LEGAL NORMS AND PUBLIC POLICIES IMPACTING ePHR IMPLEMENTATION

Dr Lara Khoury
Associate Professor
Faculty of Law, McGill University

Ms Frédérique Horwood
BSocSc (Ottawa), BCL/LLB candidate
Faculty of Law, McGill University

Dr Marie-Pierre Gagnon
Associate Professor
Faculté des sciences infirmières, Laval University

UNIVERSITÉ LAVAL

McGill

TABLE OF CONTENTS

List of Figures

List of Acronyms

AHS: Alberta Health Services
AMRC: Academy of Medical Royal Colleges
CHI: Canada Health Infoway
CHIS: Child Health Information Systems
CMA: Canadian Medical Association
CMPA: Canadian Medical Protective Association
DOH: Department of Health (United Kingdom)
ePCHR: Electronic Personal Child Health Record
ePHR: Electronic Personal Health Record
EHR: Electronic Health Record
IT: Information Technology
NHS: National Health Service (United Kingdom)
OMA: Ontario Medical Association
OPCC: Office of the Privacy Commissioner of Canada

Notes to Readers

This report is the result of research undertaken as part of the project *Defining Policies that will Facilitate the Implementation and Use of Personal Health Records: An Interprovincial and International Comparative Approach* (Principal investigator: Dr Marie-Pierre Gagnon) funded by a grant from the Canadian Institutes of Health Research (201209HIC-298617-HRA-CFBA-111141).

This report is based on data collected between December 2013 and 31 March 2014.

The authors wish to thank Mrs Julie Payne-Gagnon, M.A., for her assistance in the preparation of this report.

Cover page design by Lysanne Larose.

Main Messages

ePHR Implementation Concerns in Legal Litterature and Public Policies

- The legal literature and public policy documents analyzed express a variety of concerns that may affect the implementation of ePHR in Canada.

- Concerns of a legal nature centre mainly on:
    - The need for cohesion and interoperability
    - Privacy and confidentiality
    - Data quality
    - Control over the information and its use
    - Security
    - Impact on the relationship between patients and healthcare professionals, and on the obligations and liability of healthcare actors.

ePHR-Specific Laws and Public Policies

- Although solutions are rarely offered, the above concerns are all discussed in the Canadian public policy documents pertaining expressly to ePHRs.

- Canadian law does not address these concerns in a satisfactory manner either given the current lack of provincial and federal statutes and regulations governing ePHRs.

- England's public policy documents offer a richer variety of methods and ideas to address ePHR implementation concerns and should provide inspiration when designing policies to facilitate ePHR implementation in Canada.

Canadian Laws and Public Policies on EHRs

- Given the absence of statutes or regulations applying directly to ePHRs in Canada, policy makers should draw inspiration from the rich legal normativity governing EHRs.

- Although rarely applicable to ePHRs controlled by patients, this normativity addresses several of the implementation concerns identified in this report in a manner that could be useful, with adaptations, to the ePHR context.

Other Relevant Legal Sources

- ePHR-related policies must take into account statutes, regulations and court decisions dealing more generally with concerns such as privacy, confidentiality, access, use and quality control of information in general and in non electronic health records.

Executive Summary

Introduction

- This report reviews Canadian laws and public policy relevant to Electronic Personal Health Records (ePHRs), and their implementation in Canada.

- It also includes a review of concerns expressed in English public policy regarding ePHR implementation.

- Given the dearth of legislative texts addressing ePHRs explicitly in Canada, this report also presents an overview of Canadian legislation and public policy dealing with Electronic Health Records (EHRs), as well as a summary of the underlying Canadian legal landscape that would inform ePHR implementation.

ePHR Implementation Concerns in Legal Litterature and Public Policies

- Concerns pertaining to implementation of Electronic Personal Health Records (ePHRs) are numerous and vary depending on the stakeholder.

- The concerns most often referred to in the legal and policy literature include: the need for cohesion and interoperability; privacy and confidentiality; data quality; the control over the information and its use, including secondary uses; electronic security issues; the impact on the relationship between patients and healthcare professionals, and on the obligations and liability of healthcare actors; the ownership and custody of the information; health inequalities, and electronic literacy and access.

ePHR-Specific Laws and Public Policies

- There are no provincial and federal statutes or regulations directly governing ePHRs controlled by patients in Canada at the moment.

- A few Canadian public and professional policies address ePHRs explicitly, discussing related concerns but rarely offering solutions. In this last respect, the public policy literature in England is much richer. There is thus a clear need for more guidance on ePHRs in Canada, for which the English experience could provide inspiration.

Canadian Laws and Public Policies on EHRs

- Electronic Health Records (EHRs) on the other hand are extensively regulated in Canada by legislation, regulation and public policy. These normative texts tend to apply to EHRs in the control or custody of public bodies, healthcare service providers, health professionals and bodies that provide information management services to these custodians, as well as persons acting on behalf of trustees and custodians.

- Although their direct applicability to the ePHR context is hence limited (depending on the type of ePHR envisaged), these norms offer inspiring tools to tackle concerns related to ePHR implementation, and should thus be considered when addressing ePHR implementation challenges.

Other Relevant Legal Sources

- Finally, Canadian law provides formal legal normativity (statutes, regulations and court decisions) with regard to privacy, confidentiality, access, use and quality control of information in general and in non electronic health records, which constitutes a relevant legal environment in which the development of ePHRs would take place.

- In addition, while not in a way specifically tailored to the ePHR context, many of these norms address concerns identified above directly. Thus, ePHR development must comply with these norms and be cognizant of the way these concerns are addressed.

Conclusion

- There is a clear need for policy guidance on appropriate ways to address concerns expressed in the legal and public policy literature in Canada with a view of ensuring the successful implementation of ePHRs in Canada. The current legal normativity in Canada concerns mostly EHRs and is, for the most part, inapplicable to ePHRs controlled by patients, although it does offer examples of how policy and law can facilitate such implementation. Many concerns expressed concerning ePHR implementation are however dealt with through general legal principles that constitute a legal environment of relevance to such implementation.

INTRODUCTION

This report was prepared as part of the research project entitled "*Defining Policies that will Facilitate the Implementation and Use of Personal Health Records: An Interprovincial and International Comparative Approach"* (Dr Marie-Pierre Gagnon, Principal Investigator). It aims to provide an overview of Canadian legal and public policy relevant to ePHR implementation. In a comparative vein, it also looks to concerns expressed in English public policy regarding ePHRs.

The relevant data was collected from December 2013 to 31 March 2014. Public policy documents were identified using web browsers and by visiting Canadian and British governmental websites. Legal literature, including legislation and regulations, was collected using legal databases such as Quicklaw, Westlaw, and the Canadian Legal Information Institute's website.

In Section 1, we report on concerns expressed in legal literature as well as in Canadian public policy documents regarding ePHR implementation. Sections 2 and 3 review public policy documents dealing expressly with ePHRs in Canada and in England. Given the dearth of legislative texts addressing ePHRs explicitly in Canada, Section 4 looks to Canadian legislation and public policy dealing with EHRs for inspiration in addressing the ePHR-related concerns identified in Section 1. Finally, Section 5 provides a brief overview of the underlying Canadian legal landscape relevant to the most oft-cited concerns in the context of ePHR implementation.

1. ePHR IMPLEMENTATION CONCERNS IN LEGAL LITTERATURE AND PUBLIC POLICIES

This section reports on the different concerns expressed in Canadian legal and public policy documents with regard to factors that may facilitate or impede implementation of ePHRs. Only the legal and public policy literature dealing specifically with ePHRs – or having immediate relevance for ePHRs - was studied for the purpose of this analysis, which is further limited to concerns of a legal or public policy nature.

Perspectives on ePHR implementation vary according to the stakeholder. For instance, healthcare professionals worry about how ePHRs will affect data accuracy, their professional liability, reliance on information, and the safeguarding of information. They are also concerned about how the electronic interface will affect the doctor-patient relationship (in that it may create more distance between doctor and patient), and about ownership of information. Government and institutional stakeholders are eager to get patients more involved in their healthcare and more informed, as they view ePHRs as a way to reduce strains on the health care system (remote healthcare, healthcare communications etc.). Finally, patients view ePHRs favourably for the most part. They desire greater access to their records and to their physicians (through online communication for example). They also want access to more information about their health condition and/or treatment. Indeed, the potential for empowering patients, as well as for improving trust and communication, is seen as one of the advantages of ePHR development (Pagliari *et al.* 2007, 331). However, patients are concerned with the privacy/confidentiality of their personal information and with their ability to control its use, collection, and disclosure.

In the sections below, we comment briefly on some of the main legal concerns raised in the literature consulted. These can be illustrated in the following manner:

FIGURE 1 – SUMMARY OF CONCERNS OF A LEGAL NATURE

General	•Need for policies to incentivize use •Need for pan-Canadian policy or regulatory frameworks (cohesion) •Need for interoperability
Privacy and Confidentiality	•Information hosted on multiple computers and servers •Dependence on security of systems •Vulnerability to human error •Danger of privacy invasions by third parties or family members •Concerns about privacy of family members' health information
Data Quality	•Accuracy •Ability to safely rely on the information (physician's perspective) •Correction of information entered by others, *e.g.* healthcare providers •Role of physician in monitoring information in record
Control and Use of Information	•Control over who accesses record and purpose of use •Need for user trails •Importance of access by healthcare professionals •Secondary uses (for insurance, research, quality assurance, or commercial purposes) •Managing patient's consent
Security	•Back-up, audit trails, encryption, recovery systems, passwords •Security of patient-physician communication via email or other electronic means
Relationship and Responsibility	•Impact on patient-physician relationship •Need for clarity as to physician's role and responsibility •Physician's new duties, for *e.g.* to educate and support patients •Effect on physician's liability
Other Concerns	•Ownership/custody of information •Intellectual property aspects •Health inequalities / electronic literacy and access •Concerns specific to mental health information

1.1. General Concerns

First and foremost, the need to develop policies to incentivize the use of ePHRs is noted by several sources (Pagliari *et al.* 2007, 332; Rozenblum *et al.* 2011, E287 in the context of EHRs). Regional differences have also brought about calls for pan-Canadian policy or regulatory frameworks for EHRs that could be relevant to ePHRs (see *e.g.* Goodman, 2012 generally and 27 & 30). In the context of EHRs, authors have argued that the Canadian regulatory framework operates in a piecemeal fashion under multiple federal and provincial statutes (Goodman, 20). However, as Goodman observes in the context of EHRs, complete interoperability in Canada would require bilateral and multilateral agreements due to the constitutional division of power (2012, 51). In England, concerns for interoperability are also stressed emphatically, which is understandable given that this country has moved away from the idea of a top-down national IT strategy or programme in favour of one that is locally controlled (NHS Future Forum, 5, 18, 20).

1.2. Confidentiality and Privacy

One of the most preoccupying issues with regard to the confidentiality of health information found in electronic records flows from the fact that records are likely to be stored on multiple computers and servers, thereby making privacy dependent on the security of these systems as well as subject to human error (D'Agostino & Woodward 2010, 138). Canadian family physicians have expressed concerns about potential hacking of the information contained in ePHRs (Yau *et al.* 2011, e181). In 2009, the Office of the Privacy Commissioner of Canada (OPCC), while viewing the development of ePHRs favourably, called on both private and public sector developers to make sure privacy laws were respected and ePHRs complied with the highest privacy standards (OPCC, 2009). Authors also noted the danger of privacy invasions from family members – for instance parents wanting to have access to their older children's information - and difficulties in controlling this type of privacy breach (Pagliari *et al.* 2007, 331; Yau *et al.* 2011, e181). Nonetheless, Archer at al. (2011) report that although two thirds of adult consumers are concerned about the privacy and security of their information, those using ePHRs are not worried about privacy implications (2011, 517).

Some authors also raise the issue of how the privacy of family members – whose information may be collected to complete a given patient's family health history and to establish their risk factors – may be affected (CHI, 2007, v). Moreover, in England, authors have voiced concerns regarding the collection of mental and sexual health data, noting that some patients might want to keep certain types of information off the central NHS record (Pagliari *et al.* 2007, 331). For their part, healthcare providers who access records to obtain the information they need to provide care are concerned about the privacy of their own information. In particular, they maintain that data collected on record users should be limited to the needs of identity management and should not be used for monitoring practice patterns (CHI, 2007, vi).

1.3. Access to Data and Quality of Data

General - Commenting on the pan-Canadian Health Infoway project, Canada Health Infoway (CHI) stresses the need for a shift in culture from a disclosure-based data protection model to an access-based model "where healthcare providers access the information they require to fulfill the purposes" (CHI 2007, v).

Control of access – Concerns about patients' control of the access to their electronic health records is obviously expressed more emphatically in the context of EHRs where patients have less control over their health information than with ePHRs (*e.g.*, CMPA Handbook 2009, 7[1]). Indeed, some authors argue that control of access will be better with ePHRs than with traditional health records given that the patient controls the data (Williams and Weber-Jahnke 2010, 248), and that these systems can include mechanisms that record all attempts to access the records (Gibson 2003, 655 in the context of EHRs). But even in the context of ePHRs, the question of "how" access can be controlled by the patient is raised.

[1] The CMPA is a not-for-profit defense organization for Canadian physicians. However, given they represent a large majority of physicians in Canada and because of their status, we have included documents emanating from them although they don't qualify as "public policy", in the sense of policies originating from public entities.

Access by healthcare professionals – The importance of not letting information governance rules impede access to patients' records by healthcare professionals in patients' best interest is often stressed in England. There has been concern in this country that the current data governance legal framework impedes data sharing in the patient's interest (this concern drove England to commission a Review, the Caldicott Review, which was published in 2013) (NHS Future Forum, 6, 22-23; Caldicott 2013, 25, 28-29).

Data quality and integrity - Potential inaccuracy of data controlled by patients is a concern that comes up repeatedly in the literature, although some believe that ePHRs have the potential of improving record accuracy (Pagliari *et al.* 2007, 331). The Canadian Medical Protective Association (CMPA) expressed worries – in the context of EHRs - that multiple health professionals who are not consulting each other may rely upon the information (assuming they are granted access by the patient in the context of ePHRs), in which case the importance of accuracy is enhanced (CMPA, Data Sharing 2008, 7). Potential lack of consistency in how the data is recorded is also raised as a consideration (Wellington 2010, 2).

In addition, concerns are expressed regarding the value of the information should patients be allowed to modify entries such as lab results or prescription histories. Some sources advise that patient input should be limited to providing additional insight, for instance regarding habits or symptoms (Alberta Health Services, 22-23). While the issue of patients' right to have their health information corrected is clearly a concern with EHRs (*e.g.,* CMPA Handbook 2009, 9), it appears more secondary in the context of ePHRs given the patient has more direct control over the information. However, given that other persons can often participate to entering information into the ePHR, including healthcare providers, the issue of how requests by patients to have the information corrected can be accommodated is equally relevant in this context.

Finally, the Ontario Medical Association (OMA) takes the position that physicians should not be expected to play a role in managing or monitoring this type of record if they are not integrated in an EHR (OMA 2013, 16). Indeed, the issue of guardianship is raised from the physicians' perspective, for instance by family physicians who believe physicians lose guardianship of the medical information under the ePHR model (Yau *et al.* 2011, e181).

Secondary uses - Many worry about the management of the sharing of information contained in ePHRs or EHRs with others for purposes other than providing healthcare (“outside the circle of care”). For example, information contained in ePHRs could be of interest for research purposes, for quality assurance review, or for commercial purposes (Gibson 2003, 649). The need to circumscribe these secondary uses is raised principally in the EHR context (Gibson 2003, 650 & 663), but is similarly applicable to the ePHR context. In particular, the CMPA stresses the necessity of obtaining patients’ consent before any secondary use, as well as ensuring these secondary uses do not breach provincial laws (CMPA Handbook, 2009, 1, 6). Other questions include whether patients should be informed of secondary uses and what level of de-identification is needed “before personal health information that was collected for the purpose of treatment and care can be fairly and ethically used for research without requiring patient consent” (CHI, 2007, v).

1.4. Doctor-Patient Relationship

Archer *et al.* report that patients feel that access to online medical records helps reinforce the trust and confidence in doctors, and that they were more like partners in their healthcare (2011, 518). Nevertheless, concerns expressed by physicians revolve around the need for the development of electronic records not to impede the open exchange of information and trust that exists between patients and physicians (OMA 2013, 3-5, 9; Yau *et al.* 2011, e183). However, in England, the NHS Future Forum noted recently that concerns about the impact of electronic records use (not ePHRs) on doctor-patient relationships have not been actualized in the context of GP practices where such records have been in wide use for many years (15).

The OMA also stresses the need to educate patients so they can have a clear understanding of their choice should they decide to access laboratory results directly (OMA 2013, 17). Indeed, physicians worry that patients may not be able to understand the medical information added to their record and might experience anxiety as a result, although research has found that anxiety does not seem to be an issue for patients in this context (Yau *et al.* 2011, e181, 183; NHS Future Forum, 5, 16). Canadian physicians raise the need to provide support to patients to make sure they can interpret the information they receive through ePHRs (Yau *et al.* 2011, e181, 183). They also express concerns about giving psychiatric patients access to their medical record given the sensitivity of the information that it may contain (Yau *et al.* 2011, e182-83).

1.5. Security

Security is an oft-raised concern with both EHRs and ePHRs in Canada (CMPA Handbook 2009, 1, 8) as in England where a number of breaches of data protection laws has been documented (NHS Future Forum, 21; Caldicott 2013, 11, 49). Alberta Health Services note that patients will not be comfortable using ePHRs unless they feel security measures are adequate (AHS, 22). Therefore, they state that systems operators must ensure strict security measures (AHS, 22). Sources mention more specifically the necessity of back-up requirements, audit trails, encryption, recovery systems, and use of passwords (CMPA Handbook 2009, 1, 4-5). They also insist on ensuring the need for security of communications between physicians and patients through email or other electronic means (CMPA Handbook 2009, 1, 8).

1.6. Accountability and Professional Liability

Given how complex electronic systems can be, CHI raises the need to ensure that accountability remains clear (CHI 2007, iv). In addition, Canadian physicians worry that they currently lack clarity with regards to physicians' role and responsibilities with respect to ePHRs, and guardianship of the patient's data (Yau *et al.* 2011, e182). A survey of Canadian family physicians indicates that they believe that, in the context of ePHRs, they do not have guardianship of the information and are hence no longer responsible for it (Yau *et al.* 2011, e181). Indeed, authors observe that individual physicians lose an element of control they have traditionally enjoyed over, for example, the disclosure of medical information (Griener 2005, 15, in the context of EHRs).

Finally, an important concern from the physician's perspective relates to the necessity of exercising caution before relying exclusively on the information contained in ePHRs (Yau *et al.* 2011, e181). Moreover, the CMPA warns against physicians considering that information entered into an ePHR replaces their own record-keeping obligations and their own individualized assessment of a patient (CMPA Handbook 2009, 19).

1.7. Other

Other legal concerns not discussed here relate to questions of ownership of the information. In addition, Pagliari *et al.* note that there is a risk of creating health inequalities resulting from access disparities to electronic resources in the population (for *e.g.* resulting from poor technical skills in the elderly) (Pagliari *et al.* 2007, 332).

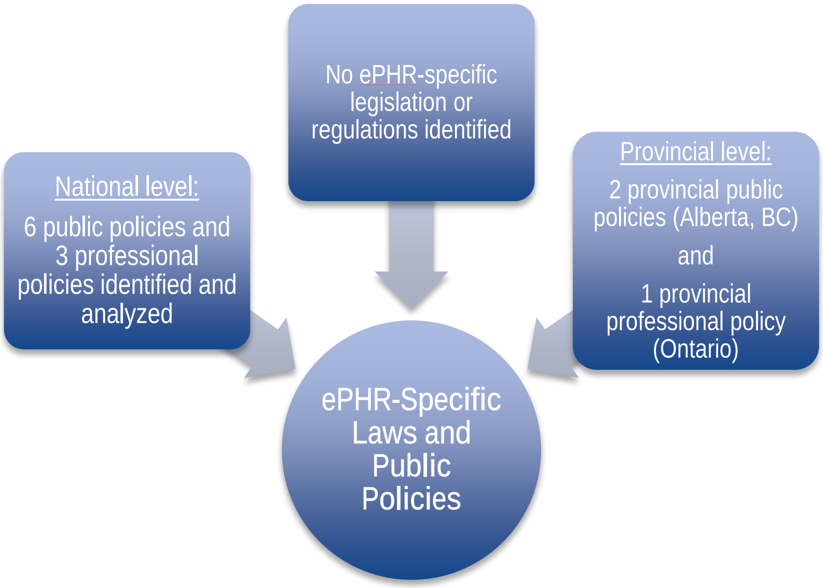
2. ePHR-SPECIFIC LAWS AND PUBLIC POLICIES – CANADA

2.1. Summary of Findings

Our analysis first dealt with ePHR-specific normativity, limited to legislation and public policy documents pertaining specifically to ePHRs in Canada. For our purposes, “public policy” was defined as policy documents emanating from public entities. However, because of the dearth of ePHR-specific public policies in Canada, we also included in our analysis, policies emanating from professional health associations of importance, such as the Canadian Medical Association (CMA).

Legal and policy sources devoted specifically to ePHRs in Canada are very limited as Figure 2 demonstrates.

FIGURE 2 – CANADIAN ePHR-SPECIFIC LAWS AND POLICIES ANALYZED



No ePHR-specific legislation or regulations identified

National level:
6 public policies and 3 professional policies identified and analyzed

Provincial level:
2 provincial public policies (Alberta, BC)
and
1 provincial professional policy (Ontario)

ePHR-Specific Laws and Public Policies

The list of policy documents analyzed can be found in Appendix A. Of note is the fact that we have not identified any statutes dealing specifically with ePHRs. This confirms the need for comprehensive policy guidance directed specifically at ePHRs in Canada. Indeed, one may legitimately wonder whether existing legal and policy norms surrounding EHRs are sufficient to tackle the governance of ePHRs, as analyzed in Section 3 of this report. Finally, some of the preoccupations raised with regard to ePHRs in Canada's policy documents are already addressed to some extent by existing laws and policies dealing with privacy, data access, confidentiality, etc. Section 4 deals with this last issue.

Each ePHR-specific policy was analyzed with the view of identifying particular issues they raise with regard to implementation of ePHRs, as well as their suggested approach to respond to these concerns. While Canadian policy documents specifically dealing with ePHRs discuss all of the typical concerns regarding implementation and make general recommendations or express desired outcomes, they rarely provide detailed solutions or guidelines as to how these concerns should be addressed. Still, some documents provide more complete guidance. CHI's *White Paper on Information Governance of the Interoperable Electronic Health Record* is one of them, although it is focused predominantly on EHR systems. The 2009 Resolution of Canada's Privacy Commissioners and Privacy Enforcement Officials is another interesting example, dealing specifically with patients' control over their health records. Finally, the OMA makes specific recommendations regarding physicians' roles and responsibilities. Notwithstanding, our overall impression flowing from the review of ePHR-specific policies in Canada is that there is a need for more precise and detailed policy guidelines for ePHR implementation.

2.2. Implementation Concerns and Canadian Policies on ePHRs

This section reviews briefly how different Canadian policy documents address the concerns identified in Section 1 with regard to ePHR implementation. The policy documents analysed are listed in Table 1 found at Appendix A. However, these policies are not all specific to ePHRs as demonstrated in Table 2 of Appendix A.

2.2.1. National Policies

Building on Values: The Future of Health Care in Canada, Romanow Report, 2002, pp. 76 - The Romanow report recommends that every Canadian have an ePHR, ready access and ownership over their personal health information, with clear privacy protection, as well as ready access to credible information on health care and the health care system.

Consumer Health Application and *Consumer Health Platform Certification*, Canada Health Infoway - Requirements for certification for "consumer health applications" and "consumer health platforms" related to privacy include: accountability; transparency; data safeguards; compliance; consent; limiting use, retention and disclosure; identifying purposes; and limiting collection.

Electronic Records Handbook: Implementing and Using Electronic Medical Records (EMRs) and Electronic Health Records (EHRs), Canadian Medical Protective Association, 2009 - This document includes calls for caution from practitioners when relying on information contained in an ePHR or a patient portal. It also affirms that in no way can these records replace a physician assessment of the patient. In terms of secondary uses, it stresses the necessity to obtain consent (EHR-specific) (1, 6). It also details requirements to ensure security of the platform (EHR-specific), including: encryption (1, 8), audit trails (1, 8), back up (1, 8), security of communications via email or other e-means (1, 8, 14), and recovery systems (4). Finally, it deals with the possibility of determining who enters information or corrections and when (10) (EHR specific).

Electronic Health Records: An overview of Federal and Provincial Audit Reports, Auditor General of Canada, 2010 (section on ePHR at page 11) - Addresses the need for compatibility with existing EHRs.

White Paper on Information Governance of the Interoperable Electronic Health Record (EHR), Canada Health Infoway, March 2007 (Focuses mainly on CHI, but many aspects relevant to ePHRs) - The White paper's section that is particularly relevant to the ePHR context insists on the fact that accountability and custodial responsibilities should be clearly assigned (iv). It addresses concerns related to privacy and confidentiality by suggesting: notices to the patient (iv), limits to the collection of information (v), dealing with families' privacy (v), risk management (v), and identity theft (vi). It also suggests audit trails (iv). Finally, it discusses the privacy of users (vi) and communities (vi-vii).

In terms of access to the information, the White Paper suggests locking away the data and means of controlling access (v, vi). It also deals with the issue of consent (v) and suggests a move to an access-based model (away from the traditional disclosure-based model) (v). The concerns regarding secondary uses are also discussed (v), including the necessity to inform the patient (v) and to de-identify the information (v). Finally, the White paper addresses requests for correction by patients (v) and the issue of compliance (v-vi).

The Promise of Personal Health Records, Resolution of Canada's Privacy Commissioners and Privacy Enforcement Officials, September 9-10, 2009, St-John's, Newfoundland - This document deals particularly with patient's control over their health records. It states that patients should have access to their record, see who accesses it, be able to choose who is allowed or not to view their information, be able to express how they want this information to be used, if at all, for health research purposes, receive notices of privacy and security breaches, request corrections, and have access to oversight offices for questions and complaints. In terms of secondary use, the OPCC recommends that patients should be able to express their wishes for how their health information is used by researchers. Finally, the resolution also recommends that patients be able to request that errors in their record be corrected.

2.2.2.Alberta

Engaging the Patient in Healthcare: An Overview of Personal Health Records Systems and Implications for Alberta, Alberta Health Services, undated - The AHS expresses the desire that systems operators ensure strict security for transfer, storage, and access of data (22). It also stresses that patients should not be able to modify information such as laboratory results and prescription histories (22). Finally, it recommends that patients' input be limited to providing additional insight (*e.g.*, about habits, symptoms) (22). Of note is the fact that the *Freedom of Information and Protection of Privacy Act* does not allow health information to be located outside of Canada (22).

2.2.3. Ontario

Ontario Medical Association, eHealth Policy Paper, September 2013, p 15-16 - Addressing access and quality of data, the OMA discusses the possibility for patients to mask information, to use lockboxes, and the need to inform patients about consequences of doing so on their healthcare (10) (EHR-specific). Moreover, they advise that physicians should play no role in managing or monitoring ePHRs if they are not integrated in an EHR (16).

The OMA views ePHRs favourably, but not as a stand-alone record. It would like to see the ePHR as a type of patient portal within the provincial EHR where patients would be more of a passive viewer of their information, as uploaded into the record by health care providers. The OMA notes the risk of medical information being misunderstood by patients. The OMA states that while the patients should have the opportunity to keep their own record, it would be too great a burden to expect physicians to play a role in monitoring this record.

Although the OMA deals with the issue of privacy, it makes no particular recommendations in this regard (4, 16). With regard to security, it advises proper technical safeguards for online communications (11-12) but makes no particular recommendations on other security issues (20).

3. ePHR-RELEVANT LAWS AND PUBLIC POLICIES – ENGLAND

3.1. Summary of Findings

As was the case for Canadian sources, we were not able to identify any English legislation dealing specifically with ePHRs. Public policy documents pertaining specifically to ePHRs are also in limited number, although there have been more extensive discussions by public bodies in England of the role informational technologies play in the delivery of healthcare and in record keeping than is the case in Canada. Conversely, policies do similarly address the full range of concerns identified in the literature (Section 1).

Likewise, public policy documents, while they stress particular concerns and make general recommendations, do not always provide detailed guidance as to how concerns should be resolved. Exceptions include *Standards for an Electronic Personal Child Health Record (ePCHR).* This document is very explicit with regard to ownership of, access to, and quality of children's records. It also explicitly makes recommendations in the context of secondary use of ePCHRs. The document *Output-Based Specifications for Child Health Information Systems* similarly provides explicit recommendations on a wide number of issues. This gives the impression that the managing of electronic children health and personal health records has attracted particular attention from policy makers. The *myhealthlocker End User Privacy Statement* is also very informative in how one may tackle issues related to security, confidentiality, secondary uses, patient information and staff training. Finally, *Information: to share or not to share? The Information Governance Review* (2013) is one of the best public policy we have come across although it is not specifically focused on ePHRs. It is exhaustively reviewed below. A few other policies interestingly address, and sometimes with great detail, many of the concerns relevant to ePHR implementation, but were not drafted to apply specifically to this type of record. However, given they often include in their assessment EHRs with patient access, they provide interesting inspiration for the ePHR context[2]. Overall, the few English policies that target ePHRs specifically tend to be more detail-oriented and developed than what we have in Canada. Appendix A lists English public policies fully (Table 3) and indicates whether they pertain specifically to ePHRs or not (Table 4).

3.2. Implementation Concerns and England's Policies Relevant to ePHR

This section reviews briefly how different policy documents from England address the concerns identified in Section 1 with regard to implementation.

Information: to share or not to share? The Information Governance Review, F. Caldicott, March 2013 - This document is very detailed not only with regard to its discussion of legal concerns regarding electronic health information, but also in making explicit recommendations as to how these concerns should be handled. However, it is not focused on ePHRs, but on health information in general. Still, it assumes this information is on electronic support for the most part, although in the control of health delivering entities.

[2] For the purpose of this Report, and although views may vary on the topic, we have not considered EHRs with patient access as qualifying as ePHRs given that the control of those records lies primarily in the hands of the medical practitioner or institution.

It is one of the best public policy documents we have come across in our research and can serve as a source of inspiration for policy design on issues of a legal nature. The document recognizes a series of rights that apply to both the patient and healthcare professionals: right to access personal records, right to privacy and confidentiality, right to be informed as to how the information will be used, right to request that the confidential data is not used beyond one's own care and treatment (13, 59-60). In addition, the following elements warrant particular note:

- Confidentiality: Recommends audit trails available in suitable form to patients (9-10; also: 13) and the sharing of information by email only when patients' consent explicitly and have been informed of potential risks (30). Communications between different care team members should be copied to the patient or user (30). The document also deals with access of children records (17, 93-94) and access to "family records" (17, 95). It stresses the need for a common approach to sharing information for children and young people given their information may need to be shared beyond the normal boundaries of health and social care services, for *e.g.* to schools (17, 96). The document also recommends that health and social care organizations be required to publish a declaration describing what personal confidential data it discloses, to whom, and for what purpose (19). It states that every proposed use or transfer of personal confidential data should be clearly defined, scrutinized, and documented with continuing uses regularly reviewed by an appropriate guardian (20). Consent to share information with third parties should be respected and documented (42). The Review also touches on respect of third party confidentiality (42-44), as well as the obligation to inform patients of any breach, to explain, and to apologize (46). It stresses the need to comply with existing laws (55).
- Right to access: Insisted on strongly given the document deals with healthcare provider controlled records (10, 13, 23, 27ff). It also underlines the need for clarity (18).
- Implied consent: Must depend on patients' knowledge as to how their data will be used (26).
- Right to use: Right of professionals to receive and share information about a patient to optimize patient care based on the principle of "implied consent" as is generally the case (11-12, 35-39, 56), unless the patient has objected (35); limited only to relevant information transmitted to professionals with a legitimate relationship with the patient (37-39). The risk of not sharing the information should be explained to patients although their wish should be respected (40). See also 20-21.

- Secondary uses: Need to explain to patients and the public how the personal information collected could be used in de-identified form for research and other purposes, also mentioning the right to refuse to give consent to such uses (12-13, 57). Consent can be changed at any time (13, 58). Need to make refusal or withdrawals of explicit consent traceable and communicated to others involved in the patient's care (13). Also stresses that the NHS and adult social services should commit to de-identifying the data used for research or care improvement purposes (13, 630). Explains how to deal with grey areas (63-66, 69). Underlines that consent is required before identifiable information is disclosed for research purposes (62). Also see: 14, 66-68 ("safe havens"); 15-16 (public health); and 23.
- Support to patient: Need to adopt international record content data standards (32) and to promote health literacy through education in schools and universities (32).
- Training: The Review discusses staff training in information governance and the presence of information governance staff (16, 89-92).
- Responding to breaches and responsibility: Suggests the use of a standard severity scale (12, 54) and stresses the need to clarify responsibilities for breaches of confidentiality when the information has been shared (47). When shared for care on the basis of implied consent, the document states that responsibility lies with the recipient (47).
- Security: 19. Need for passwords, smart cards and security locks, as well as audit trails (32-33). Need for a straightforward means to identify and authenticate anyone who has had access (33).

Standards for an Electronic Personal Child Health Record (ePCHR), 2013 *(unknown source)* - This document deals with equity issues by stressing how ePHRs should not increase inequalities in access to information or in health outcomes. It takes the stand that the ownership of the record is granted to parents/guardians, or the child when older (4.1.1) and that access is to be granted to parents, children, and those with parental responsibility (not defined) (4.2.3). It recommends a record of successful and unsuccessful access be maintained (audit trail) (4.2.4). In terms of data quality, it underlines that parents/those with parental responsibility and clinicians can update the record (4.4.1). Dates of entries by healthcare professionals cannot be edited or deleted, but requests can be made for correction (4.4.2). The document also addresses secondary uses: use of identifiable information must be approved by parents/child (4.5.1) while use of non-identifiable data must conform to a policy agreed to in advance (4.5.1). The sale of information to commercial organizations is forbidden 4.5.2).

How are you?, Cambridge Healthcare, 2013 *(Not a public body but included here as the platform was initially developed with the former NHS East of England)* - This is more of a publicity-information document. However, it interestingly stresses how patients can choose what information is shared, with whom, and how this setting can be tailored for each individual panel (14).

Output-Based Specifications for Child Health Information Systems, Child Health Information Systems Transition Steering Group, DOH, October 2012 *(Document applies to CHIS operated at local level)* - This document lists the types of secondary uses for which CHIS can be used (15). It addresses access by stressing that the CHIS should permit access by parents, carers and young people (17). It deals with control of who should have access (17, 107-08) and the fact that access is determined at a local level (107). It also discusses audit trails (18, 111) and the possibility to disable access (19, 107). Confidentiality and security are also extensively discussed, including the issues of: remote access (19, 108); access control system (19); encryption (19, 108); consent with regard to core data (32), logs of message transmissions (108), and message notifications (108). It also discusses general principles with regard to security (105) and encryption standards (105). With regard to data quality, the document stresses the possibility of corrections (19) and the necessity for data within the CHIS system to have an identified author and custodian (112).

The Power of Information: Putting all of us in control of the health and care information we need, Department of Health, 21 May 2012 - This document stresses the need for clear direction from the Government (2) and for different systems to communicate with each other (2, 43) (the Government opts for a decentralized approach to electronic record keeping (11, 64, 75, 77)). Given the document is championing the use of IT in healthcare delivery and record keeping, it tends to focus on the benefits of this approach, rather than concerns with implementation. It does touch on a number of issues from a general perspective: the need for confidentiality and for guidance as to who can and should have access to records is mentioned briefly, as is the preoccupation with protecting vulnerable members of the community from abuse that could occur if others access their records inappropriately (19, 25, 27, 84, 102). It also briefly mentions the need for support in accessing online records (25). Other issues are mentioned very briefly: security and protection of email communications (45), responsibility (73), consent to sharing information (84). The secondary use of aggregated and de-identified information from electronic records for research, public health and quality assurance purposes is discussed in a positive manner(35-37, 87, 102).

Myhealthlocker End User Privacy Statement, 13 Dec 2011 - This short document explains how specific concerns are tackled in the context of this particular electronic record (ePHR under the South London and Maudsley NHS Foundation Trust):

- Security: Security is the responsibility of the recipient of the information (1). The statement prohibits staff from storing personal identifiable information on local hard disks, pen drives, or other portable media. Limits storage to network drives with password-protected files (4).
- Confidentiality: Use or transmission for any purpose other than that for which it was requested is prohibited (1).
- Secondary use: User browsing actions and patterns are collected but in an aggregate and de-identified way (1). Specifies that the data is not shared with other organizations, unless permitted by law, and is not sold (2). Advises that researchers with a contractual agreement with the Trust may want to use clinical information to conduct scientific projects to improve care and treatment (3). Also informs that the Trust may use the information for quality assurance purposes (3).
- Patient's information: When data is collected, the patient is notified as to why it is requested and how the information will be used. Patients have the right to refuse (1-2).
- Staff training: Regarding confidentiality (2).

Liberating the NHS – An Information Revolution. A summary of consultation responses, Department of Health, August 2011 - This document is not solely focused on ePHRs, but many of the concerns it raises have general value and are relevant to the ePHR context. It mentions the concerns related to confidentiality and security (21, 25). It also calls for clear governance and consent models to ensure a balance between accessibility and data security (11). The document also emphasises concerns as to how recorded information can be abused by third parties, such as violent partners, employers, family members or insurers (20). In addition, the need for face-to-face contact with care professionals is stressed briefly (12). Finally, concerns over equity and the need to provide support to some patients in accessing and using information are also mentioned, insisting that those with greater health needs are those with the least access to technology (11-12).

The need to link the information across health, social care and public health is also stressed (11, 15).

HealthSpace Implementation Guidance for Registration Offices – Web Version v4.4, D. Corbett, 23 February 2011 - This is a guidance document for implementation of HealthSpace (shut down in December 2012). With relevance to confidentiality concerns, it gives detailed guidance on vouching for patients' identity and avoiding repeat applications (pp. 14-22).

The Care Record Guarantee. Our Guarantee for NHS Care Records in England, NHS, January 2011 (v5) - This document does not apply to ePHRs as such but rather to EHRs to which patients are given access. It contains a series of commitments:

- Privacy and confidentiality: Stresses that the patient holds the rights to privacy and confidentiality, and their importance (1), and indicates situations in which health information that identifies patients may be disclosed as well as the need to respect existing laws (2, 4, 6). Otherwise, it commits to asking for consent (7). It additionally deals with training of staff about their obligations (8). Access and consent with regard to children's records are explained but guidance is specific to English law. The approach proposed is interesting for the Canadian context however as it is based on communication (10-11).
- Right to access: 1, 4; It insists on the provision of information in a format that is accessible to the patient (3, 4).
- Access by healthcare providers: Mentions information sharing with people who provide care or to check quality unless the patient prohibits it (4), the disclosure of information only to those with a right to see it (8) and the possibility to seal portions of the record and the need for patients to understand the possible effects of this option (14).
- Data quality: Discusses accuracy, opportunity for patient to check record, to point out mistakes, and to add comments about record keeping (7).
- Security: Discusses record of access (8) and investigation in case of inappropriate access, as well as provision to the patient of report of findings and actions to be taken (8). Details different ways of ensuring security of access: smartcards, recording permission to access, access control – *i.e.,* access depends on employment - audit trails, restricting parts of record that can be seen (13-14).

Liberating the NHS – An Information Revolution, Academy of Medical Royal Colleges, January 2011 - This is a response to the consultation paper “An Information Revolution” and is therefore not restricted to ePHRs. This position paper focuses predominantly on the necessity to ensure data quality. For the AMRC, increased patient choice depends on high quality information (1). It stresses that this is particularly important to ensure engagement by clinicians: “[w]hen users feel that they are merely ‘feeding the beast’ of information collecting, it is unsurprising that the quality of data of (sic) is poor. The Academy endorses the view that accuracy of data is the bedrock of meaningful information” (2). Interestingly, the Academy states that much of the responsibility for the quality of data must lie with clinicians (2). The Academy also states that it is crucial that there is clarity over the purpose for which information is required (2). It also supports the principle of patients having *access and control* over their records, but stresses that this does not mean they will be able to remove the original record from the care provider or alter or delete what a clinician or care professional has entered into the record unless it is incorrect (3). The AMRC also stresses the need for *inter-operability* of systems: “[i]t must be a requirement on new providers entering any part of the market that the information they provide and the systems that they operate must be compatible with the rest of the NHS” (1).

Information. A report from the NHS Future Forum, undated (probably 2011) - This document is also very detailed as to the handling of some of the key legal issues identified as concerns for implementation of ePHRs. However, it is not focused on ePHRs as such, but rather more generally on electronic health records that patients should be able to access and contribute to. Still, it contains useful recommendations for the ePHR context, such as with regard to:

- Consent: The putting into place of a proper consent process for use of the patient’s information (5).
- Interoperability: Need for a system that allows full electronic data sharing against set standards and without opt-out possibilities (5, 20). Need for national data standards for the structure and content of health records (18, 20).
- Information governance: Need to find an appropriate balance between the protection of patient information and the use and sharing of information to improve patient care (6).

- Access: Recognition of patients' right to access their health information (11-12, 14, 23) with a corresponding responsibility to allow the use of data for patients' care and for improving services to others (23).
- Support to patients: Put in place appropriate structures to assist patients in understanding their information and knowing how to use it (16-17)
- Secondary uses: Allowing as a default position the use of aggregated de-identified data in the interest of clinical audits, research, and wider quality improvement efforts (17). Having a rigorous and transparent information governance practice ensuring that identifiable data is used only where absolutely necessary (17, 24-25).

Enabling Patients to Access Electronic Health Records, Royal College of General Practitioners, v1.0, Sept 2010 - This document deals only with access by patients of records held and controlled by healthcare entities and, consequently, does not address the issue of ePHRs although it applies to a situation where equal access by patient and clinician is envisaged (3). We include it as it develops interesting and transferrable ideas particularly with regard to access to information contained in the record:

- Confidentiality: Of third party providing data (13-14).
- Access by patients: Stresses its importance (vi) and the possibility of withholding of information only in exceptional cases allowed by existing laws (vi). Mentions that patients should be informed of the benefits and risks of accessing their record and of giving access to third parties (8). Access to children's records is detailed but is very dependent on existing British laws (15).
- Access by third parties: Reviews legal rules in this regard (5).
- Data quality: Reports that access by patients improves the accuracy of the record (4, 10, 17). Stresses the need to handle patient-added data with care and not to assume accuracy (18).
- Support to patients: Need for the patient to understand the information: need to link it with targeted health information and decision support (3-4) and for the language to be accessible while accepting that technical language will have to be used (9). Need for the professional to screen results that are frightening or difficult to interpret and to explain potential risks of accessing this information prior to screening (11). Raises concerns with giving access to mental health data, but insists on the need not to discriminate against those patients (14). Leaflets and systems should include advice to patients on security (12).

- Security: (vi). Technical control, audit trails, human and process elements such as assigning responsibilities (7).
- Responsibility: Stresses the absence of evidence of increased litigation (3). Need for patients to understand that when they share their information, they bear the responsibility (7-8, 12). Need for robust on-line registration and authentication methods (7). Health professionals could be held accountable if they rely on patient-added information without making their own clinical assessment (18). Additions should not be treated as a proxy for a medical assessment (18). Necessity to indicate clearly in the record the origin of the information where it is added by the patient (18).
- Training: 8, 19
- Other: Need for legal guidance to protect vulnerable individuals (4, 12-13, 15).

Liberating the NHS – An Information Revolution. A consultation on proposals, Department of Health, October 2010 - This is a consultation document that touches on a range of concerns relevant to ePHRs and contains a section on patient-centered records. It insists on the principle "no decision about me, without me". Concerns raised – but only discussed briefly as this is a document calling for opinions from other stakeholders - are linked to: patients' control over their care and their health records (5, 16-17); confidentiality and privacy (6); data quality (8); interoperability of systems in place (5, 55); use for research purposes (18, 38); need to assist patients with access to the record (36), and equity (44-45).

The case and vision for patient focused records, Academy of Medical Royal Colleges, May 2010 - Insists that the information recorded be accessible whatever the setting or context. Moreover, the information should be completely interoperable and the approach should be adopted across the NHS.

Records Management: NHS Code of Practice, Part 1, Department of Health (UK), March 2006 *(Applies to EHR, emails, text messages: pp.1-2. Applies to all types of NHS records, including records of NHS patients treated on behalf of the NHS in the private healthcare sector) – Replaces HSC 1999/053, 1998/217, 1998/153* - This document deals mostly with NHS Records but appears to include those controlled by patients, although this is unclear. It discusses the Secondary Use

Service (SUS) (public) in charge of protecting patient confidentiality (38). It also states that relevant statutory provisions and guidance documents dealing generally with disclosure should be respected (14). In terms of accountability, it identifies responsibilities and assigns them to appropriate actors in addition to stressing the need for all NHS organizations to establish a policy statement (9-10). Finally, it reviews all relevant United Kingdom legislation, directives, guidelines, and professional codes of conduct. These do not deal specifically with ePHRs or EHRs, but still govern their use (42-89).

4. CANADIAN LAWS AND PUBLIC POLICIES ON EHRs

Given the absence of legislation on ePHRs within Canada and England, this section shifts its focus to normativity relevant to EHRs. It thus aims to provide a preliminary survey of the current legal environment for EHRs in Canada, as well as to identify existing norms that could be directly or indirectly relevant to future policy development for ePHRs. The analysis was limited to legislation and public policy documents pertaining to EHRs in Canada. "Public Policy" was defined in the same way as the sections above, *i.e.* as policy documents of a normative nature emanating from public entities with the addition of policies produced by the CMA, the CMPA, and professional regulatory bodies. All the laws and policies analyzed for this section are listed at Appendix B.

4.1. Types of Documents Analyzed

At the Federal level, much of the available legal and policy literature on EHR creation, management, and governance consists of guidance provided by Canada Health Infoway, a public body funded jointly by the provincial, territorial, and federal governments. Documents stemming from the CMA and CMPA provide guidance to physicians on appropriate conduct and compliance with new legal requirements within the EHR context. At the provincial/territorial level, the legislation surveyed regulates EHRs in separate enactments, as well as specifically and implicitly[3] within personal health information protection legislation. As for provincial policies, documents analysed tend to fall into two broad categories: (i) guidance from professional regulatory bodies on

[3] Implicitly means the legislation may apply to EHRs directly, but contains no specific treatment of EHRs *as opposed to* other records containing personal health information.

appropriate conduct and compliance with new legal requirements within the EHR context; (ii) policy documents and reports issued by provincial Departments of Health (or a body created by them) discussing EHRs in the context of the strategic vision for provincial healthcare and/or specific pilot projects.

4.2. Direct Applicability to ePHRs

The legislation reviewed, whether it addresses EHRs explicitly or not, is designed for information in the control or custody of information "trustees" or "custodians". These have varying definitions, but tend to be limited across the board to public bodies, health care service providers, health professionals, and bodies that provide information management services to these custodians as well as persons acting on behalf of trustees and custodians. Insofar as ePHRs are distinguishable from EHRs precisely by a certain level of control or participation of patients in providing and/or managing their information, this policy design choice appears to preclude direct application of EHR legislation to ePHRs. Nonetheless, the lines are blurred by the fact that in provinces that are envisioning future ePHR projects (Alberta for example), the bodies regulated as custodians under provincial legislation are the same bodies tasked with creating/managing these future ePHRs. Thus, if an ePHR is in the partial custody or control of a public body, EHR legislation could be applicable. However, application to ePHRs is further frustrated where the enactments specify that the regulated information must be used, collected, or disclosed for the purpose of providing health care. Unless monitoring one's own health and/or a family member's health and inputting this information is considered "providing health care", this condition creates another barrier to direct application of the enactments to the ePHR context. Because they stem from governmental or regulatory bodies responding to legislative developments, the policy documents analysed are also drafted within the same paradigm that posits the health care provider and the government as data custodians.

4.3. Inspiration for ePHR Policy Development

Laws and policies pertaining to EHR cover a wide range of issues and concerns. We mention briefly here the different concerns they tackle that are relevant to the ePHR context. A list of these laws and policy documents can be found in Appendix B. Figure 3 first illustrates the data collected and analyzed.

FIGURE 3 – LAWS AND POLICIES ON EHRs

LAWS/REGULATIONS	PUBLIC POLICIES	PROFESSIONAL POLICIES
•None at the federal level	•11 at the federal level	•7 selected at the pan-canadian level
•31 at the provincial level *Alberta: 3; BC: 2; Man: 3; NB: 2; NS: 4; Nfld&Lab: 3; Ont: 4; PEI: 1; Qc: 4; Sask: 3; Yuk: 1; NT: 1*	•14 at the provincial level *Alberta: 1; BC: 2; Man: 3; NS: 2; Ont: 1; PEI: 2; Qc: 2; Sask: 1*	•5 selected at the provincial level

Goodman (2012, 53) underlines that there are three legislative models for EHRs in Canada: (1) provinces that have legislation specific only to the EHR environment (British Columbia and Quebec); (2) provinces that have personal data protection laws that treat EHR specifically within the context of health-specific personal data protection legislation (Alberta, New Brunswick, Newfoundland & Labrador, Ontario, Manitoba and implied in Saskatchewan); (3) territories and provinces in which EHRs are not addressed and only personal data protection legislation exists (Nova Scotia, Prince-Edward-Island, Northwest Territories, Nunavut and Yukon). One must exercise caution when referring to these norms as they are inextricable from the foundational arrangement of these enactments, where personal health information is conceived of as being both controlled and protected by government and health care providers. Indeed, the duties imposed through these norms are tied to the custodian's role within the healthcare system and within society in general. These actors (professionals and/or government bodies) are already inherently accountable to their patients and/or those they provide services to (and in this case collect information from). New duties are simply added to this pre-existing accountability. As a result, the concerns listed above are drafted in a manner unresponsive to two fundamental shifts in the ePHR context: 1) the patient-physician/patient-government (as a health service provider) relationship, especially with regards to data stewardship; 2) patient participation in information management.

Traditionally, physicians (and, by extension, the government in its role as a health service provider) were the primary guardians of medical information and were accountable for its protection.

This paradigm is reflected in the legislation of EHRs. However, in an ePHR environment, the patient has at least some level of control or custody over the record containing their information, i.e. the government and/or professionals are no longer the sole data stewards. Furthermore, the patients can often input information directly into their own record. At the same time, patients have neither special knowledge nor statutory or ethical obligations towards other citizens and/or healthcare professionals and the government. In this way, new ways to impose and attribute responsibility for the many obligations (*e.g.,* to implement security safeguards appropriate for managing electronic records, to limit collection, use and disclosure of information, to respect consent directives, to store, retain and destroy the information securely, to ensure the accuracy of data, to notify other people who use the information of any changes to the information, etc.) must be developed. This shift in duty distribution will necessarily imply adjustments to the complaints and dispute resolution process as well. Nonetheless, these responsibilities are already shared between various health care professionals in any given circle of care and between custodians and private entities who provide services to them. The way in which the norms regulating EHRs respond to this reality provides relevant ideas for managing shared responsibilities in an ePHR context. Although the detailed and very similar requirements across jurisdictions provide useful guidance as to the adequate protection of personal health information held in electronic records, these would need to be re-conceptualized in order to properly regulate the new relationships created by ePHRs. A number of relevant concerns are tackled in the legislation relevant to EHRs. We list them here briefly, without however providing a detailed analysis of the legislative treatment of these issues.

<u>Privacy and Confidentiality</u>: Relevant aspects of the legislation and policy treatment of privacy and confidentiality include recommendations for audit trails and user activity; authorized collection, use, and disclosure; information sharing agreements; consent; balancing privacy and access; privacy of healthcare provider's info; access by third parties; and, minors' records.

<u>Control and Use of Information:</u> With regard to the control and use of the information, the different documents studied provide useful tools to deal with: consent to access and use; user access management, for *e.g.* role-based access, access restrictions; disclosure obligations; masking, lock-boxing, consent overrides; and, secondary use, for *e.g.:* de-identification, consent.

Data Quality: The concern related to the quality of the data presents itself quite distinctly in the context of ePHRs compared to that of EHRs where worries tend to centre on the possibility for patients to request corrections to their record, and to receive notifications of corrections and changes.

Security: Many issues related to the security of EHRs overlap with those pertinent to the ePHR context. Thus, precautionary measures imposed for EHRs can be of great value for ePHR-related policy. The most useful tend to relate to: physical and electronic security safeguards; login, encryption, passwords, security keys, fraud detection software, security audits; back up, storage, retention and destruction; duty to notify and alerts; secure messaging; and, policies in cases of security breach, investigation process, responses to breach.

Liability and Accountability: Concerns from the medical profession about its liability are less acute in the EHR context than in the ePHR one. Still, concerns about accuracy of the information and the ability to rely on it are addressed in a way that could be relevant to the ePHR context.

Other Issues: Other issues of relevance to the ePHR context include interoperability, trans-jurisdictional issues, public's education, ownership of data, and the storing of data outside Canada.

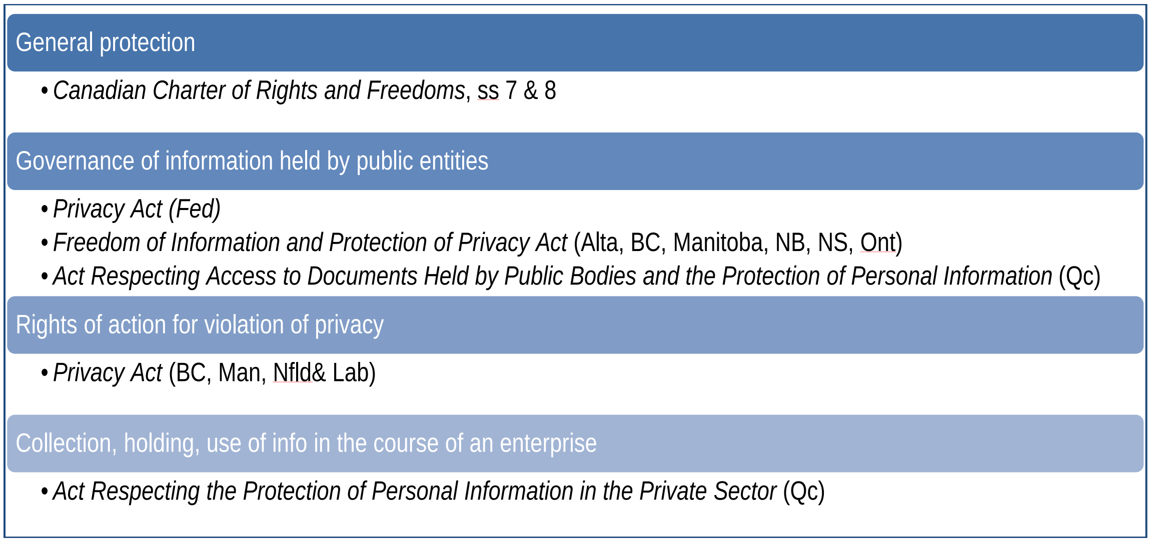
5. OTHER RELEVANT LEGAL SOURCES ON IMPLEMENTATION CONCERNS

An array of provincial and federal legislation is relevant to the regulation of several of the concerns identified regarding implementation of ePHRs in Canada. The most important concerns are amply legislated on, but given that they tend to fall under provincial jurisdiction, there is a lack of uniformity across Canada. Calls for harmonization are numerous (for *e.g.,* D'Agostino & Woodward 2010, 140). The purpose of this report is not to provide an exhaustive list of the laws that may have a direct or indirect impact on ePHR implementation - we have collected more than 150 relevant laws and regulations between December 2013 and March 2014 -, but rather to attract the reader's attention to the importance of the existing legal normativity within which this implementation will occur. In pursuit of this objective, the section below is limited to general observations accompanied by examples of the formal legal normativity (statutes and regulations) pertaining to privacy, confidentiality, access, use and quality control of information in general, as well as to non-electronic health records and information.

5.1. Privacy

Privacy is a well-recognized general legal principle, protected by the Canadian constitution, the Quebec Charter of Rights and Freedoms, and the Civil Code of Quebec. Several federal and provincial statutes and regulations deal with privacy obligations. However, many of the legislative or regulatory texts collected do not apply in the context of privately controlled records. Courts have also stated and defined the principle in many decisions. In addition, some provinces have established a statutory tort of invasion of privacy. Although the details of how privacy may be protected in the particular context of ePHRs could be the object of more precise policy, there is ample legislative guidance and protection in Canada on the general principle at this time. However, the operability of this principle and how privacy may be protected in practice in the particular context of ePHRs is a matter on which policies might be needed. Figure 4 provides statutory examples on the issue of privacy.

FIGURE 4 – STATUTORY EXAMPLES – PRIVACY



General protection

- *Canadian Charter of Rights and Freedoms*, ss 7 & 8

Governance of information held by public entities

- *Privacy Act (Fed)*
- *Freedom of Information and Protection of Privacy Act* (Alta, BC, Manitoba, NB, NS, Ont)
- *Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information* (Qc)

Rights of action for violation of privacy

- *Privacy Act* (BC, Man, Nfld& Lab)

Collection, holding, use of info in the course of an enterprise

- *Act Respecting the Protection of Personal Information in the Private Sector* (Qc)

5.2. Confidentiality

The confidential nature of health information and records is a well-recognized legal principle, with regulated exceptions (research, public health, consent, danger to the public, child protection, etc.). Several federal and provincial statutes and regulations, as well as case law, state relevant confidentiality obligations, such as those applicable to commercial providers of ePHRs or to professionals who use health information. Confidentiality is unlikely to be in issue as far as healthcare professionals are concerned. Their confidentiality obligation is recognized by the common law, by the Civil Code of Quebec, by Canadian human rights legislation, and by specific statutes. However, the question of how this confidentiality will be protected in practice can be the object of more in depth discussion in the context of ePHRs. Figure 5 provides statutory examples on the subject of confidentiality (also see Privacy Table above as privacy and confidentiality are often dealt with together).

FIGURE 5 – STATUTORY EXAMPLES – CONFIDENTIALITY (Next page)

General

- *Quebec Charter of Human Rights and Freedoms,* s. 9 (applies to the State and private entities and persons)

Information collected, used, disclosed, by “Organizations” (e.g., commercial)

- *Personal Information and Electronic Documents Act* (Fed)
- *Personal Information Protection Act* (Alta, BC)

Governance of information technology

- *An Act to Establish a Legal Framework for Information Technology (Qc)*

Confidentiality with regard to children information

- *Disclosure of Information Regulation* (Alta)
- *Child Care Regulations* (Sask), *Child Protection Act* (PEI), *Children and Youth Care and Protection Act* Nfld&Lab); *Child and Family Services Act* (Yukon)

Protection of adults

- *Decision-Making Support and Protection to Adults Act (Yukon)*

Mental health information

- *Mental Health* Act (Man, PEI, Yukon)
- *Mental Health Services Act* (Sask)

Confidentiality obligations of healthcare institutions

- *Home Care and Community Services Act, Nursing Homes Act, Long-Term Care Homes Act* (Ont)
- *An Act respecting Health Services and Social Services* (Qc)
- *Hospital Act* (PEI)
- *Health Act* (Yukon)

Professional Codes of ethics and obligations

- Quebec Codes of Ethics (physicians, nurses, pharmacists, etc.), which are all in legislative form
- *Medical Act* (PEI); *Medical Professions Act* (Yukon)

Confidentiality and disclosure in the context of public health

- *Public Health Act* (BC, Qc, PEI) and *Health Protection and Promotion Act* (Ont)

5.3. Access, Use and Quality Control of Data

Legislation dealing with health information often regulates access, use, and quality control. For instance, the Ontario *Personal Health Information Protection Act* allows individuals to request access to their personal information held by health information custodians operating within the province and applies to both paper and electronic records (D’Agostino and Woodward 2010).

Access to information (in general, not restricted to health) has also been the object of legislation in Canada and legislation dealing with privacy also touches on access and use of the information. In terms of applicability of this legislation, it turns on who the custodian of the information contained in an ePHR is. Many statutes deal with access to information held by public bodies, however, for *e.g.*: *Access to Information Act* (Federal); *Freedom of Information and Protection of Privacy Laws* and regulations (Alberta, British Columbia, Ontario, Saskatchewan, Manitoba, Nova Scotia, Prince-Edward-Island,…); *An Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information* (Quebec). Some personal information statutes deal with access and correction of information held by private entities, for *e.g.*: *Personal Information Protection Act* (British Columbia, Alberta) or *An Act Respecting the Protection of Personal Information in the Private Sector* (Quebec). Of course, where the custodian is the patient himself or herself, issues of access to the information are likely to be moot.

5.4. Health Records and Health Information Governance

Provincial legislation also deals with collection, use, disclosure, and retention of personal health information by healthcare providers (D'Agostino & Woodward 2010). Even prior to the development of health records held in electronic format, healthcare records had been the object of legislation. To the extent that this legislation deals with electronic forms of health records, it has been dealt with above. Governance of records in general in this legislation might be relevant to the ePHR context, but direct applicability is doubtful to the extent that the patient is the custodian or has control of the record.

5.5. Miscellaneous

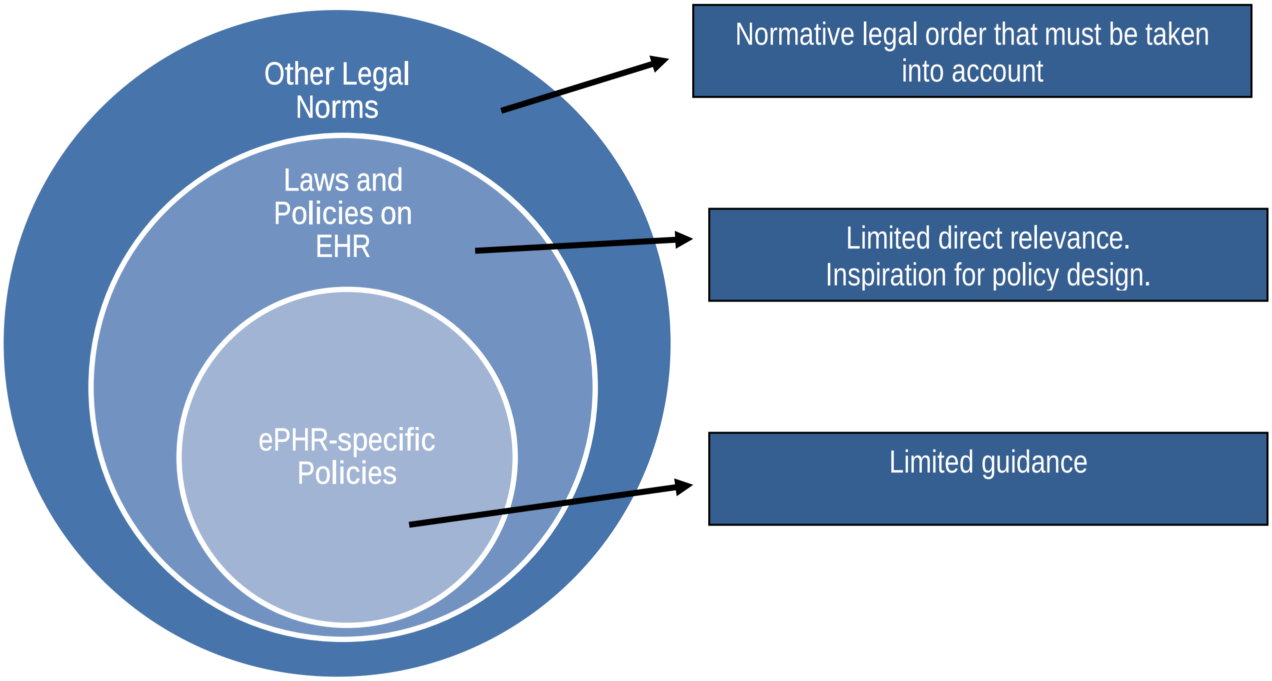
Other general norms are relevant to the tackling of ePHR implementation concerns, most notably civil liability and professional liability rules, as well as intellectual property.

CONCLUSIONS

- Clear concerns are expressed in the legal and policy literature with regard to implementation of ePHRs.
- There is very limited policy guidance on implementation of ePHRs.
- Laws, regulations and policies regarding EHRs are a clear source of inspiration for policy design with regard to ePHRs but would need to be reconceptualised in this context.
- Legal norms dealing more generally with confidentiality, privacy, access, use and quality control of data, health information, liability, etc. must be taken into account when devising policy.

Figure 6 provides a visual summary of this report.

FIGURE 6 – PORTRAIT OF LEGAL NORMS RELEVANT TO ePHR IMPLEMENTATION


Other Legal Norms
Laws and Policies on EHR
ePHR-specific Policies
Normative legal order that must be taken into account
Limited direct relevance. Inspiration for policy design.
Limited guidance

REFERENCES

Articles

1. N. Archer et al., “Personal Health Records: A Scoping Review” (2011) 18 J Am Med Inform Assoc 515-522.

2. G. D’Agostino and D.A. Woodward, “Diagnosing Our Health Records in the Digital World: Towards a Legal Governance Model for the Electronic Health Record in Canada” (2010) 22 Intellectual Property Journal 127.

3. Elaine Gibson, “Jewel in the Crown?* The Romanow Commission Proposal to Develop a National Electronic Health Record System” (2003) 66 Sask. L. Rev. 647-665.

4. Patricia Goodman, Electronic Health Record Regulation in Canada: What the Patient Experience Reveals about the Pursuit of Legislative Harmonization, Master of Laws Thesis, University of Western Ontario, 2012.

5. Glenn Griener, “Electronic Health Records as a Threat to Privacy” (2005)14:1 Health Law Review 14-17.

6. Claudia Pagliari, Don Detmer and Peter Singleton, “Potential of Electronic Personal Health Records” (2007) 335 BMJ 330.

7. Ronen Rozenblum et al., “A Qualitative Study of Canada’s Experience with the Implementation of Electronic Health Information Technology” (2011) 183: 5 CMAJ E281.

8. Waterloo Wellington Local Health Integration Network (LIHN), Key findings from the HeC Benefits Evaluation Report, November 2010.

9. J. Williams and J.H. Weber-Jahnke, “The Regulation of Personal Health Records Systems in Canada” (2010) 8:2 Canadian Journal of Law and Technology 241.

10. GL Yau, AS Williams and JB Brown, “Family Physicians’ Perspectives on Personal Health Records” (2011) 57 Canadian Family Physician e178-84.

Canadian Public/Professional Policies

1. Building on Values: The Future of Health Care in Canada, Romanow Report (2002) http://www.cbc.ca/healthcare/final_report.pdf

2. Consumer Health Application and Consumer Health Platform Certification, Canada Health Infoway. https://www.infoway-inforoute.ca/index.php/programs-services/certification-services/what-infoway-certifies/consumer-health-application https://www.infoway-inforoute.ca/index.php/programs-services/certification-services/what-infoway-certifies/consumer-health-platform

3. *Data Sharing Principles for Electronic Medical Records/Electronic Health Records Agreements*, CMA (2008)

4. Electronic Records Handbook: Implementing and Using Electronic Medical Records (EMRs) and Electronic Health Records (EHRs), CMPA (2009)
https://www.cmpa-acpm.ca/documents/10179/24937/com_electronic_records_handbook-e.pdf

5. Electronic Health Records: An overview of Federal and Provincial Audit Reports, Auditor General of Canada (2010)
http://www.oag-bvg.gc.ca/internet/English/parl_oag_201004_07_e_33720.html

6. Engaging the Patient in Healthcare: An Overview of Personal Health Records Systems and Implications for Alberta, Alberta Health Services, undated
http://www.albertahealthservices.ca/org/ahs-org-ehr.pdf

7. Ontario Medical Association, eHealth Policy Paper (2013)
https://www.oma.org/Resources/Documents/eHealthPolicy092013.pdf

8. The Promise of Personal Health Records, Office of the Privacy Commissioner of Canada (2009)
https://www.priv.gc.ca/media/nr-c/2009/res_090910_eh_e.asp

9. White Paper on Information Governance of the Interoperable Electronic Health Record (EHR), CHI (2007)
https://www.infoway-inforoute.ca/index.php/component/docman/doc_download/75-information-governance-of-the-interoperable-ehr

Public/Professional Policies - England

1. Enabling Patients to Access Electronic Health Records, Royal College of General Practitioners, v1.0 (2010)
http://www.rcgp.org.uk/Clinical-and-research/Practice-management-resources/~/media/Files/Informatics/Health_Informatics_Enabling_Patient_Access.ashx

2. HealthSpace Implementation Guidance for Registration Offices – Web Version v4.4, D. Corbett (2011)
http://www.connectingforhealth.nhs.uk/systemsandservices/healthspace/nhsorgs/offices.pdf

3. Information. A report from the NHS Future Forum, undated (probably 2011)
http://www.raceequalityfoundation.org.uk/future-forum/part2-information

4. Information: to share or not to share? The Information Governance Review (2013)
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/192572/2900774_InfoGovernance_accv2.pdf

5. Liberating the NHS – An Information Revolution. A summary of consultation responses, Department of Health (2011)
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/216664/dh_129580.pdf

6. Liberating the NHS – An Information Revolution, Academy of Medical Royal Colleges (2011)
http://www.aomrc.org.uk/doc_view/9323-academy-response-liberating-the-nhs-information-revolution

7. Liberating the NHS – An Information Revolution. A consultation on proposals, Department of Health (2010)

http://socialwelfare.bl.uk/subject-areas/services-activity/health-services/departmentofhealth/144668dh_120598.pdf

8. Myhealthlocker End User Privacy Statement (2011)
https://yp.slam.nhs.uk/Pages/PrivacyPolicy.aspx

9. Output-Based Specifications for Child Health Information Systems, CHIS Transition Steering Group, Department of Health (2012)
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/213072/201112-CHIS-OBS.pdf

10. Records Management: NHS Code of Practice, Part 1, Department of Health (2006)
http://systems.hscic.gov.uk/infogov/links/recordscop1.pdf

11. Standards for an Electronic Personal Child Health Record (ePCHR), 2013
http://www.rcpch.ac.uk/system/files/protected/page/ePCHR%20Standards%202013.pdf

12. The Care Record Guarantee. Our Guarantee for NHS Care Records in England, National Health Service (2011) (v 5)
http://www.mkhospital.nhs.uk/about-mkhft/data-protection-and-medical-records-requests/252-care-records-guarantee/file

13. The case and vision for patient focused records, Academy of Medical Royal Colleges (2010)
http://www.aomrc.org.uk/doc_download/217-academy-statement-the-case-and-vision-for-patient-focused-records

14. The Power of information: putting us all in control of the health and care information we need, Department of Health (2012)
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/213689/dh_134205.pdf

APPENDIX A

ePHR-RELEVANT POLICIES IN CANADA AND ENGLAND

TABLE 1 – ePHR-Specific Sources – Canada

ePHR SPECIFIC SOURCES - CANADA							
Public and professional policies	Privacy / Confiden-tiality	Access / Consent	Data quality	Security	Secon-dary uses	Dr-patient relation / Respon-sibility	Others
Canada							
Building on Values: The Future of Health Care in Canada, Romanow Report, 2002	X						
Consumer Health Application and *Consumer Health Platform Certification*, Canada Health Infoway.	X						
Electronic Records Handbook: Implementing and Using Electronic Medical Records (EMRs) and Electronic Health Records (EHRs), Canadian Medical Protective Association, 2009, p 19. (This is not a public policy per se as it emanates from the non-profit defence organization for Canadian physicians – See also under EHR)			X	X	X	X	
Consumer Health Application Certification, Canada Health Infoway	X						
Electronic Health Records: An overview of Federal and Provincial Audit Reports, Auditor General of Canada, 2010 (page 11)							Compatibility with EHR
Future Practice, CMA, June 2013 (Not a public policy but included as originates from CMA)							Informational / Clinical advantages.
White Paper on Information Governance of the Interoperable Electronic Health Record EHR), Canada Health Infoway, March 2007 Focuses mainly on Canada Health Infoway, but many aspects very relevant to ePHR	X	X	X		X	X	Compliance
"The Promise of Personal Health Records", Resolution of Canada's Privacy Commissioners and Privacy Enforcement Officials (Archived), September 9-10, 2009, St-John's, Nfld.	X		X	X	X		
Alberta							
Engaging the Patient in Healthcare: An Overview of Personal Health Records Systems and Implications for Alberta, Alberta Health Services, undated			X	X			
British-Columbia							
Health Sector Information Management/ Information Technology Strategy, Ministry of Health, Developed for the BC eHealth Strategy Council, January 2011 (Version 2.0)							No concerns mentioned
Ontario							
Ontario Medical Association, eHealth Policy Paper, September 2013, p 15-16	X	X	X	X			

TABLE 2 – Canadian Public/Professional Policies

Canadian Public/Professional Policies (Selection)	ePHR-specific?
Building on Values: The Future of Health Care in Canada, Romanow Report (2002)	No
Consumer Health Application and *Consumer Health Platform Certification*, Canada Health Infoway.	No
Electronic Records Handbook: Implementing and Using Electronic Medical Records (EMRs) and Electronic Health Records (EHRs), CMPA (2009)	One section
Electronic Health Records: An overview of Federal and Provincial Audit Reports, Auditor General of Canada (2010)	No
White Paper on Information Governance of the Interoperable Electronic Health Record (EHR), CHI (2007)	No
The Promise of Personal Health Records, Office of the Privacy Commissioner of Canada (2009)	No
Engaging the Patient in Healthcare: An Overview of Personal Health Records Systems and Implications for Alberta, Alberta Health Services, undated	YES
Health Sector Information Management/ Information Technology Strategy, BC Ministry of Health (2011)	No
Ontario Medical Association, eHealth Policy Paper (2013)	Sections on ePHR

TABLE 3 – ePHR-Specific Sources – England

ePHR SPECIFIC SOURCES – ENGLAND							
Legislation / Public policy / Prof policies	Privacy Conf.	Access Consent	Data Quality	Security	Sec. Uses	Dr-patient Rltsp / Respon-sibility	Others
Information: to share or not to share? The Information Governance Review, F. Caldicott, March 2013	X	X		X	X	X	Training Support to patients
Liberating the NHS – An Information Revolution. A consultation on proposals, Department of Health, October 2010	X	X	X		X		Interoperability Equity
Liberating the NHS – An Information Revolution. A summary of consultation responses, Department of Health, August 2011	X	X	X	X	X	X	Equity
Liberating the NHS – An Information Revolution, Academy of Medical Royal Colleges, January 2011		X	X		X	X	Interoperability Broad use
HealthSpace Implementation Guidance for Registration Offices – Web Version v4.4, D. Corbett, 23 Feb 2011	X						
Information. A report from the NHS Future Forum, 2011?		X			X		Interoperability Support to patients
Myhealthlocker End User Privacy Statement, 13 Dec 2011	X	X		X	X		Staff training
The Care Record Guarantee. Our Guarantee for NHS Care Records in England, NHS, Jan 2011 (v 5)	X	X	X	X			
The Power of information: putting us all in control of the health and care information we need, Department of Health (UK), 21 May 2012	X	X		X	X		Interoperability Vulnerability Responsibility
The case and vision for patient focused records, Academy of Medical Royal Colleges, May 2010		X					Interoperability Broad adoption
Records Management: NHS Code of Practice, Part 1, Department of Health (UK), March 2006 (Applies to EHR, emails, text messages: p.1-2. Probably excludes ePHR if not NHS-managed?) – replaces HSC 1999/053, 1998/217, 1998/153	X				X	X	
How are you?, Cambridge Healthcare, 2013 (Not a public body but platform initially developed with former NHS East of England so document included here) - *More of a publicity-information document*							Control of information by patients
Standards for an Electronic Personal Child Health Record (ePCHR), 2013 (source?)		X	X		X		Equity Ownership
Output-Based Specifications for Child Health Information Systems, Child Health Information Systems Transition Steering Group, DOH, October 2012 – Not clear if includes ePCHR. Document applies to CHIS operated at local level (? include ePCHR?)	X	X	X	X	X		
Enabling Patients to Access Electronic Health Records, Royal College of General Practitioners, v1.0, Sept 2010	X	X	X	X		X	Training Protection of vulnerable

ePHR SPECIFIC SOURCES – ENGLAND							
Legislation / Public policy / Prof policies	Privacy Conf.	Access Consent	Data Quality	Security	Sec. Uses	Dr-patient Rltsp / Respon-sibility	Others
Other sources *Open Data White Paper, Unleashing the potential*, HM Government, June 2012 – Not studied for now as does not specifically apply to health records. *Shared Electronic Patient Record (SEPR) system in primary care,* Royal College of General Practitioners, date? – Not found.							

TABLE 4 – Public/Professional Policies - England

Public/Professional Policies - England	ePHR-specific?
Information: to share or not to share? The Information Governance Review (2013)	No
Standards for an Electronic Personal Child Health Record (ePCHR), 2013	YES
The Power of information: putting us all in control of the health and care information we need, DOH (2012)	No
Output-Based Specifications for Child Health Information Systems, CHIS Transition Steering Group, DOH (2012)	No
Liberating the NHS – An Information Revolution. A summary of consultation responses, DOH (2011)	No
Liberating the NHS – An Information Revolution, Academy of Medical Royal Colleges (2011)	No
HealthSpace Implementation Guidance for Registration Offices – Web Version v4.4, D. Corbett (2011)	YES
Myhealthlocker End User Privacy Statement (2011)	YES
The Care Record Guarantee. Our Guarantee for NHS Care Records in England, NHS (2011) (v 5)	No
Liberating the NHS – An Information Revolution. A consultation on proposals, DOH (2010)	One section only
The case and vision for patient focused records, Academy of Medical Royal Colleges (2010)	No
Enabling Patients to Access Electronic Health Records, Royal College of General Practitioners, v1.0 (2010)	No
Records Management: NHS Code of Practice, Part 1, DOH (2006)	No

APPENDIX B
CANADIAN LAWS AND POLICIES CONTAINING SPECIFIC PROVISIONS APPLYING TO ELECTRONIC HEALTH RECORDS

TABLE 1 – Canadian Legislation Containing Specific Provisions Applying to EHR

Alberta
• *Health Information Act*, c H-5, RSA 2000, and regulations: o *Health Information Regulation*, Alta Reg 70/2001 o *Electronic Health Record Regulation*, Alta Reg 118/2010
British-Columbia
• *E-Health (Personal Health Information Access and Protection of Privacy) Act*, c 38, SBC 2008, and regulations: o *Disclosure Directive Regulation,* BC Reg 172/2009
Manitoba
• *Personal Health Information Act*, SM c P33.5, 1997 (as amended by *Personal Health Information Amendment Act,* c 41, SM 2008), and regulations: o *Personal Health Information Regulation,* Man Reg 245/97 o *Personal Health Information Regulation*, Man Reg 38/2010 amending Man Reg 245/97
New Brunswick
• *Personal Health Information Privacy and Access Act*, c P-7.05, SNB 2009, and regulations: o NB Reg 2010-112
Newfoundland and Labrador
• *Personal Health Information Act*, c P-7.01, SNL 2008, and regulations: o *Personal Health Information Regulations*, NL Reg 38/11 • *Centre for Health information Act*, c C-5.1, SNL 2004.
Northwest Territories
• Bill 4, *Health Information Act*, 5th sess, 17th Leg, Northwest Territories, 2013 (currently in standing committee after second reading).
Nova Scotia
• *Personal Health Information Act*, c 41, SNS 2010, as amended by c 31, SNS 2012, and regulations: o *Personal Health Information* Regulations, NS Reg 217/2012 as amended by NS Reg 249/2013 Other relevant regulations: o *Pharmacy Act and Regulations Definitions Regulations,* NS Reg 251/2013, under the *Pharmacy Act* o *Drug Information System Prescription Monitoring Regulations*, NS Reg 216/2013, under the *Prescription Monitoring Act*.
Ontario
• *Personal Health Information Act*, c 3 schedule A, SO 2004, and regulations: o O Reg 329/04 • Bill 78, *An Act to Amend certain Acts with respect to EHRs*, 2nd sess, 40th Leg, Ontario, 2013 (currently in second reading). Other relevant regulations: o *Physicians' Personal Information,* O Reg 54/11 under the *Health Insurance Act*.
Prince Edward Island

• *Health Information Act (received Royal assent on 14 May 2014 but not yet in force).* • *Pharmaceutical Information Act*, c P-5.2, RSPEI 1988.
Quebec
• *An Act Respecting Health Services and Social Services*, c S-4.2, RSQ, 1991 (See Part I) • Bill 59, *An Act Respecting the Sharing of Certain Health Information*, 2nd sess, 39th Leg, Quebec, CQLR c P-9.0001, 2012 (assented to and partially in force). Other relevant regulations and legislative texts: • Conditions de mise en œuvre de la deuxième phase du projet expérimental du Dossier de santé du Québec (2009) A Gaz II, page 3163. • *Règlement sur les autorisations d'accès et la durée d'utilisation des renseignements contenus dans une banque de renseignements de santé d'un domaine clinique : Loi concernant le partage de certains renseignements de santé* (chapitre P-9.0001, a. 70, 72, 110 et 121), (2013) A Gaz II, page 1929
Saskatchewan
• *Health Information Protection Act*, c H-0.021, SS 1999, as amended by c 25 SS 2003, and regulations: o *The Health Information Protection Regulations*, RRS Reg 1 (H-0.021/2005), as amended by Sask Reg 20/2007 and 28/2010. • *The Electronic Information and Documents Act*, c E-7.22, SS 2000
Yukon
• Bill 61, *Health Information Privacy and Management Act*, 1st sess, 33rd Leg, Yukon, 2013 (assented to but not in force).

TABLE 2 – Canadian Public and Professional Policies Dealing with EHR

National
• *A 'Conceptual' Privacy Impact Assessment (PIA) on Canada's Electronic Health Record Solution (EHRS): Blueprint Version 2*, Canada Health Infoway, 12 February 2008. • *An Overview of the Electronic Health Record Privacy and Security -Conceptual Architecture*, Canada Health Infoway, March 2006 • *Building on Values: The Future of Health Care in Canada—Final Report*, Romanow Report, Commission on the Future of Health Care in Canada, November 2002 • *CIHR Best Practices for Protecting Privacy in Health Research*, Canadian Institutes of Health Research, September 2005 • *Data Sharing Agreements: Principles for Electronic Medical Records/Electronic Health Records*, Canadian Medical Association, 2009 • *Data Sharing Principles for Electronic Medical Records/Electronic Health Records Agreement*s, Canadian Medical Association, Canadian Medical Protective Association, August 2008 • *Electronic Health Record (EHR) Privacy and Security Requirements* (Reviewed with Jurisdictions and Providers), Canada Health Infoway, February 2005. • *Electronic Health Records: A Medical Liability Perspective*, Canadian Medical Protective Association, August 2008. • *Electronic Health Records in Canada: An overview of Federal and Provincial Audit Reports*, Auditor General of Canada, April 2010. • *Electronic Records Handbook: Implementing and Using Electronic Medical Records (EMRs) and Electronic Health Records (EHRs)*, Canadian Medical Protective Association, 2009 • *Embedding Privacy into the Design of EHRs to Enable Multiple Functionalities – Win/Win*, Canada Health Infoway, Information and Privacy Commissioner of Ontario, 2 March 2012 • *Future Practice,* Canadian Medical Association, June 2013.

- *Guiding Principles for Physician Electronic Medical Records (EMR) Adoption in Ambulatory Clinical Practice*, Canadian Medical Association, 2008.
- *How can Canada achieve enhanced use of electronic medical records*, Canadian Medical Association, May 2014.
- *Principles for the Protection of Patients' Personal Health Information*, Canadian Medical Association, 2011
- *Privacy and EHR Information Flows in Canada: Common understandings of the Pan-Canadian Health Information Privacy Group*, Canada Health Infoway, 30 June 2010
- *The Relationship Between Electronic Health Records and Patient Safety: A Joint Report on Future Directions for Canada*, Integrated Centre for Care Advancement through Research, Canada Health Infoway, and Canadian Patient Safety Institute, 2007
- *White Paper on Information Governance of the Interoperable Electronic Health Record (EHR)*, Canada Health Infoway, March 2007.

Alberta

- *Health Information Act: Guidelines and Practices Manual*, Government of Alberta, Department of Health and Wellness, March 2011

British Columbia

- *BC eHealth Conceptual System Architecture*, BC eHealth Steering Committee, April 2005
- *Health Sector Information Management/ Information Technology Strategy*, Ministry of Health, developed for the BC eHealth Strategy Council (Version 2.0), January 2011.
- *Professional Standards and Guidelines*: *Electronic Medical Records*, College of Physicians and Surgeons of British Columbia, June 2013

Manitoba

- *Bridging General and Specialist Care—The Right Door, The First Team*, Health System Innovation, Manitoba Health, launched March 2008.
- EChart Manitoba, "What are the Benefits?", Connected Care, Manitoba eHealth <www.connectedcare.ca/echartmanitoba/mbWhatRBenefits.html> accessed 4 Feb 2014.
- Manitoba eHealth_hub, "About", <www.manitoba-ehealth.ca/eHealth_hub.html> accessed 4 Feb 2014
- «The Physician Medical Record», Guideline no 177, College of Physicians and Surgeons of Manitoba, March 2008.

Newfoundland and Labrador

- *Towards an Evaluation Framework for EHR initiatives: Final Report,* Doreen Neville and Stephen O'Reilly (et al), March 2004 (Not public policy per se but research team led by CEO of NFLD Centre for Health Information (public body in charge of implementing the provincial EHR) with many researchers also being key personnel of the Centre)

Nova Scotia

- *Guidelines for Medical Record-Keeping*, College of Physicians and Surgeons of Nova Scotia, June 2008.
- *The Renewal of Public Health in Nova Scotia: Building a Public Health System Meeting the Needs of Nova Scotians*, Mid-course Review Report, NS Department of Health and Wellness, February 2012
- "What We Do", Health Information Technology Services Nova Scotia (HITS-NS), < http://www.hits-ns.nshealth.ca/what-we-do/> accessed 4 Feb 2014.

Ontario

- "About Health Links", Archived Backgrounder, Ontario Ministry of Health and Long-Term Care, published December 6 2010, <news.ontario.ca/mohltc/en/2012/12/about-health-links.html> accessed 31 Jan 2014.
- *eHealth Policy Paper,* Ontario Medical Association, September 2013.

Prince Edward Island

- «Electronic Health Records (EHR)», Health PEI, <www.healthpei.ca/ehr> accessed 4 Feb 2014
- *Proposed Personal Health Information Legislation*, Consultation Paper, Ministry of Health and Wellness, PEI, December 2013 (consultation process open till March 2014) (*Note: now the Health Information Act 2014)*.

Quebec

- *Plan Stratégique 2010-2015*, Ministère de la santé et des services sociaux, 2010.

• *Politique sur les modalités d'accès et de rectification au Dossier de Santé Québec*, Ministère de la Santé et des Services Sociaux, Technologies de l’information, 2013. • *Record-Keeping by Physicians in Non-Hospital Settings*, Practice Guide, Collège des médecins du Québec, June 2013.
Saskatchewan
• *Annual Report 2012-2013 : Empowering Patients, Enabling Care*, eHealth Saskatchewan, July 2013.