendors to refrain from misleading or fraudulent advertisements.\(^\text{36}\)

**Post-Market Surveillance**

Post-market surveillance is a necessary supplement to pre-market and product representation controls. In general, even the best manufacturing, engineering, and communications discipline is not sufficient to prevent every form of failure or misuse. In particular, devices that perform well in the laboratory may have different characteristics when they are finally put to use outside of a controlled environment. In the Therac-25 example described earlier, a human operator with strong typing skills caused a race condition in the software – a possibility that was not caught during testing in the laboratory. As a result, it is important to continually assess the safety and performance of medical devices in real-world settings.

To this end, medical device regulators tend to rely on three main tools. First, surveillance studies can be used to augment the results of pre-market trials. In particular, studies can be required: (a) as a condition for manufacturer/vendor licensing; (b) for devices that present high risk profiles, and; (c) for devices that have been linked to harmful incidents. Second, regulators can require vendors or manufacturers to perform adverse event reporting, in which investigations are conducted on events that have resulted in (potential) harm to patients. (While mandatory reporting requirements are common for vendors and manufacturers, the duty to report adverse events can also be assigned to users.) Third, regulators can impose administrative obligations on vendors, including procedures for handling complaints and dealing with recalls.

### 3.1.3 Standards and Quality Frameworks

In the preceding discussion of pre-market controls, we mentioned that quality system requirements are a tool by which regulators can coerce

\(^{36}\) Other sources of law may also prohibit misleading or fraudulent advertising. The issue is beyond the scope of this paper.
manufacturers into adopting international standards. Standards can contain a number of components: (1) *prescriptive specifications* impose mandatory requirements on product characteristics; (2) *design specifications* impose constraints on the design of products; (3) *performance specifications* require that a product meet certain practical tests, and; (4) *management specifications* obligate manufacturers to put processes and procedures in place.37

### 3.1.4 Current Trends
One of the major trends in medical device regulation consists of harmonization efforts. Currently, vendors of medical devices must meet the regulatory requirements of each country in which they intend to market their products. The diversity of approaches to regulation can lead to increased costs and major delays in bringing products to global markets.

As a result of these concerns, regulators from Australia, Canada, the European Union, Japan, and the United States of America have formed the “Global Harmonization Task Force” (GHTF) – an organization tasked with harmonizing medical device regulations.38 The participants hope that harmonization will streamline the process of bringing products to the global market, while simultaneously standardizing the quality of the devices themselves.

### 3.2 Canada’s Medical Device Regulation and its application to PMS
Canada has an expansive and influential regime for the regulation of medical devices. Although we noted above that the administrative aspects of health care delivery are often a provincial responsibility, Canada’s medical device regulations are a creation of the federal government.39 In the following

---

37 For more information on the types of specifications in standards, see [http://www.iso.org].
38 See Global Harmonization Task Force (GHFT), online: GHFT [http://www.ghtf.org/].
39 The constitutional authority for federal regulation of medical devices was considered in *R. v. Wetmore*, [1983] 2 S.C.R. 284, 2 D.L.R. (4th) 577. In that case, the Supreme Court held that various provisions of the *Food and Drugs Act*, *supra* note 29, could be construed as measures aimed at protecting the physical health and safety of the public. As a result, the regulation of medical devices is considered to be a legitimate exercise of the federal government’s exclusive powers over matters of criminal law. See Jackman, *supra* note 28 at 99, for more information on this issue.
subsections we will briefly identify relevant portions of the Canadian regulatory framework.

3.2.1 Medical Devices: Definition and Classification
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.”

The Medical Devices Regulations (Regulations) subsequently defines a ‘medical device’ to be a device within the meaning of the Food and Drugs Act, but not one that is intended for use “in relation to animals.”

Schedule 1 of the Regulations provides rules for classifying medical devices into four increasing risk levels – Class I, Class II, Class III, and Class IV. In general, a medical device’s risk categorization is proportional to the intended purpose of the device, the type of contact that the device makes with the patient, and the degree of harm that could arise should the device fail. Schedule I, Part I of the Regulations sets out the rules for classifying medical devices.

While software has long been an embedded component within hardware-based medical devices, there has been a degree of uncertainty in the manufacturing community about the status of pure software systems. Thankfully, Health Canada has provided guidance in the form of a recently issued notice which declares that PMS qualifies as an ‘active device’.

In terms

40 Food and Drugs Act, supra note 29.
41 Medical Devices Regulations, S.O.R./98-282, s. 1 (1998) [Regulations], made under the powers granted in subsection 30(1) of the Food and Drugs Act, supra note 29.
42 Many of the rules are quite specific to various types of devices, and a full treatment is beyond the scope of this paper. According to section 6 of the Regulations, if a medical device fits into more than one class, the highest class applies.
43 For instance, pacemakers, CT-scanners, and drug infusion pumps.
44 Health Canada, “Classification of Medical Devices Class I or Class II patient management software” (31 August 2009). This notice was updated December 3, 2010: Health Canada, “Notice – Software Regulated as a Class I or Class II
of risk classification, PMS that is used only for storing, acquiring, transferring, or viewing data or images is considered a Class I medical device. In contrast, PMS with capabilities beyond basic data visualization, acquisition, transfer, and storage is considered a Class II medical device. As mentioned above, Health Canada has indicated that: (a) EMR, EHR, and PHR systems are indeed PMS in this sense, and; (b) mere scheduling and billing software do not qualify as medical devices. If a PHR, EHR, or EMR system provides decision-support, diagnostic, or automated alert functionality, it will likely qualify as a Class II medical device.

The Regulations apply to any PMS sold in Canada. The definition of ‘sell’ in the Food and Drugs Act is expansive, and includes to “offer for sale, expose for sale, have in possession for sale and distribute, whether or not the distribution is made for consideration.” At present, it appears that many EMR and PHR offerings are ‘sold’, in the sense required by the Act. An EHR that is developed ‘in-house’ by a health care organization or government (for exclusive use by that organization or government) will not qualify as a device being ‘sold’. However, if the EHR is given to another organization, it will count as a medical device being distributed.

3.2.2 Regulatory Controls
Sections 10 through 20 of the Regulations set out the safety and effectiveness requirements for medical devices – pre-market controls that apply to every


45 Any PMS used only for storing, acquiring, transferring, or viewing data, or images is considered a Class I medical device based on Rule 12, Schedule I, of the Regulations. See also ITAC, supra note 44 at 10, which states: “Only calculations that directly impact diagnosis and/or treatment of a patient merit a Class II designation for the software in which they are utilized. Calculations and manipulations, which are used to perform only administrative functions such as determining time between appointments, do not result in a Class II software classification.”

46 Supra note 29, s. 2.
medical device, save those that are custom-made, imported/sold for special access, or used for investigational testing on human subjects. At a high level, the requirements deal with the design, manufacture, and labelling of the device. Included in the requirements are provisions relating to safety, performance, sterilization, deterioration, and risk management. Manufacturers are obligated to maintain records demonstrating that the safety and effectiveness requirements are met by their products.

**Establishment Licenses**

Section 44 of the Regulations prohibits a person from importing or selling a medical device unless the person first obtains an establishment license. This requirement serves to register a vendor or manufacturer with Health Canada, allowing the latter organization to amass information on the state of the market. Establishment licenses are valid for one year. Under sections 47 and 49, Health Canada may refuse to issue a new license or suspend an existing one.

**Device Licenses**

Any organization that intends to import or sell a medical device is subject to pre-market controls that are intended to enhance the safety and effectiveness of the device. The requirements imposed on a particular device depend upon its risk classification, as well the functional role of the organization. In keeping with a risk management approach, the licensing requirements become more onerous as the risk level increases. In contrast to Class I devices, Class II, III and IV medical devices must be licensed with Health Canada.

As part of the licensure process, vendors have to provide objective evidence that their products meet the safety and effectiveness requirements referred to above. The precise requirements depend on the risk classification of the device, with higher risk classes attracting more substantial obliga-

47 A discussion of these exceptions is beyond the scope of this paper.
48 Subsection 44(2) provides carefully chosen exceptions to this rule.
49 Organizations may be acting as a manufacturer, retailer, distributor or importer. The regulatory controls in the Regulations catch each of these functional roles in a distinct manner.
50 According to section 26 of the Regulations, unlicensed devices may not be imported or sold. In addition, subsection 27(b) imposes restrictions on advertising.
Device licenses must be renewed annually. According to subsection 36(1)(b), the Minister may “amend the terms and conditions of the medical device license to take into account any new development with respect to the device.” Under subsection 40(1), the Minister may suspend a medical device license if certain conditions are not met.

Regardless of risk class, each device must satisfy a set of common requirements in order to qualify for a medical device license. In addition to the name, class, and identifier of the device, the license application must list the name and address of both the manufacturer and the manufacturing facility. Once the common requirements are achieved, the device must satisfy the requirements for its risk class.51

**Labelling and Advertising Requirements**

Subsection 21(1) of the Regulations imposes constraints on the labels attached to a medical device. Among other elements, the label must include: (a) the expiry date of the device, if the device has one, and; (b) the medical conditions, purposes, and uses for which the device is manufactured, sold, or represented.52 According to subsection 21(2), the mandatory information on a device label must be expressed in a “legible, permanent and prominent manner, in terms that are easily understood by the intended user.”53

---

51 For example, subsection 32(2) dictates that the information provided in support of a Class II device (i.e., a typical PMS) must include: “(a) a description of the medical conditions, purposes and uses for which the device is manufactured, sold or represented; (b) a list of the standards complied with in the manufacture of the device to satisfy the safety and effectiveness requirements; (c) an attestation by a senior official of the manufacturer that the manufacturer has objective evidence to establish that the device meets the safety and effectiveness requirements ... and; (f) a copy of the quality management system certificate certifying that the quality management system under which the device is manufactured satisfies National Standard of Canada CAN/CSA-ISO 13485:03, Medical devices – Quality management systems – Requirements for regulatory purposes.”

52 The description of medical conditions, purposes, and uses includes the performance specifications of the device, if those specifications are necessary for proper use.

53 In addition, section 21 and subsection 20(1) of the Food and Drugs Act, supra note 29, contains provisions relating to labelling, packaging, and advertising.
**Complaint Handling**

Subsection 57(1) requires the manufacturer, importer, and distributor of a medical device to maintain records relating to: “(a) reported problems relating to the performance characteristics or safety of the device, including any consumer complaints... and; (b) all actions taken by the manufacturer, importer or distributor in response to these problems.” The same organizations are obligated in section 58 to establish and implement documented procedures to facilitate: (a) an “effective and timely investigation” of any reported problems, and; (b) an “effective and timely recall of the device.”

**Distribution Records**

Subsection 52(1) requires the manufacturer, importer, and distributor of a medical device to maintain a distribution record in respect of each device. Section 53 mandates that this record must contain “sufficient information to permit complete and rapid withdrawal of the medical device from the market.” The Regulations also contain provisions relating to retention times for these records (s. 55).

**Mandatory Problem Reporting**

Subsection 59(1) obligates manufacturers and importers to make preliminary and final reports to Health Canada concerning any incident involving their device that: (a) is related to the failure or deterioration of the device or inadequacies in the labelling or directions for use, and; (b) has (or could have) led to a death or serious deterioration in the health of a patient, user, or other person. The Regulations contain information on the content of, and administrative procedures for, these reports (ss. 60-61.1).

**Recall**

Section 58 dictates that the manufacturer or importer of a medical device must establish and implement documented procedures for carrying out: (a) an effective and timely investigation of reported problems relating to the performance or safety of the device, including any customer complaints, and; (b) an effective and timely recall of the device. The provisions in Section 64 and 65 establish reporting obligations, whereby the manufacturer or importer must provide certain information concerning to Health Canada upon planning, executing or completing a recall. Of particular importance is subsection 65(b), which requires the manufacturer or importer to report the action taken to prevent a recurrence of the problem.
3.2.3 Invoked Standards
Medical devices of Class II are subject to CAN/CSA-ISO 13485:03 (ISO 13485), an international standard on quality management for medical devices. The standard was specifically created for regulatory purposes and currently exists in the second edition, which superseded the first edition released in 1996. ISO 13485 is based on the generic ISO 9001 quality management standard, and follows a process-focused approach to quality management, as opposed to a product-focused approach. In order to aid manufacturers and regulators, the International Organization for Standardization further published a technical report to provide guidance on applying ISO 13485.

Among other obligations, ISO 13485 requires organizations to put in place quality management processes, and to monitor and optimize their effectiveness. Some of its requirements obligate organizations to: (a) maintain a set of key documents; (b) assign defined management responsibilities; (c) maintain a focus on quality, throughout the development of human and infrastructure resources; and; (d) utilize relevant communication processes, such as customer complaint procedures and advisory notices. The standard prescribes aspects of technical as well as non-technical product lifecycle processes, such as installation and purchasing. ISO 13485 requires manufacturers to assign to products unique identifiers (for tracking returned products), and to establish traceability between product documentation and the uniquely identified products themselves, which are conforming to the documentation.

3.3 Privacy Statutes

Statutes regulating the collection, use, and disclosure of personal information have been passed at both the federal and provincial level. In general, Canadian privacy statutes take their inspiration from a set of ‘fair information practices’ promulgated 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*\(^\text{58}\), the Canadian Standards Association (CSA) created the *Model Code for the Protection of Personal Information (Model Code)* in 1996.\(^\text{59}\) While the federal government had already passed a privacy statute binding on federal public bodies\(^\text{60}\), the development of a statute for the private sector was given impetus by a directive of the European Union that prohibited member states from transferring data to jurisdictions with inadequate privacy protection.\(^\text{61}\)

The resulting *Personal Information Protection and Electronic Documents Act (PIPEDA)* is a federal statute that applies to organizations that are engaged in commercial activities.\(^\text{62}\) Although *PIPEDA* was originally described as a

\(^{25238}\text{represents an agreement of an ISO technical committee, but has not been balloted with all international member bodies. ISO/TS 25238 has been created specifically in recognition that the risk posed by using health software is increasing rapidly due to the increased complexity, adoption, and sophistication of these systems. The technical specification makes an important contribution in defining five severity risk classes for medical software, as well as a process on how to assign these classes to different types of software systems. Also see International Electrotechnical Commission (IEC), “IEC 62304:2006(E) Medical device software – Software life cycle processes”, online: IEC <http://www.iec.ch/cgi-bin/procgi.pl/www/iecwww.p?wwwlang=E&wwwprog=cat-det.p&progb=1&wartnum=036055>.}

\(^{58}\text{Organization for Economic Cooperation and Development (OECD), *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (OECD, February 2002).}


\(^{60}\text{The federal *Privacy Act*, R.S.C. 1985, c. P-21, came into force on July 1
\(^{\text{th}}\) 1983.}

\(^{61}\text{EC, *Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, [1995] O.J. L 281/31.}

\(^{62}\text{*Personal Information Protection and Electronic Documents Act*, S.C. 2000, c.5 (PIPEDA).}
means for enhancing consumer confidence in electronic commerce applications, the statute contains provisions that regulate the collection, use, and disclosure of personal information in a wide variety of additional contexts. 

PIPEDA explicitly incorporates the CSA Model Code in the form of a schedule, albeit one that is slightly modified by select provisions in the statute’s main text. PIPEDA applies to activities in the various provinces, save those that have passed legislation that is ‘substantially similar’. Generally speaking, PIPEDA will not apply to PMS deployed by health authorities or governmental agencies.

The impact of PIPEDA on organizations hosting PMS is not amenable to a brief treatment. For our purposes, the statute requires vendors to implement security safeguards, including physical, administrative, and technical security mechanisms. Vendors are obliged to protect personal information from loss and theft, as well as unauthorized access, disclosure, copying, use, or modification. Although PIPEDA imposes an obligation, it does not contain detailed prescriptions on the nature of the safeguards; on the contrary, the statute explicitly allows organizations to vary the nature of the safeguards in response to the sensitivity of the information.

In addition to the provisions concerning security, 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. Lastly, subsection 4(9) of the Schedule 1 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.

63 See, for example, Stephanie Perrin et al., The Personal Information Protection and Electronic Documents Act: An Annotated Guide (Toronto: Irwin Law, 2001).

64 PIPEDA’s provisions concerning safeguards (security) are presented in subsection 4(7) of Schedule 1.

65 At the time of writing, PIPEDA does not contain provisions mandating that organizations report privacy breaches to either: (a) those individuals whose information was compromised, or; (b) the federal Privacy Commissioner. However, proposed amendments to PIPEDA require breach notification. Section 10.1 of Bill C-29 requires organizations to report any “material breach of security safeguards” to the Commissioner, Bill C-29, An Act to amend the Personal Information Protection and Electronic Documents Act, 3rd Sess., 40th Parl., 2010. Section 10.2 requires organization to report if “breach creates a real risk of significant harm to the individual”. Guidance on the meaning of the concepts ‘material breach’, ‘significant harm’ and ‘real risk’ are provided.
3.4 Health Information Statutes

Certain provinces have passed legislation that specifically targets organizations and individuals managing health information. For instance, Ontario’s *Personal Health Information Protection Act (PHIPA)* and its accompanying regulations\(^{66}\) were drafted out of a concern that the general purpose privacy statutes such as *PIPEDA* were not suitable for application in a health care environment.\(^{67}\) As a result, health care providers in Ontario that are subject to *PHIPA* have received an explicit exemption from *PIPEDA*.\(^{68}\) In terms of application, *PHIPA* only binds a select set of ‘health information custodians’ (custodians), as well as select organizations that either: (a) provide services to them\(^{69}\), or; (b) receive PHI from them.\(^{70}\)

The bulk of *PHIPA’s* weight falls on the custodians. First, the statute contains breach notification provisions that require custodians to inform a patient at the first reasonable opportunity if the patient’s information is compromised. Subsection 11(1) requires custodians to take reasonable steps to ensure that PHI is accurate, complete, and up-to-date. Subsection 12(1)

---


\(^{67}\) In addition to the fact that *PIPEDA* requires consent for secondary uses and disclosures of personal information, the statute also contains provisions that may restrict the ability of health care providers to release information to one another. In particular, subsection 9(1) states that vendors “shall not give an individual access to personal information if doing so would likely reveal personal information about a third party.” Given the hereditary nature of many medical conditions, following this rule strictly would prohibit custodians from sharing certain types of information.

\(^{68}\) *Health Information Custodians in the Province of Ontario Exemption Order*, S.O.R./2005-399, made under *PIPEDA*.

\(^{69}\) Subsection 6(1) of O. Reg. 329/04 concerns persons who provide “services for the purpose of enabling a health information custodian to use electronic means to collect, use, modify, disclose, retain or dispose of personal health information”. Subsection 6(2) states that a ‘health information network provider’ is “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 personal health information to one another”.

\(^{70}\) Subsections 49(1) and 49(2) of *PHIPA* impose constraints on the ability of organizations to use or disclose information that has been given to them by health information custodians.
requires custodians to take steps that are “reasonable in the circumstances” to ensure that PHI in its custody or control is protected against theft, loss, and unauthorized use or disclosure.

In addition, PHIPA imposes substantial requirements on organizations that either receive data from, or provide services to, health information custodians. For example, organizations that provide services to custodians (in the sense of subsection 6(1) of O. Reg. 329/04) face constraints on their ability to use, disclose, or permit access to any PHI to which they have access in the course of providing services.\(^{71}\) Health information network providers face a much more verbose set of obligations, including mandatory breach disclosure, audit trails, and threat/risk assessments.\(^{72}\)

### 3.5 Industry Standards

Canadian industry standards for PMS are still in a state of development. Canada Health Infoway (Infoway) has recently introduced a certification program for client registries, consumer health applications, consumer health platforms, Diagnostic Imaging (DI), Drug Information Systems (DIS), provider registries and immunization registries.\(^{73}\) Infoway’s certification focuses on privacy and security. Interoperability and functionality criteria of systems applying for certification are assessed against Infoway’s EHR architecture requirements and technical standards. In addition to Infoway’s efforts, several provinces have initiated certification programs for EMR products, under the aegis of provincial initiatives to foster the adoption of EMR technologies.\(^{74}\)

### 3.6 Professional Bodies

Self-regulating professional bodies are subject to legislation that imposes constraints on the behaviour of their members. For instance, the College of Physicians and Surgeons of Ontario has received powers under both the

---

71 Subsection 6(1) of O. Reg. 329/04.
72 Subsection 6(3) of O. Reg. 329/04.
Regulated Health Professions Act, 1991 and the Medicine Act, 1991. The latter statute obligates physicians to maintain medical records in accordance with a set of core information practices. For example, section 20 of the Medicine Act, 1991,‘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 concerning security and privacy.

4 Analysis

Having introduced some of the key elements of the regulatory regime for PMS in Canada, we turn our attention to a critical examination of its adequacy. In order to guide our discussion, we identify four major policy objectives for regulators, namely: (1) privacy/security; (2) safety; (3) effectiveness, and; (4) innovation. Privacy and security are objectives that any regulatory regime for PMS should encourage, given the sensitivity and value of PHI. While traditional medical devices may not have evidenced major privacy and security risks, modern information systems are markedly different. Safety (for both the patient and the user/operator) is a long-acknowledged objective within medical device regimes, and many interesting questions arise when applying it to pure software systems. Effectiveness is also important, as a regulatory scheme should provide incentives for manufacturers to develop software that achieves its ends. Lastly, innovation is critical for the development of PMS systems; policies that retard this objective include measures that discourage competition, create strong barriers to entry, and place an undue burden on smaller companies.

A common method of analyzing regulatory regimes is to view the process of regulation as a balancing act between key policy objectives. In the case of PMS, adopting this viewpoint leads to some fairly practical heuristics. At the most abstract level, a designer of a regulatory regime for PMS

---

76 General, O. Reg. 111/94 of Medicine Act, 1991. To take but three examples: (1) the computer 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; (2) the system must include “a password or otherwise provide reasonable protection against unauthorized access”; and, (3) the system used by a physician must automatically back up files and must provide “reasonable protection against loss of, damage to and inaccessibility of, information.”
should ensure that privacy/security/safety risks of a product are outweighed by tangible benefits (effectiveness), as well as a market place hospitable to innovation and competition. Benefits may manifest at the individual level (micro-level), at the organizational level (meso-level), or at the systemic level (macro level). The latter two levels are particularly important with PMS, since electronic information management is expected to improve the long term sustainability of the public health care system, increase access to information for evidence based medical research, and provide for better public health surveillance and control of outbreaks of diseases.

Despite our concise listing of policy objectives for PMS, we caution the reader that there are many overlaps to be found. To take but one instance, there is a significant overlap (if not outright interference) between the safety and security objectives. This overlap becomes apparent when considering the three main aspects of information security, namely: (1) confidentiality; (2) integrity, and; (3) availability. Three immediate examples of safety issues spring to mind, from considering these criteria. First, a failure to make information stored in a PMS available can cause major safety concerns if that information is needed for treatment. Second, a failure to safeguard the integrity of information can lead to serious safety issues, such as the prescription of incorrect medications. Third (and perhaps most surprising), failure to safeguard the confidentiality of information stored in a PMS can compromise patient safety. Breaches of confidentiality can result in the misuse of sensitive information by an adversary, such as an ex-spouse or employer.

4.1 Privacy and Security

Privacy and security issues become quite pronounced with PMS, given the large number of users that have access to information in these systems. While sharing medical information amongst distributed teams of practitioners is a promising means of supporting collaborative care, it also entails significant privacy and security risks. As a result of this sensitive, a regulatory regime should (at minimum): (a) provide an incentive (perhaps determinative) for the development of PMS systems that provide adequate safeguards; (b) encourage organizations hosting or using PMS to adopt administrative mechanisms that reduce privacy and security risks, and; (c) educate developers about the ways in which they can embed privacy and security protections into their products.

As related in Section 3.3 of this paper, privacy and security objectives are largely articulated in privacy legislation, as well as the specialized health information statutes passed in some provinces. Although we can only present a few examples, it is clear that some of the security and privacy issues
affecting PMS are allayed by the current regulatory framework in Canada. First, privacy statutes impose restrictions on the collection, use, disclosure, and retention of personal information, including prohibitions on many types of secondary uses. Second, they provide for a set of administrative safeguards, such as a requirement to correct erroneous information. Third, privacy statutes typically address the accuracy dimension of privacy (and the integrity dimension of security) by requiring organizations to ensure that PHI stored in the PMS is accurate and up-to-date. Fourth, some statutes require organizations providing or using PMS to keep audit trails of access to PHI. Fifth, privacy statutes mandate the use of security safeguards, including physical, technical, and administrative mechanisms.

Despite the broad reach of these instruments, it is clear that there are some gaps. As a first example, the patchwork of privacy legislation has left a scattered body of law that lacks a unified vision for information security in the health care domain. Second, the regulatory framework does not adequately address the issue of encouraging developers to build privacy into their products. While the ‘privacy-by-design’ campaign has attempted to instill awareness of privacy issues in the vendor community, the lack of methodologies for integrating privacy into software development processes is a major roadblock. Third, there is a distinct lack of precision in the provisions concerning safeguards.

4.2 Safety
In Canada, legal obligations concerning safety are a product of the Regulations. First, section 10 obligates vendors to ensure that medical devices are designed and manufactured to be safe. Second, the same provision assigns manufacturers a duty to: (1) take reasonable measures to identify risks, eliminating or reducing them to the extent possible; (2) provide protection for residual risks; (3) inform the user/purchaser of residual risks, and; (4)

77 For instance, many influential pronouncements on security safeguards have been issued in by the Ontario Information and Privacy Commissioner. (For example, see Order HO-007, dealing with encryption on mobile devices). The lack of a comprehensive, pan-Canadian approach to information security has been partially addressed by COACH: Canada’s Health Informatics Association, which issues a yearly set of guidelines, online: COACH <www.coachorg.com>.
79 Supra note 41.
minimize the hazard from potential failures.\textsuperscript{80} Third, section 20 states that “[i]f 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.”\textsuperscript{81} Fourth, regulators have enforcement power; medical devices can be cancelled or suspended if they fail to meet safety requirements.\textsuperscript{82}

In addition to these protections, the imposition of quality certificates and international standards will positively influence process maturity. As we noted above, many PMS applications are developed using an immature methodology; for example, initiatives may lack formal documentation or a design process that anticipates and plans for failure. Thankfully, applying for a license under the \textit{Regulations} requires a manufacturer to provide evidence of a quality-oriented process, including technical documentation and verification/validation artifacts.

Despite these positives, it is clear that there are unique aspects of PMS that are not sufficiently addressed by the current regulatory framework. First, software safety is significantly different from hardware safety. The \textit{Regulations} contains only a few references to software, most of which appear to address properties of hardware-based medical devices. Many of the requirements involve concepts foreign to software, including sterilization, flam-

\textsuperscript{80} In addition, section 11 states that “[a] medical device shall not, when used for the medical conditions, purposes or uses for which it is manufactured, sold or represented, adversely affect the health or safety of a patient, user or other person, except to the extent that a possible adverse effect of the device constitutes an acceptable risk when weighed against the benefits to the patient and the risk is compatible with a high level of protection of health and safety.”

\textsuperscript{81} According to the Institute of Electrical and Electronics Engineers (IEEE), software validation is “the process of evaluating a system or component during or at the end of the development process to determine whether it satisfies specified requirements”, IEEE, \textit{IEEE Standard Computer Dictionary} (New York: IEEE, 1990), online: IEEE <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=182763>, \textit{s.v.} “validation”. Applying this definition to the section 20 of the \textit{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.).

\textsuperscript{82} See, for instance, section 40 of the \textit{Regulations} for the Minister’s powers of suspension.
mability, and robustness in the face of transport/storage. Although one can find creative applications for these terms, the applicability of these provisions is questionable at best, as the risks and properties of software are quite different from those inherent to mechanical devices. Subjecting software to a regulatory regime that is based on physical properties is questionable from both a conceptual and practical standpoint.

A second concern is that current lifecycle controls are insufficient for software. Software evolves rapidly, and each new release may involve significant changes. In addition, software quality deteriorates over time. While the Regulations requires relicensing of class III and IV medical devices in case of ‘significant changes’, a PMS instance will be classified as a Class II (or even Class I) device. There is no requirement to perform relicensing of a Class I or II device, even if major changes have been implemented over its lifetime. As ISO/TS 25238 clearly demonstrates, certain types of PMS are critical and should be classified in the highest risk categories. Without accommodating this fact, the Canadian approach to regulating PMS is questionable. In particular, a product-focused licensing regime that does not take into account the evolutionary nature of software will not be effective.

A third safety issue arises from the lack of attention that the current regime pays to source code. As we noted above, section 20 of the Regula-
tions specifically addresses software, holding that: (1) the software must be designed to perform as intended, and; (2) the performance shall be validated. The required ISO 13485 certification furthermore implies that the manufacturer must keep and provide documents specifying their intentions (requirements) and a record on the performance validations. This is a positive step, since it accommodates cases like the Therac-25 accidents (where the manufacturer claimed to have done performance validations of the software but they could not produce the test plans). Unfortunately, the regulation focuses on product documentation and processes, and not on the product itself. In particular, the source code is often the only reliable source of information about the true design of a software system. Although apparently overlooked by lawyers and policy makers, Parnas and Clements long ago provided a convincing explanation as to why mere validation requirements (not having access to source code) are not sufficient.

Thankfully, software engineers have produced effective tools and methods to measure design erosion and source code quality. While these tools provide auditors with an inexpensive means of validating safety properties of software, they require access to source code.

88 ISO 13485, supra note 54.
4.3 Effectiveness
The notion of effectiveness is central to many provisions in the Regulations. For instance, section 32 requires applicants for a medical device license to demonstrate that their product meets the safety and effectiveness requirements. At lower risk levels, an attestation that the manufacturer has ‘objective evidence’ is satisfactory; at higher risk levels, summaries of studies (including software validation studies) are required.\textsuperscript{91}

A major issue with the current regime is that it lacks guidance on how to validate the effectiveness of PMS. While other jurisdictions have developed concrete criteria for this purpose\textsuperscript{92}, Canada lacks such information. This deficiency makes it impossible to objectively judge the effectiveness of a given product and to compare competing offerings. Not only does this impede a purchaser’s ability to choose the best product, but it also leaves the vendor community without a set of tools by which they can demonstrate effectiveness. This could create rigidity in the marketplace; new entrants will have a difficult time demonstrating effectiveness, while established vendors can rely on their existing product installations (even if those are not well received by users).\textsuperscript{93}

A second point pertaining to effectiveness (and safety) considers interoperability. As we pointed out above, medical device regimes are based on the traditional paradigm where devices generally do not interoperate. This approach breaks down once PMS are introduced. An increasing number of PMS are able to interact with other devices (including other PMS); in fact, the industry appears to be increasingly empowering clinicians to connect

\textsuperscript{91} See the Class IV requirements for medical device licenses, outlined in subsection 34(4) of the Regulations, \textit{supra} note 41.
\textsuperscript{92} The United States \textit{Health Information Technology for Economic and Clinical Health Act} (Title XIII of Division A and Title IV of Division B of the \textit{American Recovery and Reinvestment Act of 2009}, Pub. L. No. 111-5) provides incentive payments to health care providers when they use PMS privately and securely to achieve specified improvements in care delivery. In order to qualify under the \textit{Act}, PMS vendors must certify that their products can fulfill the meaningful use objectives. For more information, see David Blumenthal & Marilyn Tavenner, “The ‘Meaningful Use’ Regulation for Electronic Health Records” \textit{Health Policy and Reform} (13 July 2010), online: New England Journal of Medicine, Health Policy and Reform <http://healthpolicyandreform.nejm.org/?p=3732>.
\textsuperscript{93} As we argue below, the cost of switching from one PMS product to another can lead to vendor lock-in, which can make existing companies complacent.
multiple devices on the fly (‘plug and play’). As a result of these developments, PMS needs to be able to interact/interoperate effectively (and safely). To be clear, section 18 of the Regulations partially anticipates the composition of devices, demanding that “[a] medical device that is part of a system shall be compatible with every other component or part of the system with which it interacts and shall not adversely affect the performance of that system.” However, the provision assumes that all other components of the system are known beforehand by the device manufacturer, who is therefore in a position to validate all potential compositions/interactions. This is usually not feasible for software components, which often have standards-based interfaces that allow them to interact with other components in a dynamic and unpredictable manner.

A third point pertaining to effectiveness (and safety) concerns the labelling requirements contained in the Regulations. These do not readily translate to software, which do not age in the same way as a hardware device. Software does not degrade physically, but updates and revisions typically introduce risks. As a result, expiration dates may still be very relevant for the safe operation of PMS. In addition, changes to the environment in which the software operates (such as interfaces to other systems, operating systems, or database management software) may also introduce risk. It has been shown that the likelihood that a software device will remain safe and reliable decreases with subsequent updates to its environment. While hardware-based notions like expiration may very well apply to purely software-based medical devices, the metaphors are not obvious; as with other terms drawn from the hardware domain, software manufacturers are likely to miss these connections without further clarification.

Similar confusion exists on how to affix labels to software as required by the Regulations subsection 21(2): in a “legible, permanent and prominent manner, in terms that are easily understood by the intended user.” The

95 Supra note 41.
96 For example, any knowledge-based systems, including but not limited to decision-support systems, diagnostic systems, and systems for automating best-practice guidelines and processes, will invariably expire and lose effectiveness if they are not updated. Indeed, the aforementioned ISO/TS 25238, supra note 57, mentions this problem as one of the hazards for such systems.
97 Operating system platform, computer platform, networking platform, etc.
seemingly obvious approach of labelling the box that contains the installation media for the software may not be effective for several reasons: (1) as we pointed out earlier, PMS is rarely ready to be used out of the box and undergoes significant customization at the point of service; (2) modern software is often updated via the network after installation, and these updates may impact its purpose and intended use, and; (3) software is increasingly provided as a hosted service rather than a boxed product.  

4.4 Innovation and Market Impact

The best innovations in information technology tend to arise from diverse marketplaces with low barriers to entry. Regulations that impose a significant cost may have the effect of discouraging competition and innovation. As a matter of fact, Health Canada’s aforementioned notification concerning PMS invoked significant criticism from the PMS vendor community. Much of that criticism pertains to the requirement of vendors to achieve ISO 13485 certification, which may represent a significant burden for small companies seeking to enter into the market. The benefit of the compulsory ISO 13485 certificate for PMS vendors is also open to debate, since ISO 13485 is a process-focused certification and does not evaluate the quality of the actual product. In particular, process-focused certification regimes have been criticized because of their ineffectiveness.

In addition to these concerns, we have identified several additional issues with the current regulatory framework for PMS that pertain to incentives and market composition. We detail these issues in the sub-sections below:

**Issue 1: Hosted Software**

The ‘software as a product’ paradigm is giving way to a ‘software as a service’ paradigm. Many software packages are already provided as services, rather than shipped products. The Canadian medical device regime does not adequately address this issue. If hosted services are removed from the scope of the regulatory framework, vendors that provide hosted applications incur

98 Affixing labels as ‘alert boxes’ prior to users logging in to such hosted systems may not be effective either, given the likelihood of routine dismissals based on the earlier observations we made about ‘alert fatigue’.

99 See discussion above in Section 3.2.1.

greatly reduced costs. This dynamic will provide an incentive for vendors to develop hosted products, which may carry greater security and privacy risks.

**Issue 2: Custom-Made Devices**

Another problem pertains to the unclear notion of what constitutes ‘custom developed’ software. Health Canada explicitly excludes ‘custom developed’ software from the licensure requirement. Unfortunately, the terms ‘custom’ and ‘mass produced’ do not readily translate to software-based medical devices, leaving much room for interpretation. For example, most current PMS can be considered mass-produced or custom-made, based on the particular viewpoint taken. Virtually no current software product contains program code that is entirely written ‘from scratch’; best practices in software engineering encourage the reuse of ‘off-the-shelf’ components, such as frameworks and libraries.

At the same time, most PMS are customized (‘custom-made’) when they are deployed to configure them to a particular clinical context, workflow, or practice model. Some PMS even provide their users with ongoing support to customize their product. Customization can be a major source of errors, in the case of large-scale software systems.

**Issue 3: Quality Assurance and Monitoring**

As we mentioned above, most medical device regimes provide for mandatory adverse event reporting on the part of vendors. Unfortunately, there are strong reasons for believing that this type of feedback mechanism is insufficient for PMS. The complexity of large-scale software systems is very high, resulting in patterns of behaviour and latent defects that are difficult to predict in advance. A system that performs well under laboratory conditions may fail in the field.

As a result of these concerns, some commentators have proposed a quality assurance and monitoring program that goes far beyond the one implied by medical device regimes. Such a program may include: (1) field testing of all software; (2) the use of local committees staffed with regional

---

101 As Owens describes: “Vendors provide rudimentary clinical content with the expectation that physicians will want to modify it to meet the needs of their individual practice style”, K. Owens, “Customizing an EHR: Lessons Learned” (2009) 23:4 Journal of Medical Practice Management 212. More clarification on this issue is needed.

102 As we saw with the Therac-25 accidents.
experts, tasked with monitoring products in the field; (3) strong pre-market approval mechanisms, and; (4) ongoing, post-market monitoring that involves proactive detection of defects.\textsuperscript{103} Adverse event reporting may be a necessary but not sufficient component of such a quality assurance and risk mitigation strategy. In particular, mandatory user reporting is an element missing in the Canadian regime. Given the Therac-25 accidents, it is worth asking whether such a requirement is worth introducing.

**Issue 4: Recall**

Once problems arise, products may be subject to recall. Unfortunately, recalling PMS is problematic. First, since software is immaterial it can be easily multiplied unless the manufacturer has put safeguards in place that impede users from making copies of the software without the manufacturer’s authorization.\textsuperscript{104} Second, in contrast to traditional medical devices, PMS have a memory. Much of their value is in the patient data accumulated in their databases, which cannot easily be migrated to alternative software in the event of a recall.\textsuperscript{105} Consequently, a recall action on a PMS may render important data about a large cohort of patients partially unavailable, therefore adversely impacting their safety. Given the dense network of contracts, data sharing agreements, and dependent organizations involved in an EHR, a recall may be an incredibly time-consuming effort on an administrative and legal level. This could lock organizations into their current product offerings, even if the quality of those offerings is not on par with market competitors.

**Issue 5: Enforcement and Incentives**

At the time of writing, it is unclear that Health Canada has the resources to effectively enforce compliance with the medical device regime, as applied to software products. Given the relatively high costs of compliance and the uncertain prospects of effective enforcement, some vendors have voiced concerns about the feasibility of subjecting PMS to medical device law.\textsuperscript{106}

\textsuperscript{103} Hoffman & Podgurski, supra note 1 at 143-150.

\textsuperscript{104} The requirement in the Regulations, supra note 41, for keeping complete distribution records can be viewed as charging software device manufacturers with an obligation to put in place reasonable safeguards to prevent unauthorized copies. This is very difficult, as the software industry has discovered.

\textsuperscript{105} Data migration efforts on EHR systems are significant undertakings, requiring expertise, resources, and many months of preparation and planning.

\textsuperscript{106} See, for example, ITAC Health – Patient Management Software Licensing Group,
This incentive structure could distort market conditions, putting compliant companies at a disadvantage; it also will give large companies (who are often less innovative and responsive to customer/user feedback) an edge.

5 Conclusion

Driven by the requirement for immediate and effective health care reform, the demand for health care ICT is growing rapidly. The transition from traditional paper-based practices to software-based solutions will have a major and lasting impact on our health care service system, bestowing benefits as well as risks. Given the critical role of PMS in the health care system, regulators have an interest in ensuring the privacy, security, safety, and efficacy of product offerings. While many jurisdictions have considered introducing (or have already introduced) legislation to regulate quality aspects of PMS, Canada has recently announced that it considers PMS to be covered by its medical device regime. In addition to medical device law, other instruments apply to PMS, including privacy legislation and industry-promulgated standards. Our aim in this paper was to: (a) characterize the concept of PMS; (b) survey the current regulatory regime pertaining to it, and; (c) to analyze its strengths and weaknesses.

Although some of the issues with PMS are clearly within the scope of the various statutes and regulations, major gaps remain. These issues range from conceptual mismatches and a failure to recognize the unique quality attributes of software systems, to concerns about development processes and quality management approaches. Below, we provide several major recommendations for addressing the issues that we discovered.

First, we recommend that regulators rethink their strategy of classifying PMS in the lowest risk categories. The current classification of PMS as Class I (low risk) or Class II (low-medium) medical devices is insufficient, as many types of PMS can be considered high risk. One main problem with the low risk level for PMS is that significant product changes do not require

“Are EMRs Medical Devices?” (11 August 2010), online: ITACH Health <http://itachealth.blogspot.com/2010/08/are-emrs-medical-devices_11.html>. 107 For example, Physician Order Entry software – a type of software that has been accounted for many injuries and deaths due to wrong prescriptions. See, for example, Ross Koppel et al., “The Role of Computerized Physician Order Entry Systems in Facilitating Medication Errors” (2005) 293 Journal of the American Medical Association 1197.
relicensing. As we know from other domains, software evolves dramatically over time and so do the quality attributes associated with it. By allowing PMS vendors to avoid relicensing (even with major changes to the system), regulators may be vitiating the policy objectives of safety and effectiveness.

Second, we recommend that regulators clarify key issues. For instance, the treatment of ‘custom-built’ versus ‘commercial-off-the-shelf’ software is quite confusing. As we pointed out earlier, virtually all modern software is built with some ‘sold’ components and also provides means for customization. Similarly confusing is the treatment of the ‘software as a service’ paradigm; the current approach creates an incentive for vendors to deploy hosted products, which often carry higher security and privacy risks.

Third, we recommend that regulators work with vendors to develop methods by which the latter may demonstrate the effectiveness of their software products. While daunting, there are precursors; Canada may learn from other jurisdictions, including the US and its ‘meaningful use’ approach.

Additional recommendations are implicit in the criticisms made throughout this work. We hope that the observations contained in this paper will prove useful to policy makers. Further effort is needed in this area in order to understand how best to meet the disparate set of policy goals surrounding the use of software in the health care domain.

108 For example, current Windows 7 operating system has very different quality attributes compared from Windows 3.1, including completely different designs and risk factors.
109 See discussion in note 92 above.