Privacy & Security for Patient Portals

2012 GUIDELINES FOR THE PROTECTION OF HEALTH INFORMATION

SPECIAL EDITION

ASSOCIATION CANADIENNE D’INFORMATIQUE DE LA SANTÉ

COACH

CANADA’S HEALTH INFORMATICS ASSOCIATION
All rights reserved. No part of this publication may be reproduced or transmitted in any form, or by any means, electronic or mechanical, including photocopying, recording, or any information storage and retrieval system, without permission in writing from the publisher.

© 2012 COACH: Canada's Health Informatics Association
ISBN 978-0-9864898-9-1

National Office
250 Consumers Road
Suite 301
Toronto, Ontario
M2J 4V6

Tel 416-494-9324
Toll Free 1-888-253-8554
Email info@coachorg.com
Website www.coachorg.com

Produced in Canada
Contents

Acknowledgments ............................................................................................................. 5

Introduction ...................................................................................................................... 7
  Purpose and Scope ........................................................................................................ 7
  How This Guide Can Help ....................................................................................... 8
  Getting Started ............................................................................................................ 9

1. Privacy and Security in the Context of Healthcare ...... 11
  Privacy .......................................................................................................................... 11
  Information Security .................................................................................................. 12

  The Evolution of Patient Portals ................................................................................ 14
  Portal Architecture:
    Two Generic Approaches .......................................................................................... 15
    Three Architectural Models ..................................................................................... 17

3. Canadian Privacy Legislation ................................................................. 25
  General Principles ...................................................................................................... 25
  Common Challenges ................................................................................................... 26
  Legislative Variations by Jurisdiction ...................................................................... 27

4. Selecting a Patient Portal Model ......................................................... 35
  Considering the Basics ............................................................................................... 35
  Knowing the Target Audience .................................................................................. 36
  Understanding Your Responsibilities .......................................................................... 37

5. Risks and Controls ......................................................................................... 39
  Commonly Available Functionality ........................................................................... 40
  Privacy Guidelines for Commonly Available Functionality ......................................... 44
  View-Only Patient Personal Health Information ....................................................... 59
  Access and Enter Personal Health Data ..................................................................... 59
  Patient Care Plans: Putting the Focus on Patients ...................................................... 63
  View Scheduled Appointments ................................................................................ 66
  Financial Transactions ............................................................................................... 69
  General Health Information ....................................................................................... 72
  Manage Access and Consent ..................................................................................... 77
6. Setting Up Your Patient Portal ................................................ 83
   Clinical Considerations .............................................................. 83
   Technical Considerations ............................................................ 84
   Legal and Regulatory Considerations ........................................... 84
   Administrative Considerations ................................................... 85
   Operations .................................................................................. 86

Appendix A: The 10 Principles of the CSA Model Code ..........87
Appendix B: Resources and Links................................................ 89
Appendix C: User Agreements....................................................... 93
Appendix D: Information Sharing Agreements ......................... 95
Appendix E: Consent Forms.......................................................... 97
Appendix F: Glossary of Terms.................................................... 99
Acknowledgments

Producing *Guidelines* and reflecting the top practices in protection of health information requires many hours of dedicated volunteer and staff time. This is especially true when creating *Guidelines* on a leading-edge topic like patient portals.

On behalf of the COACH Board of Directors, and all users of *Guidelines*, I would like to thank the following volunteers and staff who contributed to the production of *Privacy and Security for Patient Portals: 2012 Guidelines for the Protection of Health Information Special Edition*. It would not have been possible without you!

**2012 Privacy and Security Expert Group**

Reza Alemy, MD, CPHIMS
Adam Bailey, BA, MA
Abigail Carter-Langford, CIPP/C, CISA
Susan McLaughlin, RN, MBA
Bob Huard, BCS/CPHIMS-CA
Dawn Lake
Marc LeBlanc, MSc, PEng
Jason Lin, CISA, CIPP/IT, CPHIMS-CA
Patrick Lo, CISSP
Greg Lypowy, MHI
Robert Martin, BSc Elec Eng
Leahann McElveen, CPHIMS-CA
Geoffrey Pille, CPHIMS-CA
Wendy Robillard, BScMH
Michael Wilson, MSc
Patient Portals Special Edition Reviewers

Elizabeth Bodnar
Jane Dargie, CRISC, CISSP
Selena Davis, MHI, PMP
Karen Waite, CIPP/C, CPHIMS-CA

A special thanks goes to Elaine Sawatsky, Privacy and Security Expert Group Chair, for her passion, leadership, and coordination of the contributors in preparing this year’s Special Edition.

I would like to also thank:

- Ruth Wilson, of West Coast Editorial Associates, for pulling the contributions together and ensuring we spoke with a unified voice.
- Alex Hennig, of ClearDesign, for preparing this publication as a user-friendly electronic product.
- COACH National Office Staff, including Serina Nghiem, Coordinator, Programs, and Alison Gardner, Director, Programs.
- COACH Privacy and Security Steering Committee members, for providing guidance and leadership.
- Alberta, Saskatchewan, Manitoba, and Newfoundland and Labrador Ministries of Health and eHealth agencies for their ongoing support and jurisdiction-wide use of Guidelines.

Don Newsham
Chief Executive Office
COACH: Canada’s Health Informatics Association
Introduction

Purpose and Scope

The purpose of this document is to provide privacy and information security guidelines for anyone involved in designing, implementing and managing a patient portal system. It is intended to help healthcare professionals and organizations that are considering or that have already introduced patient portals to their patient population. It is not meant for technical people involved in developing, maintaining or marketing a patient portal, and it does not contain vendor-specific information for currently available portal products.

A patient portal is a controlled and secure computerized pathway between a patient (wherever that person is located) and the personal health information (PHI) about that patient, which is held by health information custodians, stewards or trustees. With the emergence of these portals, specific privacy and information security issues have arisen that are distinct from other types of clinical information systems. To address these issues, this document presents an overview of different models of patient portals and information on how to select the best one.

The extent of privacy and security issues will vary depending on the portal system implemented. Currently there is a wide functional range of systems available, from the most simple, which are little more than electronic filing systems owned, stored and controlled by the individual, to the most complex, which would operate within a fully integrated pan-Canadian electronic health record (EHR). In the middle of this range is the type of patient portal that is integrated with locally available systems, such as a regional health authority’s patient record system.

These portals may be operated by a public body or by a private body on behalf of a public body, or they may be owned and operated by a private
enterprise such as a telecommunications organization. In each case the privacy and control issues will differ, depending on who holds the data on whose behalf.

Because there is a wide range of patient portals available, each with various levels of functionality, the risks are also wide ranging and varied. For example, there are risks associated with the various types of information collected, used and/or disclosed, such as:

- **Personal information**
- Personal health information
- Publicly available health and wellness education information
- Data on health professionals, staff and volunteers
- Information related to public health surveillance
- Data about the actions of users (e.g., who accessed which records)

Thus, while a portal can be very broad in concept, it can also be implemented with limited functionality—and those functions may change over the life of the product.

### How This Guide Can Help

This guide has been developed to benefit organizations of all sizes—from single-physician offices to large, complex enterprises. The specific benefits readers derive from the information provided here will depend on several factors:

- Their current understanding of information protection issues
- The maturity of the processes already in place
- The current policies their organization has for addressing information protection
- The portal model their organization plans to implement

Those **healthcare organizations** with established information privacy and security programs and a designated information **privacy officer** and **security officer** may find that they already have in place many of the fundamental information protection structures described here. These organizations can use this guide as a reference to identify gaps and enhance existing practices and safeguards, and as a tool to promote education and advance awareness across the organization and in their patient population.

On the other end of the spectrum are those healthcare organizations that are introducing new e-health technologies and patient portal functions...
and may need detailed information. These organizations will find this
guide to be an excellent starting point for learning and understanding the
value of risk assessment, especially in the environment of participative care
that patient portals support. In this case, this guide will provide a basis
for developing organizational capacity, safeguards, processes and policies,
which can then be built on by researching further, using the suggested
resources listed in Appendix B.

All healthcare organizations and professionals, whether or not they are
experienced in privacy and security issues, will benefit from the up-to-date
information on safeguarding privacy in the Canadian healthcare context.

Getting Started

Because this guide has been developed for organizations at all stages of
implementing a patient portal system, it will be helpful to familiarize your-
self with the content and map out which sections are relevant to your situ-
ation. Begin by skimming the entire document to understand its approach
and structure. Next, read Section 1 in detail if the concept of privacy in
the context of healthcare is new to you. Section 2 then presents a useful
overview of patient portals, from which you can determine where your or-
ganization sits on the portal developmental scale. Section 3 covers the dif-
ferences in legislation among the various Canadian jurisdictions, and Sec-
tion 4 provides guidance on selecting the best portal for your organization.

The detailed guidelines on risks and controls make up the bulk of this
document and are presented in Section 5. That is followed by guidance on
how to set up a portal (Section 6). Finally, the appendices provide useful
information for further study, when needed.
Privacy and Security in the Context of Healthcare

Before an organization can effectively apply privacy and security controls for patient portals, it should have a good understanding of the primary privacy principles governing healthcare today.

Privacy protection and fair information practices are described in the 10 principles of the Canadian Standards Association (CSA) Model Code for the Protection of Personal Information (see Appendix A). These principles are included in the federal Personal Information Protection and Electronic Documents Act (PIPEDA) and are also addressed with some variation in all provincial privacy legislation. The CSA Model Code is recognized as the foundation for all privacy protection legislation in Canada, which in turn is based on an internationally accepted set of similar principles. It is, therefore, strongly recommended that organizations refer to and apply the Model Code when developing policy and procedures. If organizations consistently apply the Model Code principles, they can be confident that they will meet all generally applicable requirements.

Privacy

Healthcare practice supports the sharing of relevant health information, which is in the best interests of both healthcare workers and patients. But what constitutes appropriate sharing?

Privacy protection is not absolute and must be implemented in a practical way. The duty of care cannot be fulfilled without the ability to both...
treat illness and preserve privacy. This is why there are statutory exceptions to the rule of confidentiality. For example:

- To meet the best interests of society as a whole, some legislation requires disclosure (e.g., laws concerning child protection, communicable disease reporting, workers’ compensation).
- Healthcare records may be open to access in cases where a physician or institution is being audited by Ministry of Health programs, professional college reviews and healthcare accreditation bodies.
- In the interests of meaningful quality assurance, specifically identified documents are protected by legislation from seizure (e.g., by a plaintiff’s lawyer in a lawsuit).
- If the health or safety of the patient or another person is at risk, the ethical responsibility to the person overrides confidentiality requirements.

In short, privacy is an individual’s right. It is, therefore, an organization’s responsibility to collect only what information is needed to be accountable, and to be open about its information management practices and its application of privacy principles and legislation.

Information Security

Patient privacy depends on protecting the personal health information that the organization has legally collected in support of patient care. Information security breaks down into three protective goals:

- **Integrity**
- **Availability**
- **Confidentiality**

Patient safety and good care both depend on maintaining the first two of these goals: integrity and availability of information. Patient trust requires that confidentiality be maintained. Note that confidentiality is a narrower concept than privacy, as it is also the responsibility of the organization to ensure that information is made available only to those who need it for a defined purpose.
Patient Portals, Privacy and Security: An Overview

A patient portal is a controlled and secure computerized pathway between the patient and the personal health information (PHI) of that patient, which is held by the health information steward, trustee or custodian. Patient portals can be instrumental in building trust and collaboration between patients and providers, a prerequisite of good healthcare. Patient portals, properly developed and responsibly implemented, can increase transparency, accountability, support and access to information and services.

From the patient’s perspective, a portal is an application that runs on a home or personal computer or mobile device, allowing the patient access to PHI by securely connecting with the healthcare or service provider’s information network. Patients can view or download some or all of their own information for whatever purpose they wish. The goal is to actively engage patients in awareness and self-management, and to improve care coordination. For patients, a portal has the potential to act as the cornerstone for monitoring and evaluating their health status. Through a portal patients can, for example, schedule appointments, understand their care plans, get information on the programs and initiatives relevant to them, record their own PHI (e.g., glucometer data), obtain immediate feedback, access occupational health and safety services, conduct financial transactions and browse trusted health information provided by governmental and academic bodies.

From the provider’s perspective, patient portals are a reliable infrastructure that enhances communication and provides a unique mechanism to understand the patient. Different portal services, ranging from scheduling...
to making personalized health recommendations, allow healthcare providers to easily identify the areas where intervention is required and to ensure patients make meaningful use of the information about themselves.

The Evolution of Patient Portals

Portals were introduced in the early to mid-1990s in the United States as “affiliation tools” by hospitals. Mainly information portals, they were components of community health information networks (CHINs). The second iteration of portals expanded beyond the simple delivery of health education information to provide patients with access to results. Building on from that point, patient portals then started to supply providers and patients with information and knowledge that would increase collaboration and quality of service.

More recently, social media tools have extended what patient portals can offer to patient self-care, patient-patient interaction, focus and support groups, health promotion initiatives and provider-patient interaction. Social media–enabled portals also offer an infrastructure for evaluating and improving some health belief models. By studying patterns of visit and using web analytics and churn analysis, organizations can evaluate how successful a health message has been in reaching its audience and affecting behaviour and perception. Social media models can be further leveraged to improve effectiveness of such systems and to supply evidence for critical appraisal of their impact and value to society.

Patient portals will continue to evolve. While early models provided view- or read-only access for individual patients wanting to review their PHI that was maintained by a primary health provider, newer versions will increasingly be controlled by the patient, have increased functionality and will become more accessible to a wider audience involved in the patients’ circle-of-care (e.g., other healthcare service providers, caregivers, family members). This means that portals will increasingly need to integrate multiple sources of information into a comprehensive personal health record (PHR) that can be supplemented by patient-captured information, and that privacy and security issues will increase.
Portal Architecture: Two Generic Approaches

The architecture of a patient portal is critical to the privacy and security of personal and organizational information. Any portal should be planned using the seven Privacy by Design principles developed by the Information and Privacy Commissioner of Ontario (see http://privacybydesign.ca/about/principles).

Figure 1 illustrates two different portal types from the perspective of patient functionality: 1) a passive portal that provides read-only access to PHI maintained by the provider, and 2) an active portal that provides various collaboration features or functional variations extending the collaboration capabilities. Different privacy and security risks will arise with both types. That is, information flowing both from and to the patient raises different privacy and security issues than when information flows in one direction only.

Both of these types of architecture fall into the spectrum of integration under the categories of standalone, tethered and integrated models, which are reviewed in more detail below.

Passive portals

A passive portal provides single-user access to a subset of the health record information maintained by a healthcare provider. Data is provided in view- or read-only mode without any capability given to the viewer. This model provides limited functionality and utility as there is no interaction or collaboration between the patient and the healthcare provider.

Active portals

An active portal provides varying degrees of interaction and collaboration among the patient, service providers and the patient’s circle-of-care. The simplest version is the “offline” portal, which provides single-user access to a subset of information maintained by a provider and which is accessible in read-only mode. More collaborative versions may expand the data available to the patient and provide multi-user access to the patient’s circle-of-care (with appropriate authorization).

Extended capabilities available through active portals include real-time functionality, which offers options such as direct access by patients...
to make appointments, renew prescriptions and look at physician notes. Enhanced capabilities may include the following:

- Chat sessions
- Instant messaging
- Audio/video conferencing to link patients with their circle-of-care
- Secure integration with telehealth
- Mobile health and home sensor devices, providing near real-time alerts to selected care participants

Figure 1: Patient Personal Health Portal
Some active portals go even further, offering social networking functionality (e.g., Facebook) for targeted communities of interest such as diabetes patients, which can extend the collaboration beyond a patient’s primary circle-of-care.

All of these options can provide significant benefits to patients who live in remote areas or who have mobility issues.

Three Architectural Models

The functional architecture of patient portals can be classified into three distinct categories: standalone, tethered and integrated. Each has specific characteristics that affect the level of potential privacy and security risk. Each must be examined in light of these characteristics so that those risks can be mitigated.

Standalone portals

A standalone portal is a relatively simple system for a single user with no direct information sharing or electronic medical record (EMR) system integration capabilities. Standalone portal systems are mostly commercially developed using cloud computing, and they are generally offered for free. Figure 2 illustrates the functional architecture of a standalone portal.

Hosting organizations that offer standalone portals assume no legal responsibility for protecting PHI: they claim patients are volunteering to post their own information and therefore they require users to agree to accept the inherent risks. Some standalone systems may be enhanced by using third-party services that enable individuals to share their PHI with healthcare providers or institutions.

Several privacy and security issues arise with standalone portals. First, while it has been shown that some security controls can be applied in a cloud environment, this isn’t always done. (See paper published by OIPC of Ontario: http://www.ipc.on.ca/images/resources/privacyintheclouds.pdf.) Users should carefully examine the privacy and security policy applied by the host organization to ensure they understand where and how their data will be used and how it is protected.
Second, all the basic considerations of security must be applied, including following an appropriately constituted security program with oversight, risk analysis and controls. As well, it is important to be aware of the specific security risks that are more prevalent in the processes that are part of standalone patient portals, including the following:
• **Registration:** The basic process of registering as an anonymous person over the Internet where the individual’s identity is not verified

• **Authentication:** Basic user ID and password to authenticate a single user

• **Authorization:** Role-based access control (i.e., basic access control) to control user access to portal functions and information

• **Messaging:** Encryption over the Internet (SSL during transmission)

Risk to privacy is present with a standalone portal model when security is not appropriately applied or when the organization has not set up an accountability and transparency structure to apply to information made available. Privacy risks include, for example:

• Inadequate accountability for the information made available (i.e., functioning under the premise that a portal is an IT initiative, with little accountability for clinical, patient safety or information privacy risk)

• Inadequate security to protect information confidentiality, integrity and availability

• Inadequate education of patient-users, which could result in privacy breaches due to the patients’ lack of knowledge of the risks associated with portal use

**Tethered portals**

A tethered portal is typically an add-on component to EMR/EHR software or claims processing software that allows patient functionality. Two variations of tethered portals, provider and payer, are shown in Figure 3.

This portal model provides a “window” for the patient into information maintained either by the healthcare provider or payer. It resembles the traditional physician-patient relationship. PHI is stored on the server of the organization that becomes the information steward or trustee, and there is no access by the patient’s circle-of-care. Tethered systems often have dedicated secure messaging capabilities for appointments or feedback on health conditions.
As with any system, basic security policies must be implemented for tethered portals. As well, there are additional risks to address:

- **Registration**: Initial registration for the patient by invitation; identity is known
- **Authentication**: Basic user ID and password used to authenticate a single user once initial registration is completed
- **Authorization**: Applies the actions and permissions that the user is permitted to use (e.g., access to information, edit information, create information)
- **Secure messaging**: Provides a means to communicate securely using encryption technology and processes and associated messaging management processes
- **Encryption**: Applies to messages to provide secure communications, allowing them to travel securely over otherwise insecure networks such as the Internet (e.g., SSL during transmission)
Integrated portals

Integrated portals allow patients full access to their health information and increased opportunity to collaborate with their care providers and circle-of-care. In fact, the personally controlled health record accessible through an integrated portal could become an all-encompassing PHR, consolidating a patient’s own entries, genetic information, medication history and physician charts with assessments, care plans, case notes, referral reports, medical images and lab results, all from multiple providers.

Figure 4 illustrates the architecture of a fully integrated portal.

Figure 4: Fully Integrated Portal Architecture
A critical component to the integrated portal is the “integration engine,” which provides a secure exchange mechanism to push and pull health information to and from multiple systems, replicating and synchronizing data. Exchange can occur by using structured messaging such as HL7—a higher security standard than old messaging technology.

As with other portal models, basic security policies must be implemented for fully integrated portals. As well, the following risks are inherent in this model:

- The individual patient can have full access permission and may be able to grant anyone access to subsets of information. If not properly managed, full access to PHI can create a risk leading to a loss of information integrity, accuracy and confidentiality. Individuals must fully understand the privacy policies and controls of the patient portal they are using and the implications of granting access privileges to others, as well as the process for revoking it.
- Integrated portals require a more complex architecture that must be standards-based in order to offer a provider-neutral open EHR platform (i.e., one that is not tailored to a specific care provider). Standards-based architecture allows systems to be integrated and data to be replicated to allow for information to be exchanged between the various EMR products used by physicians, hospitals, labs, pharmacies, health registries and other healthcare-related facilities as well as with mobile and home monitoring devices. The integrated portal architecture is complementary to the Canada Health Infoway architecture blueprint. Consequently, more detailed and more personal health information is rapidly becoming available and requires that associated risks be addressed.
- All data transfers require extensive audit logging to support data governance and stewardship and to ensure accountability for data quality, confidentiality, availability and integrity.

Other specific privacy processes related to integrated portals include:

- **Registration:** Initial registration for the patient by invitation (The patient’s identity must be known, provable and proven.)
- **Registration authority:** A robust mechanism to accurately authenticate the patient-user (This may be a third party and may require face-to-face identification processes.)
- **Authentication:** Strong user ID and password policy to authenticate the user (Optional “two-factor” authentication may be required.)
• **Single sign-on:** Eliminates the necessity for the patient to manually authenticate when accessing external repositories

• **Authorization:** Basic access control (e.g., RBAC) to control user access to portal functions and information

• **Consent management:** Manages the directives to authorize access to data by others and the specific uses to which the data may be put (It is managed by patients, and so requires that the patients understand their responsibilities regarding access by others.)

• **Audit logs:** The log of all access to the patient portal, which is available to the patient-user (Health data transfers between an EMR and PHR must also be logged indicating the data source.)

• **Secure messaging:** Provides a means to communicate securely using encryption technology and processes and associated messaging management processes

• **Encryption:** Applies to messages to provide secure communications, allowing them to travel securely over otherwise insecure networks such as the Internet (e.g., SSL during transmission)

• **Database encryption:** Optional requirement to enhance privacy and security of personal health-related data, documents and images

The following table summarizes the privacy and security components required for each of the portal architectures and functions.
Table: Portal Architecture—Privacy and Security

<table>
<thead>
<tr>
<th>Functions</th>
<th>Portal Architecture Models</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Standalone Portals</td>
</tr>
<tr>
<td></td>
<td>• Patient-managed PHI</td>
</tr>
<tr>
<td></td>
<td>• Self-managed</td>
</tr>
<tr>
<td></td>
<td>• Provider/Patient participation</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Mitigating Requirements</td>
</tr>
<tr>
<td>View-Only PHI</td>
<td>• Registration – Anonymous</td>
</tr>
<tr>
<td></td>
<td>• Basic authentication</td>
</tr>
<tr>
<td></td>
<td>• Basic authorization</td>
</tr>
<tr>
<td></td>
<td>• Encryption – SSL</td>
</tr>
<tr>
<td>Access &amp; Enter PHI</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Patient Care Plans</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>View Scheduled Appointments</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Portal-Licensed General Health</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Information</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Financial Transactions</td>
<td>May be limited to subscription fees</td>
</tr>
<tr>
<td>Manage Access &amp; Consent</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Public Accessible General Health</td>
<td>Accessible via links to external portals and information websites</td>
</tr>
<tr>
<td></td>
<td>May require:</td>
</tr>
<tr>
<td></td>
<td>• Registration – Anonymous</td>
</tr>
<tr>
<td></td>
<td>• Basic authentication</td>
</tr>
</tbody>
</table>

Jurisdictional license for use only by healthcare organizations and providers in Ontario.
Canadian Privacy Legislation

General Principles

The laws affecting privacy and patient portals vary among provincial, territorial and federal jurisdictions, and it is important to understand what laws affect your organization.

All Canadian privacy laws, irrespective of jurisdiction, fundamentally support an individual’s right of access to personal and/or health information. As well, several other basic principles are common to all legislation, including the following:

• Patient portals do not negate a legal obligation to respond to a formal request for access to information received under applicable provincial or federal laws. (While patient portal initiatives can form an important component of a data steward’s strategy for providing patients with access to their health information, they must not be relied on to fulfill all requirements for access.)

• Health and/or personal information should be collected directly from the individual. The ability to collect information must be weighed against the need to collect, use and disclose the information. For example, a health services provider may need to validate health information provided by a patient before that information is considered sufficiently reliable upon which to base clinical decisions.

• Data stewards, custodians and trustees, and organizations must take reasonable steps to protect health and/or personal information against reasonably anticipated risks to privacy. Several jurisdictions and funding bodies require or recommend that these risks and the corollary...
mitigation strategies be described in a privacy impact assessment (PIA). COACH recommends that PIAs be conducted as a privacy best practice.

**Common Challenges**

Simply put, privacy laws apply to public bodies, data stewards, custodians and trustees, and organizations that have custody and/or control of personal and/or health information. Knowing how to apply the law requires knowledge and skill.

First, it can be challenging to determine which laws apply under different circumstances. That is, the various functions associated with a given patient portal and its deployment determine an organization’s obligations in relation to the portal, and those obligations may be derived from different laws.

For example, a patient portal initiative offered by a regional health authority that is defined as a custodian under the provincial privacy law would likely fall under the custody and control of that health authority. But in the same jurisdiction, a private sector company offering a fee-for-service patient portal that is not affiliated with a custodian will likely be subject to federal or provincial private sector privacy laws. Further, if a data steward were to negotiate the services of that same private sector company to provide a portal on its behalf, the company would then become an agent or affiliate of the regional health authority, which means the relevant laws are those that apply to the organization in charge.

It is crucial for data stewards, trustees and custodians, as well as organizations looking to implement patient portals, to determine their legal obligations under the relevant privacy laws. This includes fully understanding all legal requirements related to collecting, using and/or disclosing health information, including any requirements that may be passed along to vendors and other third-party service providers.

Another challenge is how to implement new technologies under existing laws, which are typically “technology neutral.” Few statutes address the concept of electronic health records, and none expressly acknowledge patient portals. This means that custodians and organizations looking to
establish patient portals must draw inferences about how the general requirements expressed in law apply.

The issue of data storage location and associated risks also must be assessed by every data steward choosing to participate in a patient portal initiative, regardless of jurisdiction. Several jurisdictions prohibit or restrict the disclosure of and access to health information outside of Canada. Those that do not forbid foreign disclosure and access without express consent often require a data steward to implement additional safeguards to protect health information that may be stored outside of the jurisdiction. Further, where individual consent for foreign disclosure, access or storage is required, individuals must be advised of the potential risk when being asked for their consent.

Finally, several jurisdictions have codified a patient’s right to express a “consent directive” related to sharing health information. A consent directive, more correctly termed a “disclosure directive,” allows individuals to exercise some control over how their information is disclosed to others. Where such directives are in use, a data steward may not disclose information without the consent of the individual, unless that disclosure meets certain other requirements (e.g., information needed in a medical emergency).

Depending on the data steward’s level of involvement in a patient portal initiative, there may be a legal requirement for that data steward to implement functionality to allow patients to restrict the disclosure of information they place in a portal environment, and this might be done through a disclosure directive.

Legislative Variations by Jurisdiction

The COACH publication Guidelines for the Protection of Health Information provides an overview of the various health privacy laws in effect in each jurisdiction. The information below does not attempt to repeat that publication, but it highlights those issues that custodians of health information must pay particular attention to when developing and implementing patient portals.
British Columbia

Applicable statutes:
- E-Health (Personal Health Information Access and Protection of Privacy) Act
- Freedom of Information and Protection of Privacy Act (FIPPA)
- Personal Information Protection Act

Health information in B.C. is protected by a network of public and private sector privacy laws, with a specific statute geared to the development of the provincial EHR. Custodians looking to develop patient portals in B.C. must pay particular attention to understanding which law will regulate their portal.

- Any portal that is intended to interface with the B.C. provincial EHR may be required to comply with the E-Health Act, including the ability to adhere to a patient’s consent directive.
- Any portal held by a public body that has not been designated as a health information bank will be required to meet the level of protection of health information described in the Freedom of Information and Protection of Privacy Act (FIPPA).
- A patient portal offered by a third party (i.e., not a public body under FIPPA) is subject to the Personal Information Protection Act, which allows for the collection, use and disclosure of personal information with consent. It is therefore possible that a private sector company offering a portal would be able to perform functions with personal information that a public body would not, as the public body is limited to performing functions authorized by law.
- B.C. expressly prohibits public bodies from storing health information outside of Canada without the consent of the individual. Data stewards considering a patient portal with support from a third-party vendor must consider the extraprovincial storage of health information and the extent to which the information could be accessed.

Alberta

Applicable statutes:
- Health Information Act
- Personal Information Protection Act

Most provider-offered patient portals will fall under the Health Information Act. The exception is a patient portal that is exclusively offered by
a third-party vendor through a relationship established directly with the individual. In this case, the governing statute is the Personal Information Protection Act.

Other factors to consider:
• Custodians implementing a patient portal are required to submit a privacy impact assessment to the information and privacy commissioner before a system is implemented.
• Health information to be included in the Alberta EHR is determined by the Minister of Alberta Health and Wellness and health professional regulatory bodies. It is therefore possible that information uploaded to a patient portal by the patient could be targeted for inclusion in the Alberta EHR, which raises significant privacy concerns.
• Custodians must consider the express wishes of individuals when deciding how much health information to disclose or make available through the Alberta EHR.
• Any patient portal that becomes a component of the Alberta EHR is subject to the same requirements as other EHR systems, including a need for robust access logging functionality and the ability for an individual to obtain an audit log showing which users have accessed their health information.

Saskatchewan

Applicable statutes:
• Health Information Protection Act (HIPA)
• Personal Information Protection and Electronic Documents Act (PIPEDA—federal)

The Health Information Protection Act (HIPA) regulates the collection, use and disclosure of health information by public bodies, specified regulated health professionals and designated organizations.

HIPA specifies that consent for the collection, use and disclosure of health information can be deemed, expressed or implied. While an argument can be made that a patient using a portal has provided implied consent within the portal, trustees under the Act must evaluate whether it would be prudent to obtain express written consent. This is particularly important with complex portal initiatives that involve multiple uses and disclosures of health information; in these cases relying on deemed or implied consent will not be possible unless it can be demonstrated that the
individual understood the consequences of entering information into the portal.

As with the legislation in other jurisdictions, HIPA contains specific requirements for legal agreements between trustees and information management service providers. The Act also recognizes a comprehensive health record called the Saskatchewan Health Information Network (SHIN). Should a patient portal initiative become a part of SHIN, HIPA’s requirements to limit the disclosure of health information through SHIN would affect information included in the patient portal.

Manitoba

Applicable statutes:
- Personal Health Information Act (PHIA)
- Personal Information Protection and Electronic Documents Act (PIPEDA—federal)

The Personal Health Information Act (PHIA) regulates the collection, use and disclosure of health information by a health professional, healthcare facility, public body or health services agency that collects or maintains personal health information (called “trustees”).

Trustees can enter into agreements with information managers to provide information management/information technology services. PHIA does not contain specific requirements for the EHR, although privacy impact assessments are required by Manitoba Health.

Ontario

Applicable statute:
- Personal Health Information Protection Act (PHIPA)

The Personal Health Information Protection Act (PHIPA) contains the strongest consent model in Canadian health privacy law. Under this Act, individuals must consent to the collection, use and disclosure of their health information, although there are circumstances where the consent can be implied by the actions of the individual and where it can be demonstrated that the individual had reasonable knowledge of the intended use and disclosure of health information.

The PHIPA consent model introduces a unique consideration for portal developers—specifically, health information custodians are required to respect the decisions of individuals related to the collection, use and
disclosure of health information. This means that patients may enter information into a portal for their use, but wish to restrict the disclosure of the information to care providers. In these circumstances, it is particularly important that individuals receive reasonable notification about the use and disclosure of their health information and the process that should be followed to restrict access to it.

Organizations that are not public bodies subject to public sector privacy laws or custodians subject to PHIPA but that wish to develop or implement patient portal technology will be subject to the federal PIPEDA.

Quebec

Applicable statutes:
• An Act Respecting Access to Documents held by Public Bodies and the Protection of Public Information
• An Act Respecting the Protection of Personal Information in the Private Sector

Quebec’s relevant legislation is a complex network of privacy laws covering the public sector, private sector and regulated professionals. While consent requirements for the disclosure of health information have shifted over time, the current expectation is that consent is required for the collection, use and disclosure of health information unless the communication must be performed as part of the delivery of a health service to the individual. Consent must be “manifest, free, and enlightened,” and must be given for a specific purpose and time.

New Brunswick

Applicable statutes:
• Personal Health Information Privacy and Access Act (PHIPAA)
• Personal Information Protection and Electronic Documents Act (PIPEDA—federal)

The Personal Health Information Privacy and Access Act (PHIPAA), proclaimed in force on September 1, 2010, is similar to other provincial health privacy statutes in that it regulates the collection, use and disclosure of health information. PHIPAA requires custodians to notify individuals if PHI has been lost, stolen or otherwise inappropriately destroyed, disclosed to or accessed by an unauthorized person where it is reasonable to conclude that harm could occur. The PHIPAA consent model more closely parallels
the Ontario consent model than the implied or deemed consent models adopted by other provinces.

**Nova Scotia**

**Applicable statutes:**
- Freedom of Information and Protection of Privacy Act
- Personal Information International Disclosure Protection Act (PIIDPA)
- Personal Information Protection and Electronic Documents Act (PIPEDA—federal)

While health privacy legislation has been proposed in Nova Scotia, it remains unproclaimed at the time of writing. Under the current legislative regime, health information held by public bodies is regulated by the Freedom of Information and Protection of Privacy Act, and personal information held by private sector and not-for-profit organizations are subject to federal legislation (see federal section below).

In light of concerns related to the disclosure of personal information to foreign law enforcement agencies, Nova Scotia enacted the Personal Information International Disclosure Protection Act (PIIDPA), which prohibits the storage of personal information outside of Canada unless specific requirements are met.

Bill 89, Nova Scotia’s proposed Personal Health Information Act, considers mandatory privacy breach reporting. It has not yet been determined whether custodians of health information under any proposed health privacy law in Nova Scotia will be required to adhere to the PIIDPA.

**Prince Edward Island**

**Applicable statutes:**
- Freedom of Information and Protection of Privacy Act
- Personal Information Protection and Electronic Documents Act (PIPEDA—federal)

Health information in the public sector is subject to provincial public sector privacy law and the Freedom of Information and Protection of Privacy Act. Information in the private sector is subject to the federal PIPEDA (see federal section below).
Newfoundland and Labrador

Applicable statutes:
- Personal Health Information Act (PHIA)
- Personal Information Protection and Electronic Documents Act (PIPEDA—federal)

The Personal Health Information Act (PHIA) applies to custodians involved in delivering healthcare services in both the public and the private sectors. PHIA positions itself as a “consent-based” health privacy law with similarities to Ontario’s PHIPA. PHIA contains “lock-box” provisions, which limit the collection, use and disclosure of health information in circumstances where the individual has withdrawn consent.

Custodians must notify the information and privacy commissioner if there is a material breach of the Act, and they must notify individuals if their PHI is lost, stolen, disposed of or disclosed in an unauthorized manner.

Yukon

Applicable statutes:
- Access to Information and Protection of Privacy Act
- Personal Information Protection and Electronic Documents Act (PIPEDA—federal)

Health information in the custody or under the control of a public body in Yukon is subject to the Access to Information and Protection of Privacy Act. Any health information in the private sector is subject to the federal PIPEDA (see federal section below).

Northwest Territories

Applicable statutes:
- Access to Information and Protection of Privacy Act
- Personal Information Protection and Electronic Documents Act (PIPEDA—federal)

Health information in the custody or under the control of a public body in the Northwest Territories is subject to the Access to Information and Protection of Privacy Act. Any health information in the private sector is subject to the federal PIPEDA (see federal section below).
Nunavut

Applicable statutes:
- Access to Information and Protection of Privacy Act
- Personal Information Protection and Electronic Documents Act (PIPEDA—federal)

Health information in the custody or under the control of territorial departments and most territorial agencies, boards and commissions in Nunavut is subject to the Access to Information and Protection of Privacy Act. Any health information in the private sector is subject to the federal PIPEDA (see federal section below).

Federal legislation

Applicable statute:
- Personal Information Protection and Electronic Documents Act (PIPEDA)

The federal Personal Information Protection and Electronic Documents Act (PIPEDA) applies to personal information held by organizations engaged in commercial activities in those jurisdictions where a provincial statute has not been established as “substantially similar.” At the time of writing, only British Columbia, Alberta, Ontario and Quebec have laws that have been deemed substantially similar to PIPEDA. Therefore, the Act applies in those other jurisdictions where portals are being developed and offered directly by third-party vendors or regulated health professionals performing a commercial activity.

Organizations developing patient portals that require compliance with PIPEDA or substantially similar legislation must do so with high consent standards in mind. Unlike some public or health sector privacy laws, PIPEDA severely restricts the collection, use and disclosure without consent. In other words, for a patient portal to comply with PIPEDA, that portal will require express consent, and the consent must be freely given and must be obtained after reasonable notification has been provided to the individual. Organizations will also need to consider how data should be retained in the event that an individual withdraws that consent.
Selecting a Patient Portal Model

The convenience and flexibility of patient portals offer many benefits to both patients and providers. Selecting the best model for your organization—one that will provide safety, reliability and privacy—requires making an investment in time to thoroughly assess the various options.

Considering the Basics

The first step is to reach consensus on the purpose for the portal. The goals and objectives should be feasible, advisable and achievable. Once the purpose is agreed upon, an organization should create selection criteria and a set of measures against which the criteria can be assessed. This process can be simplified by using a systematic approach. Consider the following:

- **Usability:** To ensure usability, which in turn supports an error-free, secure and private solution, clinical content must be in line with the provider’s standard. Knowledge, information, data and the language used should be acceptable to the organization hosting the portal as well as to its clients. The functions provided by the portal should complement the way in which the hosting organization does its business.

- **Technical requirements:** To ensure the functionality and security goals are adequate, all tools for a particular portal model, such as the development environment, back-end software and database management system, must be easily maintained, have a sufficient market lifetime, support the common goals of the organization and support accepted messaging protocols and technical standards, including security standards.
• **Operational aspects:** Usability and error-free operation is assured through formal testing that engages a spectrum of user types. The support system provided for the portal should be examined for capability in all phases of development, maintenance, use, evaluation and evolution. Ideally, the model will include metrics to monitor various impacts, including but not limited to patient and provider satisfaction, process quality, efficiency, positive effects on the attitude of patients and other indicators that demonstrate how well the portal is achieving its purpose.

After these factors are evaluated, an organization must put effort into developing a clearly defined policy that periodically assesses these issues and ensures that the portal remains congruent with, and complementary to, other care processes. The policy should consider any changes to the purpose of the portal, along with goals, objectives, deployment, use, operation, access, evaluation, backup and recovery.

The fiscal components of choosing a portal are, of course, also important. All costs, whether capital or operational, must be considered over the lifetime of the portal. As well, vendor and support contracts must address the need for flexibility in this newly emerging environment in order to support change and long-term use.

Once all the above factors have been considered, an organization will be able to objectively evaluate different model options, understanding the strengths and weaknesses of each.

---

**Knowing the Target Audience**

Users of patient portals do not fall nicely into one demographic category or description, and providers must consider who their users are when choosing the best model to employ. For example, users of a portal for a mid-sized doctor’s practice will have different requirements from users of a portal that focuses on long-term care or terminal and cancer care. As a result, a patient portal model that suits one provider may not be the best choice for another.

Each provider needs to ensure that users understand what the portal can do for them, how they can use it, what their responsibilities are and what to do if something goes wrong. Based on the language, culture, demographics and severity of the health problem, the protocol to convey
both clinical and privacy information can differ. Definitions of usability may change, and the requirements for privacy and security may need to be revised.

Engaging all relevant clinical providers and targeted users in the process of defining, designing and developing the portal will ensure that it will be both usable and durable. Such a process also signals to users that the organization is following proper development methodology and is committed to a long-term investment of providing reliable patient data that is targeted at the particular audience.

Keep in mind that the portal is only there to support the larger care process, and the patient’s use of the portal must be integrated with other patient information and care structures. Providers need to ensure that the portal content and ways in which it is used do not negatively affect the other parts of their care processes.

The patient users themselves can provide some of the best information to an organization for selecting a portal. It is worthwhile asking patients, in private of course, if they object to any of the services or practices offered by the portal. Users should have effective but secure access to information about themselves and be helped to understand it. The portal should be the vehicle for such information and, at the same time, should protect patient privacy and information security. Patients should not be left guessing what their information is being used for or how their health service delivery will be affected by the use of the portal.

Understanding Your Responsibilities

Providers of healthcare information are responsible for ensuring that anyone who uses a patient portal is ensured the continuum of safe care and confidential service. When selecting a model, it is crucial to keep this responsibility in mind. Consider the following:

- When assessing different models, ask for access to metrics and review them periodically. Today’s business intelligence solutions commonly provide dashboards to track metrics over time and to stratify them in different degrees of granularity. Ask to see how the portal will reveal usage, security violations, patient satisfaction and other metrics. Take the time to discuss the portal with your patients
as you visit them, asking what they think of the system and if they have used all its features.

- Stay in contact with the governing body of the portal. Participate in stakeholder meetings, and provide regular feedback on pros and cons of the system as you use it and observe your patients’ use of it.
- Review service-level agreements and privacy statements frequently, as well as patient consent forms.

For further information on selecting an appropriate model, see Appendix B, which provides links to organizations and resources that can provide answers to specific questions about this evolving subject.
Risks and Controls

The following discussion provides risk and control guidelines for patient portals organized by portal functionality. The first two sections here, Commonly Available Functionality and Privacy Guidelines for Commonly Available Functionality, describe 11 basic functions available in most portals. These are:

- Function #1: Administrative information
- Function #2: Proxy and substitute decision maker (SDM)
- Function #3: Review cumulative patient profile
- Function #4: Review lab results
- Function #5: Messaging
- Function #6: Alerts and reminders
- Function #7: Patient education materials
- Function #8: Scheduling
- Function #9: Access audit
- Function #10: Printing and downloading
- Function #11: Chronic disease information

For each of these functions, risks and controls are discussed. The remaining sections describe the degree of patient engagement with the functions of the portal and with reference to risks and controls as they apply to the 11 basic functions, plus any additional functions.
Commonly Available Functionality

Function #1: Administrative information

Patients can enter and update certain pieces of their personal information that are maintained in their provider’s EMR, such as a change of address or telephone number, and access administrative information about their physician and clinic. Clinics can also post administrative information for patients, such as the clinic address, telephone number, list of physicians working out of the clinic, pharmacies, procedures for making health plan claims, and so forth.

⚠️ Risks: Some administrative information is extremely sensitive, and if it is compromised in any way there can be serious consequences for the patient and the provider in terms of privacy.

🔒 Controls: Standards exist to ensure security and privacy of administrative information, each having its own level of granularity. Be sure to obtain and apply the specific requirements for the jurisdiction.

Function #2: Proxy and substitute decision maker (SDM)

Patients can register one or more other individuals (a proxy) to access their health information and, in the case of a formalized substitute decision maker, to make healthcare decisions for them. For example, a woman may want all her children to be able to access her health information in her portal, but assign only one of them as her SDM.

To function effectively, portals must have the capacity to limit what the proxy can do and see. For example, one proxy may be able to see limited and specified information only, another may be able to see everything, and yet another may be able to write information to the portal. None of them may receive the alerts that go the patient. Proxy functionality must support the organization’s policy and process to institute a legal SDM.

⚠️ Risks: The patient may assume that SDM access is restricted to a subset of information, a limited timeframe, specific circumstances or a specific purpose. If that assumption is not correct, the SDM may be able to access data outside the wishes of the patient.
**controls:** Ensure the patient is aware of the capabilities of the portal to revoke and restrict SDM access. Audit SDM access according to security standards and product documentation.

**Function #3: Review cumulative patient profile**

Patients can be given access to their medical record, including information on allergies, medications, immunization records, medical procedures, family history and more. Access may be to their cumulative patient profile, or be limited to information a physician chooses to release.

⚠️ **Risks:** Aside from risks that are not in the security and privacy domain (e.g., patients misunderstanding medications or procedures), there is a risk that patients may inadvertently compromise their data by accessing it in a non-secure environment.

🔒 **Controls:** Patients must be educated about the risks of accessing private information over insecure networks, such as in public places with free Wi-Fi. Audit and log functions should alert the responsible party to any unauthorized access, or display an alert regarding access from an unfamiliar IP address or user.

**Function #4: Review lab results**

Patients may be given access to all results from any lab or diagnostic imaging visits, or physicians may select which results to release to patients, and perhaps provide comments. For example, patients may have access to view final results, but not interim results. If full access is granted, version control must be managed.

This function could also notify patients at login when results are available and inform them if their physician requests a follow-up visit.

⚠️ **Risks:** Aside from risks that are not in the security and privacy domain, such as patients misunderstanding lab results, there is a risk that patients would inadvertently compromise their data by accessing it in a non-secure environment.

🔒 **Controls:** See above controls for **Function #3**.
Function #5: Messaging

The messaging function allows patients to securely receive communications from physicians or their staff. Messages may range from simple announcements of new portal features to follow-up instructions from a recent visit.

⚠️ Risks: Messages may divulge confidential information.

🔒 Controls: Restrict information in messages to the minimum, making sure the patient has to login to the portal to see them. To protect against illicit or unintended use, remove messages from the portal after they have served their purpose.

Function #6: Alerts and reminders

Patients can be alerted by email that an important message has been posted on the portal. The trigger for sending a notification email could be an automatic function of the portal (e.g., when a lab result is available, an email is sent), or be done manually (e.g., a physician emails patients to alert them to a new message on the portal).

⚠️ Risks: See above risks for Function #5.

🔒 Controls: See above controls for Function #5.

Function #7: Patient education materials

Educational materials can be made available on the portal, either to all patients (e.g., general health guides) or to specific individuals. In the latter case, the material can be tailored to particular conditions or requirements.

⚠️ Risks: Confidentiality concerns arise if patients are profiled by health issues. For example, if it can be deduced that a patient is diabetic by the information being sent, that patient could be targeted for product marketing.

🔒 Controls: Mark any documents that require downloading by the patient as confidential, and include a statement notifying patients of their own responsibility to protect their confidential documents.
Function #8: Scheduling

Patients can review upcoming scheduled appointments with their physician or other members of their clinical team, as well as specialist and referral appointments. They may also be able to make appointments from a list of available slots and receive reminders of upcoming appointments.

⚠️ Risks: See above risks for Function #5.

🔒 Controls: See above controls for Function #5.

Function #9: Access audit

Under legislation that governs providers, patients could be provided with a report showing who has accessed their information contained in the EMR.

⚠️ Risks: For information to be meaningful, patients may need to know both the name and the position of the person who accessed their records. In the case of appropriate access by a care provider, neither the name of the person nor the role may be meaningful to the patient. In the case of inappropriate access, the name may be highly meaningful but the role may not be. These scenarios may result in patients facing the risk of misunderstanding what they discover. That is, the information about access may be accurate, but it may not clearly tell them who accessed the data and whether the access was appropriate.

🔒 Controls: Depending on the number of different users who are authorized to access patient records, it may be necessary to adjudicate all access audit information given to patients.

Function #10: Printing and downloading

Patients may print and make copies of information to use when communicating with other care providers, their family and social networks, and legal and personal advisors.

⚠️ Risks: Information printed and downloaded may divulge confidential information.

🔒 Controls: See above controls for Function #7.
Function #11: Chronic disease information

Patients suffering from chronic diseases may be given access to educational material (e.g., information pamphlets on how to manage the condition) and specific clinical information (e.g., flow sheets or other trending displays of their results).

⚠️ Risks: See above risks for Function #3 and Function #7.

★★ Controls: See above controls for Function #3 and Function #7.

Privacy Guidelines for Commonly Available Functionality

Presented here are some of the most important considerations when making information available to patients for viewing within a patient portal. Note that this is not an exhaustive analysis of all risks associated with the view-only functions identified. Note also that not all of the 10 principles of the CSA Model Code apply to all patient portal functions.

Function #1: Administrative information

GENERAL PRIVACY CONCERNS

Administrative information on a patient portal is especially sensitive because it can provide direct identifying details relating to a patient or imply clinical conditions. If breached, this information could be used to commit identity theft or to otherwise embarrass a patient. Therefore, when patients download administrative information, the service provider should ensure it is encrypted during transmission. Patients should be informed of all confidentiality protection measures or controls.

ACCOUNTABILITY

⚠️ Risks: The portal owner is responsible for the information until it is in the custody of the recipient. Patients expect that their healthcare providers and service providers will treat their PHI as confidential and be accountable for its security, but patients cannot be expected to understand or be interested in the details of the risk and how it is
managed. Patients therefore cannot be asked to accept security risks that they may not understand and over which they have no control.

**Controls:** The point where responsibility is transferred, and the scope of each participant’s responsibility, must be clearly communicated to patients. Information sources must be corrected as applicable if new data becomes available. Patients need to be informed that they always have the opportunity to request changes if information is out of date or inaccurate.

**ACCURACY**

⚠️ **Risks:** If a patient wants to download PHI, it is reasonable to assume that one of the patient’s primary intentions may be to verify the accuracy of the information.

偏好 **Controls:** Make patients aware that their “copy” of the PHI is only a snapshot in time. They must understand that while it will be useful for checking accuracy, it could be out of date as soon as the next update modifies the source system.

**SAFEGUARDS**

⚠️ **Risks:** Stewards, trustees, custodians and service providers of PHI are legally responsible for providing appropriate safeguards (physical, technical, administrative) for the PHI in their custody and under their control. However, once PHI is passed to the patient via the patient portal, the patient may not be able to provide the same level of protection, which presents a risk of a privacy breach.

偏好 **Controls:** Inform patients that they must accept responsibility for protecting their PHI from the point that they view it in the patient portal. Require the service provider of the portal to provide all users with standard security and privacy tips for securing the privacy of downloaded PHI.

**OPENNESS**

⚠️ **Risks:** The healthcare provider and/or the service provider are required to demonstrate how they protect the PHI in their care. The risk is that such openness includes detailed descriptions of the actual security techniques used, which could be maliciously exploited. Nonetheless, it is not appropriate to ask patients to accept security risk
that is not adequate, or to expect them to understand the controls to the degree required to evaluate the risk. However, patients must be given enough information so that they understand the risks of having PHI in their possession, and that they are responsible for protecting it once they hold it.

**Controls:** Healthcare providers and service providers should avoid detailed descriptions and instead show summaries of independent assessments of how well their safeguards are designed and implemented. The service provider should also provide patients with security and privacy tips on protecting PHI on their own computing devices and environment (e.g., iPhone, at home).

**INDIVIDUAL ACCESS**

⚠️ **Risks:** Privacy legislation requires that stewards, trustees and custodians of information make a patient’s PHI available to the patient upon request. This fundamental principle of individual access is exposed to the risk of someone posing as the patient online (e.g., by hacking into the patient portal or by fraudulently using the patient’s access credentials).

⚠️ **Controls:** Administrators of patient portal systems must implement secure processes to support patient identification, authentication and privilege assignment. Patients requesting access to their PHI through the portal must be required to identify themselves, in person, before being provided with a secure user ID and unique password, which must be used to login to the portal system and view PHI.

**Function #2: Proxy and substitute decision maker (SDM)**

**GENERAL PRIVACY CONCERNS**

⚠️ **Risks:** A patient may temporarily delegate all or part of the decision-making authority to a proxy or an SDM, including authorizing access to the patient’s record via the patient portal. The risk is that the extent of the authority may not be clearly specified. For example, a patient may intend an SDM to make decisions only during a time of specific treatment, and for that authority to terminate once the patient is fully recovered. The patient may not intend the SDM to have access to sensitive information about prior conditions.
**Controls:** Patients wishing to authorize a temporary SDM should be able to set up a set of consent-based rules that clearly prescribe what, if anything, of their record an SDM can access and what actions they can take.

**ACCOUNTABILITY**

**Risks:** Patients may wish to verify when the appointment of an SDM was recorded and what decisions, if any, were made by the SDM on their behalf. There is a risk that an SDM, knowingly or otherwise, could produce evidence of being appointed, and follow up with a request to access some or all of the patient’s record.

**Controls:** The data steward or custodian and/or service provider must be able to demonstrate through an audit trail all the details of the SDM appointment and any decisions made. Patients can establish access through a set of consent-based rules, which restricts what, if anything, the SDM may access. Ideally, the audit trail of events, which is maintained by the EMR/EHR system, should be able to filter by significant factors so that only those events specific to this request will be shown.

**IDENTIFYING PURPOSES**

**Risks:** Establishing a formal SDM is a serious legal decision, usually made when a patient expects to be incapacitated. One risk to privacy is that the SDM may feel it is part of his or her responsibility to know the full health history of the patient, and therefore access the information through a portal, whether the patient intended that or not.

**Controls:** Patients must be guided to clearly define and document how and when PHI may be accessed and used by an SDM. Organizations providing such guidance should be clear about their own legal responsibility both for the advice and for what is set up.

**CONSENT**

**Risks:** When a patient formally appoints an SDM, generally the SDM assumes the full authority of the patient regarding health matters, including access to the EHR. The establishment of an SDM will be recorded in the patient’s EHR as part of the access rules to support the assignment of responsibilities. However, if this all-encompassing
authority is not what the patient intended, it may risk more information being exposed than the patient would wish.

**Controls:** The implications of appointing an SDM must be explained to the patient, and options provided. This will allow patients to clearly direct the healthcare provider and/or service provider on the extent of access to be allowed.

### LIMITING USE, DISCLOSURE AND RETENTION

**Risks:** The portal functionality may not allow patients to set access by their SDM in a granular way. In other words, if functionality is “all or nothing,” it may not be acceptable to the patient.

**Controls:** When discussing the pros and cons of establishing an SDM with patients, healthcare providers should make sure the patients understand all the ramifications of such a decision, including gaining access to their health records via the EHR. They should be guided on how to put constraints on the SDM’s access to the EHR if they so desire.

### SAFEGUARDS

**Risks:** Stewards, trustees, custodians and service providers of PHI are legally responsible for providing appropriate safeguards (physical, technical, administrative) for the PHI in their custody and under their control. However, once PHI is passed to the patient via the patient portal, the patient may not be able to provide the same level of protection, which presents a risk of a privacy breach.

**Controls:** Inform patients that they accept responsibility for protecting their PHI from the point that they view it in the patient portal. If an SDM is involved, then that person, too, should be informed that once the PHI has been downloaded, either by the patient or by the SDM, they jointly and collectively have responsibility (in the privacy interests of the patient) to provide the strongest privacy protections that they can. Require the service provider of the portal to provide all users with standard security and privacy tips for securing the privacy of downloaded PHI.
OPENNESS

⚠ Risks: Patients and their SDMs may not be familiar with their privacy rights and responsibilities.

🔒 Controls: The data steward, custodian or trustee and/or the service provider must demonstrate how well they are protecting the PHI in their care. The service provider should provide the SDM with guidelines that clearly outline rights and limitations of the SDM role.

INDIVIDUAL ACCESS

⚠ Risks: Privacy legislation requires that data stewards, trustees and custodians make a patient’s PHI available to them upon request. The patient portal must provide that function or provide another way of meeting the legal requirement. Not to do so is a risk to the patient’s right of access.

🔒 Controls: Healthcare providers should describe to patients who has access to their records so that each patient may make an informed decision to place any limits on the SDM’s access.

CHALLENGING COMPLIANCE

⚠ Risks: Patients are legally entitled to ask for evidence that proves only authorized personnel are accessing their PHI. Creating an audit trail by analyzing millions of transactions from multiple systems and looking for the few that involve a single patient is a large, complex task. There are simpler and quicker ways of handling such a request, such as downloading the consent directives associated with a patient. However, this option presents the risk of exposing sensitive information that may be improperly viewed.

🔒 Controls: If limits on SDM access have been set up under the instructions of the patient, the SDM, with legal authority, must also be able to see and change those limits.
Function #3: Review cumulative patient profile

GENERAL PRIVACY CONCERNS

⚠️ Risks: If the patient portal has no controls, unauthorized individuals might view a patient’s PHI. When patients download their cumulative patient profile to print or permanently store on their computer, they risk exposing this potentially sensitive information to other parties.

🔒 Controls: PHI available for download should be encrypted. Everyone who uses the patient portal must first be registered. For patients, this means properly identifying themselves when they register and then using an assigned login ID and password each time they access the portal. This will help prevent anyone else (except individuals whom the patient has authorized and their own healthcare providers) from viewing the information. Patients should be advised to keep downloaded information in encrypted form in storage on their computer except when viewing it, and to store any printed copies in a very safe place.

ACCURACY

⚠️ Risks: If the information on the portal is not synchronized in real time with the source, patients may not be viewing the most current version. This presents the risk of patients sharing outdated information with another healthcare provider—and potentially making health decisions based on outdated information.

🔒 Controls: In cases where there is a delay in posting the current version of information to the portal, there must exist some mechanism by which the provider can indicate this time lag. For example, a date and time-stamp could be prominently displayed on any information patients view.

OPENNESS

⚠️ Risks: There is a risk that patients will be reluctant to participate in the digitalization of their PHI into the EHR if they do not trust the methods and the environment to ensure privacy.

🔒 Controls: Both healthcare providers and service providers must make readily available to patients (perhaps in the portal registration process)
specific information about the policies and practices they follow regarding their management of PHI. This includes options such as consent directives that patients can adapt to their own circumstances.

Function #4: Review lab results

GENERAL PRIVACY CONCERNS

⚠️ Risks: When patients review their lab results, they need some context (or, possibly, have some previous experience) in order to prevent them from misinterpreting the results. While they have a right under privacy law to access any and all of their PHI, patients should be advised to discuss their interpretation of the results with their care provider. Consideration also needs to be given to whether patients will be able to view interim results or final results only and how version control issues will be managed.

The general risk here is not one of privacy, but rather that having access to this information could create more problems than it solves—unless the results are reviewed with the professional interpretation of a healthcare provider.

🔒 Controls: Unless patients have a good understanding of their health condition, they should they first be educated about the risks associated with having access to lab results. Patients with chronic conditions (e.g., diabetes) should be encouraged to familiarize themselves with the range of results that indicate that their condition is being controlled and, with the guidance of their healthcare provider, to develop an understanding of how they can use the test results to improve their health regimen (e.g., by knowing when to raise or lower their insulin dosage, or adjust their diet).

CONSENT

⚠️ Risks: There is a privacy risk that someone who is not authorized may access the lab results.

🔒 Controls: Patients need to clearly define their circle-of-care and, if they wish, put into place consent directives imposing further limits on access. Patients must also be prudent with any PHI they download.
RISKS AND CONTROLS

LIMITING USE, DISCLOSURE AND RETENTION

⚠️ Risks: The main privacy risk is that test results may be retained beyond the minimum time they are required for the purpose for which they were collected.

 зло Risks: Health information stewards, trustees and custodians, and service providers and other stakeholders (such as patient representatives) must establish sound business rules for how long information will be retained. In some cases, it will be appropriate to keep test results on file indefinitely; in other cases, for only a few days or weeks.

ACCURACY

⚠️ Risks: As in any computerized system that requires some data entry, there is a small risk that a lab result could be entered incorrectly or be corrupted during transmission. As well, there is always the risk that a viewer (whether a patient or a healthcare provider) will view an old lab result thinking it is the most recent one.

 зло Risks: In most cases systems are designed to prevent data-entry errors. To prevent outdated results from being viewed, test results should be clearly identified by the name of the healthcare provider who ordered the test, the patient’s identification (as a minimum, the health number), and a unique identifier for the test, including the date submitted.

Function #5: Messaging

GENERAL PRIVACY CONCERNS

⚠️ Risks: It is not expected that patients will have their patient portal open all the time, but only when they want to view or download their PHI. This means that if a healthcare provider wants to send sensitive information through the patient portal, there is some risk that it may sit there waiting for the next time the patient opens the portal. If PHI is sent to a patient’s general email address or to a phone via SMS text, there is a risk that it could be intercepted by or exposed during transmission. Email can be encrypted, but that requires the decryption routine to be available to the general email program, which poses a possible security risk.
Controls: Consider having the patient portal program being able to generate messages that contain no sensitive information to be sent by Internet to a patient’s general email. These can serve as alerts that secure messages are waiting on the patient portal.

ACCOUNTABILITY

Risks: Healthcare providers are accountable for protecting the privacy of PHI they have collected about patients. They also have a responsibility to communicate information in a secure and timely manner. Circumstances that delay or prevent communications create risk to the care provider’s responsibility of accountability for the system and ultimately for the care of the patient.

Controls: To maintain security but also to address timeliness, implement a system where the healthcare providers or the system generates a message notifying patients as soon as PHI is transmitted to the portal. The message can be sent to a patient’s general email account, Twitter account, or any other account (as identified by a particular patient). The message could simply state that it is from “patient portal,” for example, without any information identifying the healthcare provider who sent the message.

IDENTIFYING PURPOSES

Risks: Patients who receive alerts on a personal computing device, smartphone or other mobile device when in a public place may be tempted to login to the patient portal, and download and view the secure message, which creates a risk of the information being viewed by unauthorized persons.

Controls: Patients should be in control of their own decisions about where and when to view their PHI. It is, however, prudent for service providers to remind patients (perhaps in the alert message itself) that accessing secure messages in a public place may compromise privacy.

LIMITING USE, DISCLOSURE AND RETENTION

Risks: If any amount of PHI is included in a message sent to a patient, there is the risk that healthcare providers may use features such as secure messaging to deliver information to patients that would be more appropriately delivered in a face-to-face encounter.
**RISKS AND CONTROLS**

_Controls_: Using messaging for communicating PHI should be evaluated, and guidelines should be developed. At a minimum, healthcare providers should ask themselves whether they would deliver the information over the telephone. If not, then messaging should not be used; instead, a face-to-face appointment should be set up.

**ACCURACY**

_ Risks_: The accuracy of information being viewed on a portal, such as test results, is at risk of being misinterpreted by patients. Additionally, there may be a risk that the accuracy or version of the PHI could be called into question if there are any vulnerabilities in the mechanisms used to communicate.

_Controls_: Develop clear guidelines to identify which types of PHI are appropriate for delivery through messaging.

**SAFEGUARDS**

_ Risks_: There is a risk to privacy if patients respond to an alert that a secure message is waiting for them and they subsequently view and/or download it to a less secure device and in a public place.

_Controls_: Remind patients of the risks of viewing and downloading in public where security may be compromised. Remember, however, that ultimately the decision to accept this risk remains with the patient.

**OPENNESS**

_ Risks_: There will always be some residual risk involved in PHI being passed from a source to a patient.

_Controls_: The risks should be explained to patients so they are well informed prior to initiating the download. They then can reasonably accept the risks involved.
Function #6: Alerts and reminders

GENERAL PRIVACY CONCERNS

⚠️ Risks: The privacy of any message is at risk of being breached.

🔒 Controls: Develop guidelines for using alerts and reminders. Any message that contains PHI should be communicated only through secure messaging technology (e.g., encrypted).

ACCOUNTABILITY

⚠️ Risks: There may be a risk of a breach if the alert contains PHI that identifies the patient and the alert has not been routed through a secure communications path.

🔒 Controls: Service providers should ensure that rules are documented in guidelines that help those generating alerts and reminders to decide whether they contain identifiable PHI, and if they do, to ensure that those reminders are sent through a secure link.

SAFEGUARDS

⚠️ Risks: Users may trivialize alerts and reminders without recognizing that they may contain PHI and therefore should be treated with the same level of security and privacy as the EHR itself.

🔒 Controls: The functions that permit healthcare providers and others to generate alerts or reminders should include a note to users that if a message contains PHI it is sensitive and should be treated accordingly.

Function #7: Patient education materials

SAFEGUARDS

⚠️ Risks: Patients requesting information or educational materials about a specific condition may communicate to others PHI about themselves.

🔒 Controls: A patient’s access to educational information should be considered no less sensitive than other information associated with that patient, and the portal system should safeguard this information accordingly.
5 RISKS AND CONTROLS

Function #8: Scheduling

GENERAL PRIVACY CONCERNS

⚠️ Risks: The simple act of communication between patients and their healthcare providers is arguably an exchange of PHI. In practical terms, in smaller communities where there may be just one institution delivering healthcare, such an inferred relationship between patient and provider is not likely to be “secret.” This means there is a risk to making routine appointments, as doing so may indicate a health condition—that is, it reveals PHI.

🔒 Controls: Sending information about healthcare appointments through a secure link (e.g., the patient portal) can reduce the risk of others inferring information.

Function #9: Access audit

GENERAL PRIVACY CONCERNS

⚠️ Risks: It is incumbent upon the service provider and any involved healthcare providers to ensure patients or applicants understand the purpose of an audit in order to avoid the risk of being flooded with frivolous or malicious requests. It is reasonable to ask patients to identify any suspicions they have about a possible access breach in order to tailor the investigation. Otherwise, there is a risk of having to respond to trivial questions, which can overload the system and take time away from more serious and valid requests for an audit.

🔒 Controls: It is recommended that service providers produce information sheets that describe the requirements for and the consequences of carrying out an audit. Where requests are either frivolous or made with the malicious intent of keeping the organization preoccupied, there must be recourse by the organization to appeal to a higher body to adjudicate the requests. Typically, this is done through a complaint to the jurisdiction’s privacy commissioner.

ACCURACY

⚠️ Risks: Where patients suspect that an unauthorized person accessed their information within the portal, the service provider must show
interested parties that it can capture and retrieve all information about the access that has occurred. The primary risk is that the service provider will not be able to produce a full set of access records because of circumstances beyond its control (e.g., complexity of locating records from multiple systems to build the audit record).

**Controls:** Service providers may consider having a third party evaluate and certify their auditing practices to ensure a thorough and open process.

**SAFEGUARDS**

⚠️ **Risks:** Access to the audit logs must be strictly limited so that the logs themselves are not at risk of being changed intentionally or inadvertently.

🔒 **Controls:** Only a very limited list of users should be able to access the audit logs. An organization’s support staff may need direct access, but patients and their SDMs must not have such access. As well, any forensic investigative team within the service provider’s organization charged with investigating any possible breaches must do so under a controlled process.

Service providers may need to produce information bulletins that summarize at which points in time systems change and capabilities to track detail at a lower level become available. These bulletins should include caveats about how much audit information was available preceding those system change dates.

**Function #10: Printing and downloading**

**GENERAL PRIVACY CONCERNS**

⚠️ **Risks:** PHI downloaded by patients may not be secure, and computer security may not be sufficient to avoid possible breaches.

🔒 **Controls:** Service providers should encourage patients who are registering on the patient portal to strengthen their own security and privacy protections by publishing best practices and tips on the topic.
5
RISKS AND CONTROLS

ACCOUNTABILITY

⚠️ Risks: The portal owner is responsible for the information until it is in the recipient’s custody. Patients expect that their healthcare providers and service providers will treat their PHI as confidential and be accountable for its security, but patients cannot be expected to understand or be interested in the details of the risk and how it is managed. Patients, therefore, cannot be asked to accept security risks that they may not understand and over which they have no control.

🔒 Controls: Service providers should publish a policy and make it available to the patient (perhaps at the time of registration on the portal) that maps the flow of information from the sources to the portal and onto the patient’s environment, and that clearly shows the point in the flow at which the responsibility transfers.

ACCURACY

⚠️ Risks: There may be risk of patients relying on downloaded PHI without understanding that it is valid only for that particular point in time and will be out of date as soon as another update modifies their information in the portal.

🔒 Controls: Service providers should produce an information bulletin that describes this scenario to patients and clearly explains that all PHI on the portal is time sensitive. Dates and time-stamps should be prominently displayed on all data, indicating when the information was last updated.

SAFEGUARDS

⚠️ Risks: Custodians and service providers of PHI are legally responsible for providing appropriate safeguards (physical, logical, administrative) for the PHI in their custody. When patients cannot provide the same level of protection for PHI that is passed to them through the patient portal, there is higher risk of a privacy breach occurring.

🔒 Controls: Patients must accept their responsibility for protecting information from the time of receiving it. Service providers should encourage patients who are registering on the patient portal to strengthen their security and privacy protections. They should publish and provide best practices and tips on how to improve their protection.
Function #11: Chronic disease information

GENERAL PRIVACY CONCERNS

⚠️ Risks: A chronic disease management portal serves patients that are generally more concerned about their health and more active in their own care. Often this heightened concern overshadows any worries about privacy and security, increasing the risk of privacy breaches.

🔍 Controls: This population may require a greater degree of security education, rather than less.

View-Only Patient Personal Health Information

A view-only portal is one that is designed to connect patients with their PHI and allow them to download all or part of the information. Using a view-only portal, patients may be able to see any of:

- Their own PHI from their EHR/EMR record
- Information that their healthcare services provider wishes to send to them (e.g., notes about a test result, reminders of an upcoming appointment)
- Educational material about health conditions and pertinent treatment regimens

For a review of risks and controls concerning view-only portals, see the discussion above for Functions #1 through #11.

Access and Enter Personal Health Data

In addition to offering access to PHI, patient portals allow patients to enter information from sources other than their primary care physician (e.g., blood pressure, weight, glucose readings from other sources). As well, through a portal, patients can securely communicate with their primary care physician, specialist or any other caregiver, provided that they are all linked to the same patient portal.
The feature allowing patients to enter information increases the level of responsibility needed to ensure that security and privacy issues are recognized and addressed. While patients are not the focus of this document, it is important to note that before patients are given access to any tethered portal they should be offered portal training and even required to be accredited. Patients should be provided with a list of what they could or should look for in a portal before committing to using one. Patients should also understand the implications of having a proxy or SDM.

The portal offers an excellent opportunity to offer training to patients in the form of short e-learning exercises that provide meaningful examples and that test their understanding of personal accountability. The e-learning could form rudimentary accreditation, without which a patient is not permitted to use the portal. The intent of such e-learning should not be to exclude participation; rather it should educate and enable patients to make informed decisions about what information to share, and with whom.

**Additional Function: Entering information from other sources**

This function allows information that has come from a variety of sources to be entered into the patient portal. A system that allows patients to enter and manage their own data changes the nature of the risks and the controls required.

**ACCOUNTABILITY**

⚠️ **Risks:** Patients must be made aware of their own responsibilities when using portals. If they do not acknowledge this responsibility, or if they believe responsibility and accountability are in the hands of others, data protection can be compromised.

🔒 **Controls:** Implement a user agreement or disclaimer so that patients understand the implications of entering information into the portal and accept that they have a responsibility to protect their own privacy.

**IDENTIFYING PURPOSES**

⚠️ **Risks:** Misunderstandings may arise about how clinicians will use information, which could result in gaps in patient care.

🔒 **Controls:** Healthcare providers should make clear to patients how information will be used. For example, doctors should state whether
they will review and comment on any information entered within a specific timeframe, or whether they will review it only at the next face-to-face meeting.

LIMITING USE, DISCLOSURE AND RETENTION

⚠️ Risks: Many people are responsible for the continuing treatment and care of other individuals, and information may be entered by people other than the patient. For example, if a patient has authorized a proxy, that person may have access to the portal and enter important data. Whenever other people have access to the portal, there is increased risk of privacy breaches. In order to judge if access is appropriate, both patients and providers must know who is authorized to access the information, when it is accessed and for what purpose.

🔒 Controls: Healthcare providers must be aware that proxies may be entering information and communicating through the portal. The actions and identities of proxies should be recorded. The patient portal should provide an audit log of who has accessed what information. Ideally, an audit log will also track where information has been updated and changed. It should have full auditing capabilities to capture all access to any data. Patients should be aware that they can change their mind at any time and opt to disable their portal account. Steps should be taken to educate everyone involved on notification of use, consent models and the scope of access.

ACCURACY

⚠️ Risks: It is important to be able to verify the validity of the data. When information is transferred directly from a patient’s home, the physician and patient should agree on the suitability of the device being used in order to be certain it produces accurate data. Risks to accuracy can result in risks to patient safety.

🔒 Controls: Clinicians should verify with patients how health information will be added to the patient portal system—whether it will be entered by patients directly, by someone on their behalf, or by a direct feed from a particular home care device or system. Any information entered directly from point-of-care systems (e.g., hospitals, labs, home care systems) should not be modifiable in any way.
SAFEGUARDS

⚠️ Risks: If patients are not aware of the safeguards in place that help protect their health information, or if they do not agree to uphold the safeguards that are controlled by process and policy, the portal itself, including the data it holds, may be at risk. Before using the patient portal to communicate with the patient, healthcare providers should verify with patients the email address associated with the clinical portal to ensure a secure communication link. Other email addresses should not be used.

🔒 Controls: Safeguards include administrative, technical and physical means of protecting data confidentiality, integrity and availability while enabling information to be shared appropriately. Legislation and policy set out the means to protect health information and personal information when used by providers. However, legislation cannot conceptualize how a patient interacts with health information and how a patient and provider should use information during an encounter in the portal environment. The technical capabilities of the portal must establish appropriate boundaries for patients entering information and the subsequent uses of that information by providers. For instance, it may be preferable from a provider’s perspective to limit the type of information that a patient can share. Prescribed formatted forms of data offer a better source of information than does a “blob” of unstructured text in an email. Other standard, administrative, physical and technical safeguards must be included, such as refreshing passwords, verifying identity and encrypting messages.

The healthcare provider should verify that the patient portal has the necessary controls in place to address the risks identified in a security threat and risk assessment. The portal should have a robust process that assigns unique IDs to patients, and it should allow users to set their own passwords that cannot be read by anyone else. Before granting permission to access and enter information in a portal, it is imperative that the identity of the individual be verified. Patients must have some means to authenticate their identity. The portal should also have a secure email or other secure messaging system that encrypts communication between the user and the system and all stored messages.

Transmission of data from home care devices must be by a secure link using encryption. The portal must have a mechanism in place to ensure that the information being transmitted is from a secure source.
and is linked to the correct patient. Finally, patients should be made aware of conditions of appropriate use of communications and what will, and will not, be accepted via email.

Patient Care Plans: Putting the Focus on Patients

Over the past several years the healthcare model has shifted away from the traditional visit to the doctor by a compliant patient to a patient-centric environment with a focus on education and disease prevention. Patient portals are a key aspect of this modern healthcare model: they provide a tool for patients to access reliable, secure, commercial-free information, and, more importantly, they serve as a framework for patients to monitor changes in their health status.

As with other aspects of patient portals, patient care plans must address privacy and security concerns. For example, healthcare providers may wish to use a portal to identify those patients who may benefit from advice on weight reduction, or to encourage suitable candidates to undergo a Pap smear or colonoscopy examination. But it is important to make sure such profiling, and so-called churn analysis, cannot be performed for commercial services or used to negatively impact patients (e.g., by restricting employment or insurance coverage).

Additional Function: Simple participative care planning

This function allows patients to make decisions about their care, in collaboration with their care providers.

GENERAL PRIVACY CONCERNS

⚠️ Risks: Placing sensitive patient information on a portal creates risks to use and disclosure. It can also lead to accountability risks if it is not clear who has the control responsibility for the data (i.e., who is accountable for protection, use and disclosure).

🔒 Controls: When patients are shown healthcare plans that providers have devised for them, the portal is expected to pass at least three acceptance tests to be considered secure and safe for deployment. First, it should not be possible for anyone other than patients themselves
and their providers to see the plan, without explicit patient consent. Second, patients should be able to revoke an assignment from anyone at any time, and to disagree with the plan and stop it. Third, any third party using planning information for research or future design should not be able to trace it back to a patient and should only be able to indirectly access a healthcare provider through a governing party of the portal (i.e., the organization that is legally considered the collector of the information and that has control responsibilities for it). The governing body may be required by law to provide some level of notice, or solicit consent from the patient to provide such service.

SAFEGUARDS

⚠️ **Risks:** Services cannot be provided in the absence of information. Information must be available if a patient is relying on the portal system for a service. Risks to availability can be created through intentional disruption or destruction of the system and/or service, or through unintended actions and errors.

🔒 **Controls:** Robust security must be applied. Security controls should be based on a comprehensive and professionally applied threat and risk assessment.

**Additional Function: Active participative care planning**

This function allows patients to make more decisions about their care in collaboration with their care providers. At this level, the portal actively makes suggestions about healthcare based on personal criteria of patients (e.g., gender, age, history, current medical problems) to promote disease prevention.

While there are many benefits to this functionality, including increasing the likelihood of patient compliance and participation in preventive initiatives, there are also increased privacy and security concerns.

**CONSENT**

⚠️ **Risks:** Individuals may have the right of consent to have their information used for some purposes, such as research. This, however, varies from jurisdiction to jurisdiction. For example, where data is used for research, that use should be explicitly stated so that patients can exercise their rights of informed consent. Without adequate information,
the consent may be weak or even invalid and could compromise the research itself if a patient later protested.

**Controls:** Information must be used for explicitly stated purposes only. Consent must be obtained by fair means, and patients must be able to revoke consent at a later date and have it refreshed as needed.

### LIMITING USE, DISCLOSURE AND RETENTION

**Risks:** If legislation and policy requirements governing information use and permissions are not complied with, privacy may be breached. This might happen, for example, if a university were permitted to look at plans for diabetic patients using a portal hosted by a health authority.

**Controls:** Researchers should never be allowed to contact healthcare providers directly. However, a health authority can randomly assign an identifier and contact the provider on behalf of the researchers. The engine that finds and selects the appropriate candidates should be entirely closed, not only to the outside world but also to the governing party of the portal.

### ACCURACY

**Risks:** Without proper controls in place, there is a risk that data could be changed or removed without leaving a trace.

**Controls:** To satisfy the basic requirement of guaranteeing the integrity of the information, the system needs to ensure that no part of the data can be changed or removed without authorization or without maintaining a protected record of those changes.

### Additional Function: Fully active participative care planning

This function allows patients to supply information directly to their care providers through the portal and to provide feedback on their experiences. Such feedback can be very helpful in adapting the care plan to the patient.

### GENERAL PRIVACY CONCERNS

**Risks:** Where there is active patient input and feedback to the care provider, there is always a risk of misidentification, hacking or spoofing.
RISKS AND CONTROLS

Controls: A high degree of confidentiality and integrity is required. A full threat and risk assessment should be carried out and the identified risks mitigated.

IDENTIFYING PURPOSES

 Risks: Based on clinical recommendations, a program can refine care plans based on results. If there are abnormal results, the program may suggest that the care provider be notified. Where the portal is governed by a health organization, an abnormal result can be verified, effectively eliminating the risk of human error on the patient’s part and removing any risk to accuracy of information.

Controls: Patients and care providers must understand where their decisions are applied and where decision support algorithms are used. Both patients and providers must be able to modify or override decisions or recommendations made in software.

SAFEGUARDS

 Risks: Because patients are actively involved and will not have the same degree of training and understanding of the implications of information they provide, there exists the potential risk of collecting inaccurate or incomplete information, which could negatively affect patient care.

Controls: The portal software and the decision support algorithms must be free of risk of error in their conclusion and applied actions. Rigorous acceptance tests must be carried out. The portal should have a strong authentication mechanism to confirm the identity of the patient. It should also have built-in checking to eliminate data-entry errors, and it should guarantee that the results are restricted, as appropriate.

View Scheduled Appointments

Scheduling is one of the most commonly requested functionalities of patient portals. Consequently, it has received considerable attention and analysis. At its most basic level, a scheduling module provides some sort of calendar service that notifies patients of scheduled appointments. Providers
and patients can negotiate the time and place by other means (e.g., by telephone or during face-to-face visits), after which the portal is updated by the provider or a staff person for the patient to view.

Additional Function: Simple scheduling and reminders

This function allows patients to view reminders, which may range in complexity from notices that are displayed when patients login to emails to automated telephone calls to text messages.

GENERAL PRIVACY CONCERNS

⚠️ Risks: There is always a risk this information can be tampered with if a system is not in place to ensure the authenticity of the appointment and its source.

🔒 Controls: The portal must employ an authorization protocol that guarantees that the entity has, in fact, the privileges to make the appointment or change a record. It is imperative for the portal to have a logging mechanism to record who did what and when. Such a mechanism is referred to as “triple A,” which stands for Authorization, Authentication and Accounting.

If patient reminders are used, it is imperative that the portal engine has safeguards in place to make sure that the reminder is delivered to the patient only. It is not acceptable to make an automated telephone call that may then be answered by someone else at the patient’s residence and therefore disclose confidential information.

LIMITING USE, DISCLOSURE AND RETENTION

⚠️ Risks: The portal must ensure that an appointment record is viewable only by the parties who are directly involved (i.e., provider and patient). To do otherwise risks inappropriate use and/or disclosure.

🔒 Controls: If third parties wish to “consume” the records (in other words, to integrate them), for example to research the workload of centres in an area, they must only do so in a manner that protects the identities of both provider and patient, and so that churn analysis and profiling are not possible. Health authorities, universities and other research and administrative organizations that wish to use the data, for example to study workload and utilization of MRI centres under their coverage, should use their own systems and not be allowed access to a patient
portal. If such data is needed from the portal, then the availability is subject to laws and policy that govern such disclosure and use.

**Additional Function: Complex scheduling**

This function assists patients and providers to schedule tasks, where portals actively pull data from different providers to show the availability of services, and then allows the patients to choose. The portal should be able to provide the wait times for various diagnostic tests by facility, which will then help providers and patients to find the appropriate time and place for the test. The portal must ensure the timeliness of the data and avoid conflicts or double booking.

**GENERAL PRIVACY CONCERNS**

⚠️ *Risks:* A general risk of confidentiality exists with this search function.

🔒 *Controls:* Identification, authentication and authorization must ensure that only authorized users can view the information. There should be no way for an unauthorized party to find out which patient is looking for which service.

**SAFEGUARDS**

⚠️ *Risks:* Since the patient is relying on the appointment, it is imperative that the system be continuously available, or an alternative route be provided at all times. Any risk to availability from intentional or unintentional service interruption must be identified and addressed.

🔒 *Controls:* The availability of the system must be ensured. Security must be routinely applied to address confidentiality, availability and integrity issues, based on security threat and risk assessments.

**Additional Function: Complex scheduling including inter-provider relationship management**

Patient portals can include additional functionality for inter-provider relationship management. A common example is a healthcare provider completing pre-consultation forms and attaching them to the request for appointment when referring a patient to another care provider. This functionality supports scheduling optimization. The waiting list that the patient is on is managed by a software engine that tries to match the patient
to the most conveniently available time or place for the service to be carried out. Known as “service matching,” this demands a complex engine that calculates a score indicating the convenience of each recommendation.

**GENERAL PRIVACY CONCERNS**

⚠️ **Risks:** A service this complex can have a high degree of unpredictability, making it vulnerable to privacy and security threats.

🛡️ **Controls:** A vigilant review of the mechanisms in place and a minimum acceptance criteria selection go a long way to making certain that a safe and reliable service is provided. A two-level transmission can be applied in which both parts of the record are encrypted: the first level contains just enough information to triage the patient and make the appointment, and the second portion is detailed enough for the two providers to collaborate. The receiving physician should only see the patient information that is necessary and pertinent to the care being provided. As well, the portal must make sure that the receiving service that is being queried has no more data than it needs to triage the patient, and that the patient cannot be identified.

**Financial Transactions**

Because Canada’s healthcare system is publically funded, the idea of using patient portals to make payments is generally not considered. However, some healthcare services are not covered by provincial plans (i.e., uninsured services), and portals can also address the payment function.

**Additional Function: Fee-based patient portals**

This function is used by those using fee-based services such as private primary care, nursing and self-management services.

In the past, some large software provider companies hosted personal health record systems on the “cloud,” independent of any physician or healthcare institution. PHI was meant to be entered by the client and a number of third-party services were offered, often on a fee-for-service basis. In these cases the developers promoted making these services fee based. In many cases, the business model was not feasible. Patients expressed
RISKS AND CONTROLS

Concerns about the privacy and security of their PHI, and there were questions about the regulatory and legislative feasibility of hosting these services on the cloud. Many of these services are now either free or have simply ceased to be available.

However, physicians and healthcare institutions can offer, or even prescribe, patient portals that are largely controlled by patients (integrated portals). Patients can choose to make PHI accessible to various circles-of-care including family members, primary care providers and hospitals. The usual payment model is a monthly subscription fee.

Provincial governments have recognized the value of integrated patient portals and have proposed either provincial architectural solutions or regional health models for patient access. The security and privacy of these systems are greater than with standalone systems because the PHI is more tethered to the provider, primary care team or health institution.

GENERAL PRIVACY CONCERNS

⚠️ Risks: Variation in design, functionality, approach and operator perspective can lead to confusion for the patient-user and a lack of understanding about how to interact with the software. It can also lead to variability in managing the software.

🔑 Controls: Organizations that implement and operate portals, including vendors, should ideally be moving toward interoperability. By adopting available interoperability standards such as HL7, vendors can ensure that consistency of design and operation supports overall security design.

Additional Function: Payer-tethered fee-based portals

This function is more widely used under private healthcare systems where individuals pay directly for services. Not only are patients given access to their PHI through a secure portal networked to their healthcare provider, they are also able to look at payment schedules and make secure payments. As well, insurance companies are increasingly offering patients electronic access to their records and the means to submit claims and be directly reimbursed.
GENERAL PRIVACY CONCERNS

⚠️ Risks: With this function, both sensitive health information and financial information may be available, which can be attractive to fraudsters. Consequently, there is an increased risk of malicious attack to obtain data.

🔒 Controls: As with any financial transaction system, full security of confidentiality, integrity, availability, traceability, auditability and accountability must be built in.

Additional Function: Provider payer patient portal

There is a growing trend toward remote home-monitoring services, and many private primary care and nursing services are leading these initiatives on a payment basis. Smartphone, Bluetooth and wireless integration of medical devices with patient portals allow patients to pay directly for healthcare services. This option is particularly helpful in the self-management of chronic disease, but it is also used by sports therapists, sports trainers and rehabilitation services.

Private billing of uninsured services is possible in many jurisdictions with direct payment through third-party insurance. These services include e-prescribing and pharmaceutical renewals.

GENERAL PRIVACY CONCERNS

⚠️ Risks: With this function, both sensitive health information and financial information may be available, which can be attractive to fraudsters. Consequently, there is an increased risk of malicious attack to obtain data. The availability of greater quantities of health information can create greater risk if it indicates an increased level of patient vulnerability.

🔒 Controls: As with any financial transaction system, full security of confidentiality, integrity, availability, traceability, auditability and accountability must be built in. Appropriate legislation must be applied. Care should be taken to ensure that there is no expectation of care, and that patients understand that the system is for administrative and financial services support only.
5 RISKS AND CONTROLS

General Health Information

Health information is one of the most popular topics for Internet searches, but search results are highly subjective and may not be relevant to the individual looking for specific information. As well, privacy and confidentiality principles cannot be easily applied to general health information on the Internet. However, once an individual has logged into a portal with a username and password, any searches can be subject to privacy guidelines. The access to information provided by a portal is designed not only to provide credible medical information, but also to customize the health information search to the identified individual.

Additional Function: Consumer health informatics

There are a number of websites that provide open and accessible health information for the public. Some of these also offer the option of downloading or subscribing to patient portals or standalone personal health record systems.

GENERAL PRIVACY CONCERNS

⚠️ Risks: There are several general privacy risks to this function:

1) If individuals search health information from work, their searches will likely be logged. Most portals do not protect health information with SSL connections, which means that an individual’s health concerns may be disclosed to the employer.

2) As wireless information communication and technology systems are developing very rapidly in the healthcare domain, patients should be aware of how their PHI is being transmitted, stored and archived. Where large amounts of data are available, it may be tempting to store everything. However, data that is not needed creates a confidentiality risk and so should not be collected. Although not all data may be useful, data from monitoring devices that integrates with smartphones and patient portals can be valuable. Tracking trends, historic data points or messaging trigger points is becoming increasingly important. It is therefore important to determine the value of all information before a decision is made to collect and store it.
3) Increasingly the Internet is being used to search for information on fitness, exercise, diet and wellness. For instance, mobile devices are being adapted to track personal performance levels. Sometimes these devices can be integrated with patient portals, consequently giving rise to privacy and security concerns. Organizations offering these applications, especially those that do so for no charge, have little incentive to provide details on how they intend to use the information collected.

**Controls:**

1) Employees should know and understand the risks associated with the location from which they search.

2) Dynamic data feeds can be set up within or outside of a patient portal and do not present many privacy or security concerns. In the case where patients have a condition or disorder that they want to keep private, they need to take the precaution of setting up their RSS feed on a dedicated and private computer. Encrypting PHI on smartphone wireless networks is a precaution most IT departments or companies are willing, if not obligated, to take.

3) Typically only trend data needs to be stored. Those portals that are dedicated to tracking diet and exercise behaviour do not require as much security as those requiring maintenance of medical records.

**LIMITING USE, DISCLOSURE AND RETENTION**

Many large organizations, including the military, are increasingly offering portals for secure maintenance of PHI. For example, Dossia and Keas are portals funded by employers that allow their employees to track their own personal health measures while maintaining privacy and security of that information. Corporations also track the Internet-searching behaviour of their employees.

**Risks:** Large amounts of personal data can be a target for identity theft. Also, large companies can be a target for disgruntled members of the public.

**Controls:** Searching for health information at work on open and accessible sites should be done with caution.
5 RISKS AND CONTROLS

SAFEGUARDS

⚠️ Risks: Some organizations, such as online advertising agencies, may track web-surfing habits to a particular identity. Some web surfing on smartphones can be linked to location-based services in the same device.

🔒 Controls: These types of issues are largely outside the control of portal providers, but users should be made aware of the risks.

Additional Function: Trusted health information on the Web

This function allows patients to search for information that has been professionally vetted for accuracy and credibility. For example, electronic medical journals and other publications are now available online through PubMed, Medline and Elsevier. Many of these journal search sites will provide information on clinical research and evidence-based medicine. They are often highly technical and academic in nature and are not targeted for the general public. As well, websites operated by associations of medical practitioners and health ministries are popular. One way a consumer can determine if a website is trustworthy is by looking for the Health on the Net (HON) logo. The HON Foundation has created this logo to verify the reliability of information.

GENERAL PRIVACY CONCERNS

⚠️ Risks: Many consumers looking for health information use popular search engines such as Google, Bing and Yahoo, which generally lead them to Wikipedia, which may not be reliable. Even attempts to measure reliability for consumers are not risk-free. For example, the HON logo is not widely used, and the HON Foundation lacks power to enforce compliance on websites where the logo is displayed. (See http://www.jmir.org/2000/1/e7/.)

🔒 Controls: Until credibility can be guaranteed for medical information on general sites such as Wikipedia, patients should be discouraged from using them. The portal must be able to provide evidence-based medical findings in terms an average consumer can understand. Further, patients should understand the limitations of relying on the HON logo. Patients should also be referred to the Canadian Medical Association’s proprietary patient portal (mydoctor.ca) for their ongo-
ing treatment and care, as it offers a model of trust and privacy for the patient’s PHI. This site can also be linked to the EMR.

**Additional Function: Public health informatics**

Information and alerts on public health issues, which are generally public data sources, can be subscribed through a patient portal. Individuals who maintain a personal health record can customize their portals to receive alerts on influenza or other disease outbreaks. PHI in a personal health record is potentially a great source of knowledge generation for health research. Data on everything from clinical trials, longitudinal studies of aging, immunization records and even genomic research can be accessed through the PHR.

Maintaining records in a patient portal is a practical way to track and share records for disease prevention. Some public health offices, frustrated by the data silos across their various domains, are moving toward making records electronic. Having this kind of information available in case of a pandemic could benefit efforts of control and prevention. Immunization data self-reported in patient portals, or actual data integrated from the EMRs, can serve the same purpose.

**GENERAL PRIVACY CONCERNS**

⚠️ **Risks:** There are several privacy concerns with this function:

1) Some medical record systems visually display influenza-like illness outbreak trends by combining area codes and disease incidents with geographic information systems and web services. This data allows public health officials to view real-time tracking of health conditions and disease outbreaks. But this information also increases the risk of patient data being exposed.

2) Physicians have a duty to inform public health officers of certain legally reportable diseases, but patients who are used to maintaining their own PHI record may feel that their privacy rights are being compromised.

3) Many people are willing to have their PHI used for research, but just as many are concerned about the privacy and security of their health information being used.
CONTROLS:

1) Patient data must be strictly controlled and limited to users who have authority to review disease patterns in an individually specific and identifiable way. Such functions and analysis of data should not be made available except to a narrow set of authorized individuals under a duly constituted and controlled public health program.

2) Patients need to be given a valid and effective notification process to explain when, how and under what authority information can be disclosed for public health reasons.

3) While legislative and research ethics principles that govern the consent for using PHI for research must be adhered to, and while they vary from jurisdiction to jurisdiction, the PHR promises a more integrated approach for giving informed consent. Although PHI can be safely depersonalized, both legislative and ethical requirements for consent for the use of information for research must be adhered to.

Additional Function: Online health and wellness social support groups

The open, interactive, and collaborative nature of social networking on the Internet extends into many areas of healthcare, changing the traditional patient visit to the doctor’s office to a virtual clinical point-of-care interface. One example is an online patient discussion group with access controls and a definite expectation of privacy. This access might be granted only through the patient portal authentication level. The discussion is moderated by credentialled health practitioners who lend support when needed. Similar functions are used in clinical trials involving patient portals when data submitted by participants is triaged by a nurse or trial coordinator for any signs of clinical significance that may require reporting.

GENERAL PRIVACY CONCERNS

Risks: The privacy settings in many non-healthcare devised social media forums are ultimately in the hands of the individuals who use them. Many users do not perceive any risk and do not understand the controls needed to protect privacy.

Controls: Ideally a healthcare practitioner or perhaps a patient advocacy group will work with patients to help educate them on the use of
social media and online discussion support forums and any expectations of privacy in the online world.

Manage Access and and Consent

The power of a PHR or portal is not only its ability to enter and retrieve data from an EHR, but also to customize and manage individual experiences. If the PHR is a standalone system, managed and owned by the client and not interacting with a broader system, then the protection of the data is in the hands of the individual and, therefore, some of the CSA Model Code principles will not apply. However, if the application is hosted by a private or a public healthcare organization, and certainly if the information can be intelligently mined to produce health-related communications, then there are risks that patients should be aware of. These integrated functions are the focus of this section.

Additional Function: Communication preferences

This function provides services to uphold patients’ wishes to receive health information communications from the portal hosting organization, family proxies, care providers or care facilities with access to the portal. It refers to a portal’s ability to be supported by various mobile devices and to interface with various health products in order to download health information directly.

⚠️ Risks: See above risks for Function #5.

🔒 Controls: See above controls for Function #5.

Additional Function: Set access

This function encompasses access control and consent management. Access control services are meant to ensure that health information is available only to identified and authorized users on a need-to-know basis. Common models include role-based access control (based on either the care provider’s specific role in the healthcare system or in the client’s circle-of-care) and work group–based access control (based on the care provider’s association with a group or delegated access where an individual has authority to grant access to another user).
Consent management services relate to recording, managing, applying, logging and/or overriding a client’s specifically outlined information sharing directives. The most commonly used consent models are those of implied consent and express (or expressed) consent:

- **Implied consent** is the voluntary agreement with what is being done or proposed that can be reasonably determined through the actions or inactions of the individual.
- **Express, or expressed, consent** is the voluntary agreement with what is being done or proposed that is unequivocal and does not require any inference but does require rigour in its implementation.

In every case, implied or express consent requires that the patient be informed, which means that the patient knows or should have known what would happen. If the consent model does not inform, it is invalid.

Another consent model is *deemed consent*, where in the context of a statutory requirement the patient does not need to actively consent but is deemed by the data collector to have done so. In this case, organizations are permitted to behave as if the individual has consented and there may or may not be any right to withhold consent.

⚠️ **Risks:** If organizations do not actively and clearly define their consent model and meet its requirements, they risk relying on policy and process that does not meet ethical and/or legal requirements and having their actions challenged. The risk can reach legal proportions and result in shutting down programs or research initiatives.

🔒 **Controls:** Organizations must fully understand the consent model they choose and implement it accurately and comprehensively. A large volume of information is available on consent models and their associated requirements from privacy commissioner offices, research bodies and legal resources.

### Additional Function: View client rights and privacy information

This function includes those services and information provided to the individual by the responsible data steward or trustee to uphold privacy rights under the CSA Model Code principles. This includes a statement of accountability, descriptions of permitted purposes of use, descriptions on limits to collection, use and disclosure, descriptions of retention times, statements relating to appropriate security of data, statements of openness including health information management policies, individual access to
information including knowledge of who accessed the data (secure access audit) and, finally, the patient’s right to challenge the compliance of the organization with laws, ethical requirements and privacy principles.

ACCOUNTABILITY

⚠️ Risks: The principle does not apply if the data is only in the hands of the individual to whom it refers. However, if the system is hosted by any other party, or is operated by another provider organization such as a health authority or hospital, or if the PHR is part of a larger healthcare system and bi-directionally shares information with an EHR or other healthcare providers or government, then accountability becomes important for both legal and practical reasons. The risk of conflict increases where patients can see and interact with their own data.

🔒 Controls: The hosting organization must identify a person responsible for ensuring that the privacy principles and legal requirements are complied with and that appropriate privacy policies and training are in place. Where the PHR or portal is part of a larger interoperable EHR, effective governance and ethical and legal responsibility requires clearly articulating accountability through possible information sharing agreements, setting minimum standards, fully elaborating on policies and procedures and objectively measuring compliance. Patients can control some areas of access such as determining who can access their portal and even the granularity of access. This is different from traditional provider-driven models and changes the way healthcare is delivered, and it should be carefully implemented.

CONSENT

⚠️ Risks: Where the PHR or portal is part of a larger and integrated EHR, and therefore accessible not only by the individual but also to providers, healthcare organizations and persons within the individual’s circle-of-care, it is important that whatever consent model is chosen be fully and accurately implemented so that patients know who can see their data and no misunderstandings occur.

🔒 Controls: Consent is a complex and multifaceted subject; it must be applied to patient portals using the same concept and foundation policy as is used to share information in traditional ways. Patients should
be able to withhold or withdraw their consent for the collection, use or disclosure of their PHI in accordance with applicable privacy legislation. For example, if permitted in legislation, an individual could restrict access to, or disclosure of, specific health information such as HIV status or mental health records. It would be beneficial if patients could express their consent intention for the EHR through the patient portal at least where the portal links to the EHR.

**LIMITING COLLECTION**

⚠️ *Risks:* Care must be taken to limit information to the purposes that have been justified and identified to the individual.

🔒 *Controls:* The hosting or collecting organization must state the purposes for data collection by the organizations responsible for the specific collection. Where an organization hosts the portal, it must be clear about its use of any of the available information. This must be articulated in administrative controls such as use agreements, describing terms and conditions that apply to individual’s access to, and use of, the PHR.

**LIMITING USE, DISCLOSURE AND RETENTION**

⚠️ *Risks:*

1) While health information is recorded in patient records, it may also exist in other types of records including financial records (e.g., insurance claim records or patient payment receipts).

2) Sensitive information stored by the hosting organization, such as client email addresses and medical profiles, may be vulnerable.

3) Individuals are often concerned about who has accessed their records. Often it is only the patient who can recognize an inappropriate access, such as access by a neighbour who is also a nurse in the care provider’s organization.

🔒 *Controls:*

1) The hosting organization must limit the use of the information to those stated in consent agreements, or obtain consent for new purposes unless that purpose is required by law. Health information should be retained only as long as necessary to fulfill those purposes.
Care must be taken to ensure that federal and provincial legislation is explained and best practice guidelines are available.

2) An organization hosting the PHR or portal, whether or not it has any permitted use of or interest in the data, must retain it securely and uphold the security goals of confidentiality, integrity and availability according to accepted industry standards and regulations.

3) The access control services, if implemented appropriately, ensure that health information is available only to users with an identified need-to-know in the context of a care relationship. The model most likely supported by a PHR is delegated access, which allows authorized users to nominate someone else (a delegate) who they feel also requires access (e.g., a family physician). For example, the family physician who has access could delegate access to a specialist to whom the client is being referred.

4) Audit logs must be defined to collect meaningful information and to maintain it securely so that there can be no doubt about its integrity and availability if it is needed in an investigation. Audit logs should not contain any personally identifiable information. If they do they too must be protected. Rather, audit logs should contain only metadata that allows the information to be linked to the identifiable information.

5) Secure auditing allows the portal system to record significant privacy and security related events such as access or changes to the record. Sophisticated systems include logging events and analyzing activities related to access and use of the system, including changes to data and denial of access. They also enable patients to see who has accessed their PHR and record the activities of proxy relationships.

SAFEGUARDS

⚠️ Risks: If client profiles are made globally available in a searchable directory, there can be a risk of identity theft or breach of confidentiality. In other words, other clients or providers may know about and reach out to individuals. As well, it is becoming increasingly necessary to consider the issue of the care provider as a proxy. In the case where all proxy accounts show up automatically when patients open their portal, the risk to confidentiality can be higher (e.g., a general practi-
tioner opens his or her portal on a home computer, and it displays the client portals).

Control: Where the email address is used as the unique account login identifier, to remove a confidentiality risk, the PHR should include an optional secondary email address for other users to communicate with the individual. Otherwise, it is not recommended to use the email address as any part of the login identification or authentication. Also, physical safeguards should be implemented, such as using computers in secure locations to minimize the risks of modification, loss, access, theft, view and disclosure by unauthorized individuals.

CHALLENGING COMPLIANCE

An individual must be able to challenge the organization’s implementation of ethical and legal requirements of information management. If the organization being challenged is a public body, the individual need not be a client or patient of the organization but may simply be a citizen.

Risk: In an integrated system such challenges may increase as the information becomes available beyond the traditional walls of a care provider. Challenges to information management policy, uses, disclosures and security or protection can also have non-constructive motives. This can put the organization at risk of public criticism if it does not have a privacy program that is prepared for public challenges.

Control: While the detail is beyond the scope of this document, meaningful, understandable, and applicable policy and procedures must be available to the individual to whom the information refers to ensure that these individual rights are upheld.
Setting Up Your Patient Portal

When setting up a patient portal, there are a number of important factors to consider. These are summarized in the lists of questions below, organized into five different categories: clinical, technical, legal and regulatory, administrative and operational. Carefully answering each of these questions will serve your organization well during the set-up process.

Clinical Considerations

- Is the clinical content (knowledge, information, data, vocabulary, etc.) and emphasis of the portal correct and kept up-to-date relative to expected norms within the Canadian medical community?
- Is medical educational content created, updated and distributed in a manner that demonstrates a proper duty of care?
- Do the clinical processes expressed in the portal align with those of the medical providers and organizations that may be interacting with the patients through the portal?
- Have representative clinical providers and targeted users been engaged in and approved the definition, design and development of the portal?
- If information is shared from medical professionals, are technical terms and medical jargon defined and/or translated for the lay reader?
Technical Considerations

- Which tools will patients be using to access the patient portal services? Each type of access tool has its own specific security strengths and weaknesses that must be evaluated individually (e.g., computer web browser, mobile web browser, mobile app, iPad/Android/Blackberry, computerized patient kiosks).
- Have all crucial technical standards (e.g., messaging protocols) been adhered to?
- If the application is web based, is it regularly scanned for vulnerabilities?
- Is the browser supported?
- Are there any potential incompatibilities in the technology selected and the browser used?
- Does the PHI stay within the portal? Or can it be downloaded or shared with a hospital-based or physician practice-based electronic chart?
- How is the transfer of information and authentication managed?
- What type of monitoring is conducted to ensure the availability of the service?
- Have technologies been chosen that will limit the types of tools that can connect to the portal (e.g., Flash, which isn’t supported by iPhone/iPad devices)?
- Have the technologies that support the portal been chosen so that they can meet the confidentiality, availability, scalability, support and information integrity requirements of the portal over its life?
- Has the portal been evaluated for usability by a wide range of users (e.g., seniors, youth, non-English speakers, patients with disabilities)?
- Are audit logs properly kept across a range of places to support a potential forensic investigation in the event of a security incident?

Legal and Regulatory Considerations

- Where is the patient portal hosted? (If the portal is hosted outside of Canada it may not have the same legal privacy protection or support for individual rights as what is available in Canada. Information may be subject to access by foreign governments.)
- Are physicians eligible to charge patients for the service? (Restrictions apply in some jurisdictions.)
• Does your jurisdiction have specific healthcare privacy legislation and breach reporting requirements, or is the relevant legislation based primarily on requirements for public versus private organizations?
• Does your jurisdiction have specific legislation related to people with disabilities?

Administrative Considerations

• What are you trying to achieve (e.g., cost savings, self-service, higher satisfaction)?
• Are the strategic goals and objectives of the portal feasible, advisable, doable and deliverable given the interventions attempted through the portal (i.e., does the portal motivate users to behave in the desired way)?
• Have policies been developed and promulgated related to alterations in the portal purpose, goals, objectives, deployment, usership, operation, access, evaluation, backup and recovery?
• What do patients want and why would they use the proposed services?
• What is the business model and who will pay for the portal services?
• What selection of services will you provide?
• How easily can patients register for the service and how well integrated are the different components (e.g., do they need to remember multiple user IDs and passwords)?
• Do hospital and/or clinic staff need to support the registration process?
• How is a patient’s identity verified prior to linking that person to the medical data?
• Do patients have control over who their data is shared with?
• If payments for services are processed through the portal in another jurisdiction, are appropriate taxes applied? Are industry-standard security controls applied? Are security standards complied with (e.g., the payment card industry)?
• Is a proper incident management process in place?
• How are links with medical providers managed and kept up-to-date?
Operations

• Are sufficient resources and expertise available for all phases of the portal’s life: development, maintenance, use, evaluation and evolution?

• How simple is the service to manage?

• Do you have the skills and sufficient staff to manage it within your organization or should certain services be outsourced to a third party?

• Do patients have the information and tools to solve most common problems by themselves, if they want (e.g., forgotten password)?

• Do patients have the option of calling someone for help if they need it?

• What types of reporting and targets are required for the proper management and success of the portal over time?

• Are periodic assessments done related to level of use, access, security violations, and to ensure the portal remains aligned with other care processes?

• Do periodic assessments also include an evaluation of patient outcome improvement, patient and provider satisfaction, process quality, process efficiency, positive effects on the attitude of patients and providers and any other desirable impacts?

• Do the contracts address the need for flexibility of the process of the project, such as the ability to handle unexpected and/or evolving requirements that emerge?

• What service-level agreements (SLAs) have been established for the patient portal services? Are the SLAs consistent when portions of the service are managed by different vendors? How well do the SLAs meet the expectations of patients and the medical providers who may be linked to them?

• Is there a complete marketing plan to target medical providers, patients and staff?

• Are there regular content updates, reminders, newsletters and other mechanisms to engage patients to use the service?

• Have medical providers been engaged to help promote the services to their patients?

• Are medical professionals paid for any extra work that may be required of them by the patient portal?
Appendix A:
The 10 Principles of the CSA Model Code for the Protection of Personal Information

1. **Accountability**
   An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization’s compliance with the following principles.

2. **Identifying Purposes**
   The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

3. **Consent**
   The knowledge and consent of the individual are required for the collection, use or disclosure of personal information, except where inappropriate.
4. **Limiting Collection**

The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

5. **Limiting Use, Disclosure and Retention**

Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.

6. **Accuracy**

Personal information shall be as accurate, complete and up-to-date as is necessary for the purpose for which it is used.

7. **Safeguards**

Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

8. **Openness**

An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

9. **Individual Access**

Upon request, an individual shall be informed of the existence, use and disclosure of his or her personal information, and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

10. **Challenging Compliance**

An individual shall be able to address a challenge concerning compliance with the above principles to the designate individual or individuals accountable for the organization’s compliance.
Appendix B:
Resources and Links


**Useful websites:**

Dossia: [www.dossia.org](http://www.dossia.org)

Keas: [www.keas.com](http://www.keas.com)

Mydoctor: [www.mydoctor.ca](http://www.mydoctor.ca)

Privacy by Design: [www.privacybydesign.ca](http://www.privacybydesign.ca)
Appendix C: User Agreements

Generally, a user agreement is a document that binds users, such as patients or clients in a patient portal context, to the organization providing the portal. Its purpose is twofold:

- It clearly describes to users their responsibilities and required actions, and provides them with a degree of confidence that their information is adequately protected.
- It offers to the healthcare organization providing the portal a form of risk mitigation by identifying limits of service provided. This risk mitigation can be made more effective at the time of registration by requiring users to acknowledge that they have read and understood the conditions of the agreement. Whether or not this step in registration is taken, the user agreement should be prominently displayed and proactively presented to all users.

User agreements typically contain the following information:

- **Description of services provided**: A clear outline of what the portal will do.
- **Expectation of use**: Statements showing that the user needs to acknowledge the following:
  - The medical content and functions of the portal should not be considered medical advice and do not replace a physician.
  - The portal should not be used for medical emergencies.
  - Use of the site does not create a physician-patient relationship between the owner of the portal (or its physicians) and the user.
  - Any products that may be mentioned on the site are not necessarily endorsed by the site.
- **Adherence to legislation**: A statement to draw attention to the jurisdictional legislation and regulations that govern the collection or
use of the information on the portal, plus any college or professional bylaws that govern the actions of the provider.

- **Privacy statement:** A statement from the provider clearly articulating that the privacy of the user’s information is paramount. This section could include actions that the provider takes to ensure privacy, such as regular reviews and audits (although these statements should be at a sufficiently high level to avoid redundancy with the section “Expectation the user has of the provider”—see below.

- **Confidentiality statement:** A statement from the provider outlining that the user’s information will not be divulged without consent or used for purposes other than those defined.

- **Expectations the provider has of the user:** Information to help educate the users on their responsibilities for protecting their own information. Since a user’s account login information provides full access to all information about that user, it is paramount that the user utilize strong security practices to protect that account. Include in this section a list of expectations the provider has of the user, such as not sharing accounts and using strong passwords. In some cases, providers may suggest users do not access their portal account from public computers or via unsecured, public networks. A user agreement may outline that the provider will not be responsible for harm as a result of breaches of a user’s information if the expectations in this section are not followed.

- **Expectation the user has of the provider:** An outline of what the provider will do to protect the confidentiality, availability and integrity of the user’s information. This section builds on previous sections regarding legislation and privacy and security with specific statements of activity. Typical best practices such as utilizing redundant systems (availability), regular audits of system activity (confidentiality) and regular testing of system backups (integrity) should be included here. In addition, this section should outline any requirements of the provider to ensure that the service is rendered to the user in an appropriate time frame (service-level agreement).

- **Exclusions and limitations:** A statement outlining the limits of liability the provider has to assume while providing services through the portal. This section will vary depending on jurisdiction, type of portal and risk appetite of the provider.

A good resource for developing a user agreement is the Terms of Use Agreement template available on the website of the Canadian Medical Protective Association. See [http://www.cmpa-acpm.ca](http://www.cmpa-acpm.ca).
Appendix D: Information Sharing Agreements

An information sharing agreement (ISA) is a legal document that outlines in detail how two or more organizations will collect, use, disclose, transfer and manage information. It sets out the nature of the business relationship and the respective responsibilities of each party to the agreement. An ISA must meet specific jurisdictional requirements imposed by legislation and/or regulation, and may also be governed by business standards of the participating organizations. Any information sharing agreement must include a list of topics that, if not addressed, may result in a lack of clarity leading to risks to the information’s protection.

The following is a list of topics that should be included.

Data Privileges and Responsibilities

Confidentiality and privacy: An outline of the basic tenets to which each party will adhere to protect the information being shared.

Security and access: An outline of the rules for who can grant access, to whom access can be granted and the minimum security requirements needed. It might be possible to combine this section into the confidentiality and privacy section; however, in most cases the requirements will be different enough to warrant individual sections.

Accuracy and data quality: An outline of each party’s responsibilities for ensuring that the information is not improperly manipulated, and what processes need to be followed if any data quality issues arise.
**Record maintenance requirements:** An outline of which party is responsible for maintaining the record and adhering to the maintenance requirements. Most jurisdictions have legal requirements outlining how long data must be kept and when to dispose of data. In addition, legislation or governing bodies may outline best practice requirements for ensuring that data is kept up-to-date during its useful life. This section differs from the accuracy and data quality section, which is more about ensuring that data remains valid while going through transformations between systems. The focus of record maintenance is on making changes to data as required.

**Other Sections**

Depending on the jurisdictional requirements, the ISA may include a section on quality assurance requirements needed to ensure that auditable and repeatable data management processes are in place. As well, depending on the relationship of the parties in an ISA, a section on services and functionality might need to be included to ensure both parties agree to their respective roles. This is more likely to be required in an arrangement where one party is providing consultative or value-added services to the other.

**Legal Clauses**

The following is a non-exhaustive list of legal clauses to be placed in ISAs to protect the interests of both parties. Legal counsel should be consulted when drafting the text in these sections:

- Termination
- Indemnification and limitation of liability
- Representations and warranties
- Dispute resolution
- Governing law

More details on ISAs are available on the website of the Canadian Medical Protective Association. See [http://www.cmpa-acpm.ca](http://www.cmpa-acpm.ca).
Appendix E: Consent Forms

The need for data to support healthcare is so integrated into the care process that those who request data can sometimes miss the point that consent to collect and use data for specific purposes and/or to disclose data is a separate concept and operational issue from consent for the care itself. There are legislative requirements for information collection, use and disclosure that apply. The organization must meet these requirements before it collects the data or further uses or discloses it, and it must securely store the data and uphold security standards. This means that there must be security policies in place at the organization that transmits and/or holds the data.

When designing consent forms a number of practical, legal and ethical requirements must be met. If these requirements are not addressed, the consent obtained may not be valid. Use the following list for developing a consent form:

- Language should be simple enough to be understood by the ordinary reader.
- The form should:
  » Clearly state the names of the organizations involved.
  » Describe the parties involved as legal entities or organizations.
  » State the accountable organization. (There must be one or a shared accountability which is outlined within a structure.)
  » Include a description of the information to be collected and its sources (e.g., direct collection from the patients and individuals and indirect collection from patient care sources, physicians and/or other sources). Do not talk about obtaining information from general sources such as “the patient’s health record”; be sure to name the sources.
» Clearly state the uses to which the data will be put.
» Clearly state what the individual is consenting to.
» Describe how long the data will be retained and how and when it will be securely destroyed.
» Describe any opportunities for patients to opt out of certain types of uses or disclosures.
» Describe any opportunities for patients to learn about new or expanded data uses (e.g., reuse of the data).
» Describe any opportunities for patients to exert control over use of data or the degree of identifiability of the data.
» Describe what patients will be told about their right to withdraw their data at any time.
» If compensation is involved, explain what patients will be told about compensation if they withdraw (i.e., it will not be used; it is logistically impossible to remove individual’s data; it will be used if the participant agrees).
» Describe how agreement to use patient data will be obtained if they withdraw.
» Describe how patients may know about and request/review a copy of their personal information.
» Describe how a record will be kept of the decisions and reasons for refusing such requests.
» Clearly state how to contact the accountable organization/person.
» Describe generally the physical storage protection and sites.
### Appendix F: Glossary of Terms

<table>
<thead>
<tr>
<th>Term/Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access</td>
<td>For the purposes of protecting privacy, disclosure of personal information by providing access to personal information.</td>
</tr>
<tr>
<td>Access Control</td>
<td>The control of user privileges (e.g., read, update) with respect to information, an application or a database.</td>
</tr>
<tr>
<td>Aggregate Data</td>
<td>Data averaged or grouped into ranges (e.g., five- or 10-year age groupings).</td>
</tr>
<tr>
<td>Anonymize</td>
<td>The transformation of personally identifiable information into a state in which it cannot be reidentified.</td>
</tr>
<tr>
<td>Asset</td>
<td>An item/object that has value to an organization (e.g., PHI is a valuable information asset to health organizations).</td>
</tr>
<tr>
<td>Audit</td>
<td>An independent examination of information systems and processes to detect unauthorized activities.</td>
</tr>
<tr>
<td>Audit Log/Access Audit/ Audit Report</td>
<td>A chronological listing of access-to-information resources. Items that are typically logged include user identity, time of access, resources that were accessed, device used to access the information and modifications that were made.</td>
</tr>
<tr>
<td>Term/Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Audit Mechanisms</td>
<td>The tools used to record, in chronological order, users who have accessed, modified, distributed and deleted personal health information.</td>
</tr>
<tr>
<td>Authentication</td>
<td>Corroboration that the source of the data is as claimed, based on information used to establish the validity of a claimed identity (ISO 7498-2).</td>
</tr>
<tr>
<td>Authentication Token</td>
<td>A cryptographically protected, binary-encoded string or object containing minimal user information, a timestamp and an expiry time. It is created by the EHR after the system has first authenticated a user as part of the login process. This token is then returned to the user’s system to be used for subsequent access to EHR functions during that session without the user having to re-login.</td>
</tr>
<tr>
<td>Availability</td>
<td>The property of being accessible and usable upon demand by an authorized entity (ISO 7498-2).</td>
</tr>
<tr>
<td>Breach of Information</td>
<td>An action by an authorized or unauthorized user that results in a negative impact, or causes interruption, disclosure, unauthorized access, modification, destruction or denial of service. An information security breach is sometimes referred to as an information security incident.</td>
</tr>
<tr>
<td>Security</td>
<td></td>
</tr>
<tr>
<td>CDMS</td>
<td>Consent directives management service.</td>
</tr>
<tr>
<td>Change Management</td>
<td>The processes that ensure the secure control of all changes to equipment and software. These are sometimes referred to as change control processes.</td>
</tr>
<tr>
<td>Processes</td>
<td></td>
</tr>
<tr>
<td>CHI</td>
<td>Canada Health Infoway.</td>
</tr>
<tr>
<td>CHIMA</td>
<td>Canadian Health Information Management Association.</td>
</tr>
<tr>
<td>CHRA</td>
<td>Canadian Health Records Association.</td>
</tr>
<tr>
<td>CIA</td>
<td>Confidentiality, integrity and accessibility.</td>
</tr>
<tr>
<td>Term/Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>CIHI</td>
<td>Canadian Institute for Health Information.</td>
</tr>
<tr>
<td>Classification</td>
<td>A system for determining the sensitivity of personal health information and for establishing priorities for information security and privacy protection.</td>
</tr>
<tr>
<td>COACH</td>
<td>Canada’s Health Informatics Association.</td>
</tr>
<tr>
<td>CoBIT</td>
<td>Control objectives for information technology.</td>
</tr>
<tr>
<td>Code of Conduct/Code of Ethics</td>
<td>A documented set of rules outlining appropriate behaviour for the members of a health organization or professional group. A code of conduct is often based on a code of ethics—ethical principles outlining rules for appropriate behaviour.</td>
</tr>
<tr>
<td>Collection (of Information)</td>
<td>The process of gathering or obtaining personal health information, either directly from an individual, or indirectly (e.g., from an individual’s legally authorized representative or a health services organization).</td>
</tr>
<tr>
<td>Collection, Direct</td>
<td>Information collected directly from individuals.</td>
</tr>
<tr>
<td>Collection, Indirect</td>
<td>Information gathered from any source other than from the individual to whom the information relates.</td>
</tr>
<tr>
<td>Compliance</td>
<td>The meeting of requirements as set out in relevant laws, regulations, standards, ethical principles, codes of conduct, contractual agreements or policies and procedures.</td>
</tr>
<tr>
<td>Confidentiality</td>
<td>The property that information is not made available or disclosed to unauthorized individuals, entities or processes (ISO 7498-2).</td>
</tr>
<tr>
<td>Consent</td>
<td>Voluntary agreement by an individual, or his or her legally authorized representative, to allow the collection, use or disclosure of the individual’s personal health information.</td>
</tr>
</tbody>
</table>
## Glossary of Terms

<table>
<thead>
<tr>
<th>Term/Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consent, Deemed</td>
<td>In the context of a statutory requirement, the concept that it does not matter whether the person has actually consented; the law permits organizations to act as if the person has consented; there is no right to withdraw or withhold consent.</td>
</tr>
<tr>
<td>Consent, Express or Expressed</td>
<td>Voluntary agreement with what is being done or proposed that is unequivocal and does not require any inference on the part of the organization seeking consent. Express consent may be verbal or written.</td>
</tr>
<tr>
<td>Consent, Implied</td>
<td>Voluntary agreement with what is being done or proposed that can be reasonably determined through the actions or inactions of the person.</td>
</tr>
<tr>
<td>Consent, Informed</td>
<td>The requirement that consent is not valid in the absence of knowledge.</td>
</tr>
<tr>
<td>Consent, None</td>
<td>In the context of a statutory requirement, where consent is not required for a particular purpose.</td>
</tr>
<tr>
<td>Control (of Information)</td>
<td>Responsibilities for maintaining control of information; more specifically described in privacy legislation. An information collector or data steward can retain accountability for information, even when the information leaves the organization's direct custody. This control of information is typically enforced on vendors or information service providers through contracts, specific contract language and information sharing agreements.</td>
</tr>
<tr>
<td>COSO</td>
<td>Committee of Sponsoring Organizations.</td>
</tr>
<tr>
<td>CRUD</td>
<td>Create, read, update and delete.</td>
</tr>
<tr>
<td>CSA</td>
<td>Canadian Standards Association.</td>
</tr>
<tr>
<td>CSE</td>
<td>Communications Security Establishment Canada.</td>
</tr>
</tbody>
</table>
## Glossary of Terms

<table>
<thead>
<tr>
<th>Term/Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Custodian (of Health Information)</td>
<td>As defined in some legislation, an individual or organization that collects, uses or discloses personal health information for the purposes of care and treatment, planning and management of the health system, or health research.</td>
</tr>
<tr>
<td>Custody (of Information)</td>
<td>The act of having information in one’s physical, or logical, setting and of having responsibility for its protection, but not authority to define its uses, disclosures and management.</td>
</tr>
<tr>
<td>Data</td>
<td>Pieces of information (e.g., individual facts or results).</td>
</tr>
<tr>
<td>Data Accuracy</td>
<td>The concept that data is accurate if it reflects reality. Accurate data is required in order to make decisions about individuals.</td>
</tr>
<tr>
<td>Database</td>
<td>A means of managing large amounts of data and administering collection, classification, access and disclosure. Through the use of databases, health organizations can collect and access data from a variety of sources to assist them with administration, clinical decision making, research and other health-related needs.</td>
</tr>
<tr>
<td>Database Administrator</td>
<td>A person who directs or performs activities related to maintaining a successful database environment, using tools designed for this purpose. Typical responsibilities include designing, implementing and maintaining the database system; establishing procedures pertaining to the management, security, maintenance and use of the database management system; and training employees in database management and use.</td>
</tr>
<tr>
<td>Data Custodian</td>
<td>In provinces without health information Acts that explicitly define “custodian” as the organization or person who holds the physical information, but who does not set control responsibilities. Data custodianship relates primarily to responsibility for data storage and integrity, and such responsibilities are generally set in contracts or by service agreements. See also Custody (of Information), Data Holder and Data Steward.</td>
</tr>
<tr>
<td>Term/Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Data Dictionary</td>
<td>A collection of descriptions of data objects or items, each consisting of its name, relationship(s), data type, and brief description, used for the benefit of programmers and others. When developing or using systems that use the data model, a data dictionary can be consulted to understand where a data item fits into the structure, what values it may contain and what the data item means in real-world terms.</td>
</tr>
<tr>
<td>Data Holder</td>
<td>An individual or organization that may have custodianship and/or stewardship functions (i.e., custody and/or control). These functions may be executed within the same institution/body, or may be delegated to distinct but coordinated institutions/bodies. See also Data Custodian and Data Steward.</td>
</tr>
<tr>
<td>Data Owner</td>
<td>A concept that does not apply to PHI. FIPPA states that data belongs to the individual, while the media upon which it is recorded is owned by the organization.</td>
</tr>
<tr>
<td>Data-Sharing Arrangements</td>
<td>Strategic information partnerships with other health organizations to provide an enhanced level of care and service for subjects of care.</td>
</tr>
<tr>
<td>Data Steward</td>
<td>The person or organization with legal and ethical responsibility for the collection, use, disclosure, management and overall protection of data. Data stewardship relates primarily to responsibility for data definition and access authorization, particularly data access and disclosure to third parties. See also Data Custodian and Data Holder.</td>
</tr>
<tr>
<td>Data Use (Primary)</td>
<td>Information that is used by a care provider or organization responsible for the direct care of a subject of care.</td>
</tr>
<tr>
<td>Data Use (Secondary)</td>
<td>Information that is used by authorized persons or agencies for purposes other than direct care of the individual. These include administrative planning, accreditation and licensing, payment for services and treatment, quality improvement activities, research, teaching or legal use as required by law.</td>
</tr>
<tr>
<td>Term/Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>De-identified Information</td>
<td>PHI modified so that the identity of an individual cannot be determined by a reasonably foreseeable method (e.g., removal of name and address; removal or encryption of identifying numbers, such as personal health number and chart number; truncating postal code to the first three digits; converting date of birth to month and year, age, or age group; converting date of admission and date of discharge to month and year only; and reviewing the remaining data elements to ensure they do not permit identification of the subject individual by a reasonably foreseeable method).</td>
</tr>
<tr>
<td>Disclosure</td>
<td>The act of releasing or making available PHI to someone other than the person the information concerns, or a person employed by, or in the service of, the party holding the information.</td>
</tr>
<tr>
<td>Disclosure, Residual</td>
<td>A situation where the identity of an individual could be determined by reasonably foreseeable methods from PHI (including when the information has been aggregated or has had direct identifiers stripped, encrypted or masked).</td>
</tr>
<tr>
<td>Educational Awareness Program</td>
<td>A comprehensive organizational program designed to foster a <a href="#">security-conscious</a> organizational culture aimed to support diverse goals in information protection.</td>
</tr>
<tr>
<td>EHR</td>
<td>See Electronic Health Record.</td>
</tr>
<tr>
<td>Electronic Health Record</td>
<td>A secure and private lifetime record of a person’s health history and care within the health system. The record is available electronically to authorized healthcare providers and the individual anywhere, anytime, in support of high-quality care.</td>
</tr>
<tr>
<td>EMR</td>
<td>Electronic medical record.</td>
</tr>
<tr>
<td>Encryption</td>
<td>The process of mathematically converting information to render it unintelligible without a key to decode it.</td>
</tr>
<tr>
<td>Term/Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Hacker</td>
<td>An individual characterized as a “computer expert” who has expertise in programming and information systems. The term is now commonly used to refer to someone who can gain unauthorized access to other computers to cause harm.</td>
</tr>
<tr>
<td>Hardware</td>
<td>The physical components of computers, telecommunications and other information technology systems.</td>
</tr>
<tr>
<td>Healthcare Organization</td>
<td>Any organization engaged in the planning, funding, management, manufacture or delivery of health services or products.</td>
</tr>
<tr>
<td>Healthcare Professional</td>
<td>Any individual employed or engaged in the delivery of health services to a subject of care.</td>
</tr>
<tr>
<td>Health Information System</td>
<td>An organized array of technologies used to coordinate the collection, filing, storage, retrieval and transmission of PHI.</td>
</tr>
<tr>
<td>Health Region</td>
<td>A geographical region where boundaries define the area in which the delivery and administration of health services are coordinated.</td>
</tr>
<tr>
<td>HIA</td>
<td>Health Information Act.</td>
</tr>
<tr>
<td>HIAL</td>
<td>Health information access layer.</td>
</tr>
<tr>
<td>Identifiers, Direct</td>
<td>Variables that provide an explicit link to a respondent (e.g., name and address, health insurance number).</td>
</tr>
<tr>
<td>Identifiers, Indirect</td>
<td>Variables that, in combination, could be used to identify an individual (e.g., date of birth, sex, marital status, area of residence, occupation, type of business).</td>
</tr>
<tr>
<td>IM</td>
<td>Information management.</td>
</tr>
<tr>
<td>Information Protection</td>
<td>A broad term used to discuss the privacy, confidentiality and security of PHI.</td>
</tr>
<tr>
<td>Term/Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Informational Self-Determination</td>
<td>The right of individuals to determine with whom they share their PHI and under what circumstances.</td>
</tr>
<tr>
<td>Integrity</td>
<td>The property that information has not been altered or destroyed in an unauthorized manner (ISO 7498-2).</td>
</tr>
<tr>
<td>Internet</td>
<td>A worldwide decentralized network of computer networks, generally using the same communication protocol (TCP/IP). The Internet is not synonymous with World Wide Web.</td>
</tr>
<tr>
<td>ISA</td>
<td>Information sharing agreement.</td>
</tr>
<tr>
<td>ISO</td>
<td>International Organization for Standardization.</td>
</tr>
<tr>
<td>IT</td>
<td>Information technology.</td>
</tr>
<tr>
<td>Linking (of Data) or Data Linkage</td>
<td>The bringing together of two or more records of PHI to form a composite record.</td>
</tr>
<tr>
<td>LM</td>
<td>Log management.</td>
</tr>
<tr>
<td>Need-to-Know</td>
<td>(1) The legitimate requirement of a person or organization to know, access or possess sensitive or classified information that is critical to the performance of an authorized, assigned mission.</td>
</tr>
<tr>
<td></td>
<td>(2) The necessity for access to, or knowledge or possession of, specific information required to carry out official duties.</td>
</tr>
<tr>
<td>Network</td>
<td>A series of points or nodes that are interconnected by communication paths. Devices can be attached to network nodes enabling users to perform a variety of functions: access information stored at other locations on the network, communicate with other users on the network or print documents to networked printers.</td>
</tr>
</tbody>
</table>
### Glossary of Terms

<table>
<thead>
<tr>
<th>Term/Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-Identifiable Information</td>
<td>The condition in which any element or combination of elements that allows direct or indirect identification of an individual that was never collected, or that has been removed, although some elements may indirectly identify a group or region. There is no code linking the information back to the individual’s identity.</td>
</tr>
<tr>
<td>OIPC</td>
<td>Office of the Information and Privacy Commissioner.</td>
</tr>
<tr>
<td>Outsourcing</td>
<td>An arrangement in which one organization provides services for another. In many cases, these services may once have been provided in-house.</td>
</tr>
<tr>
<td>Personal Health Information</td>
<td>Information about an individual that identifies the individual; or that may be used or manipulated by a reasonably foreseeable method to identify the individual; or that may be linked by a reasonably foreseeable method to other information that identifies the individual and that may include information related to the physical or mental health of the individual; the provision of health services to the individual; the registration of the individual for the provision of health services; the donation of any body part or bodily substance of the individual, or is derived from the testing or examination of any such body part or bodily substance; payments or eligibility for healthcare; a number, symbol, or particular, assigned to an individual to uniquely identify the individual for health system purposes; information that is collected in the course of the provision of health services to the individual; or registration and practice information about a health professional.</td>
</tr>
<tr>
<td>Personal Information</td>
<td>Information about an identifiable individual; includes employee personal information but does not include contact information or work product information.</td>
</tr>
<tr>
<td>PHI</td>
<td>See Personal Health Information.</td>
</tr>
<tr>
<td>PIA</td>
<td>See Privacy Impact Assessment.</td>
</tr>
<tr>
<td>PKI</td>
<td>Public key infrastructure.</td>
</tr>
<tr>
<td>Term/Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>POS</td>
<td>Point of service.</td>
</tr>
<tr>
<td>Primary Purpose</td>
<td>Specific purpose for which information collected to be used by a care provider or organization responsible for the direct care of a subject of care.</td>
</tr>
<tr>
<td>Privacy</td>
<td>(1) The right to be free from intrusion and interruption. It is linked with other fundamental rights such as freedom and personal autonomy. In relation to information, privacy involves the right of individuals to determine when, how and to what extent they share information about themselves with others.</td>
</tr>
<tr>
<td></td>
<td>(2) Freedom from intrusion into the private life or affairs of an individual when that intrusion results from undue or illegal gathering and use of information about that individual.</td>
</tr>
<tr>
<td></td>
<td>(3) The right of individuals to live free of intrusive monitoring of their personal affairs by third parties not of their choosing.</td>
</tr>
<tr>
<td></td>
<td>(4) The claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others.</td>
</tr>
<tr>
<td>Privacy-Enhancing</td>
<td>The combination of technology, applications and processes that form a privacy architecture that enables an appropriate level of security and privacy in electronic information management. It involves encryption, policy, filtering and anonymization tools to support services and applications such as privacy-friendly business models and user interfaces; privacy management including classification of information, authorization policies and enforcement; information minimization, including attribute-based authorization, anonymization and trusted relationships; security technology, including access control, encryption and cryptology control; privacy violation detection, including real-time monitoring and auditing; and verification and certification, including analysis and formal verification of processes.</td>
</tr>
<tr>
<td>Technologies</td>
<td></td>
</tr>
<tr>
<td>Term/Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Privacy Impact Assessment</td>
<td>A comprehensive process for determining the privacy, confidentiality and security risks associated with the collection, use and disclosure of personal information. Also defines the measures used to mitigate and, wherever possible, eliminate the identified risks.</td>
</tr>
<tr>
<td>Privacy Officer</td>
<td>The individual in an organization whose role is to assist management provide leadership for protecting the privacy and security of personal health information through specialist skills and advice. The privacy officer is primarily responsible for ensuring that the organization complies with privacy requirements determined by legislation, standards and guidelines.</td>
</tr>
<tr>
<td>Pseudonymization</td>
<td>A particular type of anonymization that both removes the association with an individual, and adds an association between a particular set of characteristics relating to the individual and one or more pseudonyms.</td>
</tr>
<tr>
<td>Read-Only</td>
<td>A level of access to information that only allows the user to review information. The user with read-only access is unable to modify, delete or transmit information.</td>
</tr>
<tr>
<td>REB</td>
<td>Research ethics board.</td>
</tr>
<tr>
<td>Remote Access</td>
<td>The ability to logon to a computer or a network from a remote place. In health organizations, outsourced service providers, people at branch offices, telecommuters and people who are travelling may need remote access to be able to logon to the organization’s network.</td>
</tr>
<tr>
<td>Research</td>
<td>A systematic investigation designed to develop or establish principles, facts or general knowledge.</td>
</tr>
<tr>
<td>Retention</td>
<td>The process of holding information in a secure or intact manner, usually for a defined period of time after which it may be permanently discarded.</td>
</tr>
<tr>
<td>Risk</td>
<td>The uncertainty that surrounds future events and outcomes. Risk is the expression of the likelihood and impact of an event with the potential to influence the achievement of an organization’s objectives.</td>
</tr>
<tr>
<td>Term/Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Risk Management</td>
<td>The department or individual (e.g., risk manager) whose role is to minimize the risks associated with poor information protection. Risks can result in significant damage to an organization’s reputation and a loss of trust in the ability of the organization to protect personal health information, fines, liability and investigations by the privacy commissioner.</td>
</tr>
<tr>
<td>SDM</td>
<td>See Substitute Decision Maker.</td>
</tr>
<tr>
<td>Secondary Purpose</td>
<td>Information that is used by authorized persons or agencies for purposes other than for which it was originally collected. For example, information collected primarily to administer care to an individual may also be used for secondary purposes that include administrative planning, accreditation and licensing, payment for services and treatment, quality improvement activities, research, teaching or legal use as required by law.</td>
</tr>
<tr>
<td>Security</td>
<td>The preservation of the confidentiality, integrity and availability of PHI. Information security is achieved by implementing policies and procedures based on relevant legislation, standards and ethical principles, careful planning, design, implementation and maintenance of appropriate technology solutions, and managing ongoing operations related to the collection, classification access and disclosure of PHI.</td>
</tr>
<tr>
<td>Security Officer</td>
<td>The individual whose role is to manage the security function within a health organization. The security officer requires a sound understanding of the information technologies used within the organization, an expert knowledge of security technologies and techniques, and a current knowledge of threats and risks to health information systems.</td>
</tr>
<tr>
<td>Security-Conscious</td>
<td>Behaviour exhibited by users to support a security-conscious organizational culture. Examples include wearing photo ID badges at all times, reporting known or suspected security breaches or incidents promptly to the privacy officer and participating in regular educational awareness programs.</td>
</tr>
<tr>
<td>Term/Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Sensitivity (of Information)</td>
<td>The potential for harm or stigma that might attach to the identification of an individual or community because of the nature of information. The type of information that an individual may consider sensitive could relate to sexual attitudes, practices and orientation; use of alcohol, drugs or other addictive substances; illegal activities; suicide; sexual abuse; sexual harassment; an individual’s psychological well-being or mental health; genetic information; and any other information that might lead to social stigmatization or discrimination.</td>
</tr>
<tr>
<td>Software</td>
<td>Programs that support the use of computer resources. Application software allows users to access and process information in a user-friendly way. System software includes the operating system and any other program that supports the application software.</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure sockets layer, a protocol for transmitting private documents via the Internet. SSL uses a private key to encrypt data that is transferred via a program layer located between the Internet’s hypertext transfer protocol (HTTP) and transport control protocol (TCP) layers. “Sockets” refer to the method of passing data back and forth between a client and a server program in a network, or between program layers in the same computer.</td>
</tr>
<tr>
<td>Storage</td>
<td>The holding or placing of information in a location for later retrieval, use or disposal.</td>
</tr>
<tr>
<td>Strong Authentication</td>
<td>Also called two-factor authentication, where two out of the following three proofs exist: something known, like a password, something possessed, like a driver’s licence, and something unique about appearance or person, like a fingerprint. Using strong authentication provides more protection for sensitive information than a simple username and password can provide.</td>
</tr>
</tbody>
</table>
## Glossary of Terms

<table>
<thead>
<tr>
<th>Term/Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subject of Care</td>
<td>The individual who is the subject of personal information collected. Refers to individuals seeking care or information from healthcare professionals or organizations. The individual may not be an active subject of care in all cases (e.g., someone seeking immunization or documentation, or acting on behalf of a subject of care).</td>
</tr>
<tr>
<td>Substitute Decision Maker</td>
<td>In relation to a subject of care, unless the context requires otherwise, a person who is authorized under legislation to consent on behalf of the subject of care to the collection, use or disclosure of PHI about the subject of care.</td>
</tr>
<tr>
<td>Third Party</td>
<td>In relation to a request for access to a record, or for correction of personal information, any person, group of persons or organization other than the person who made the request or a public body.</td>
</tr>
<tr>
<td>Threat and Risk Assessment</td>
<td>A process used to identify information assets, threats to those assets and possible security safeguards. It has three major components: a threat analysis, a risk analysis, and an assessment of safeguards.</td>
</tr>
<tr>
<td>TRA</td>
<td>See Threat and Risk Assessment.</td>
</tr>
<tr>
<td>Trustee</td>
<td>In Saskatchewan, under the HIPA, any public body that has custody or control of PHI.</td>
</tr>
<tr>
<td>Use (of Information)</td>
<td>The treatment and handling of PHI within an organization. Disclosure does not constitute use.</td>
</tr>
<tr>
<td>User</td>
<td>In this document, any individual who collects, accesses, uses or discloses PHI.</td>
</tr>
<tr>
<td>Virus</td>
<td>A computer program, typically hidden, that attaches itself to other programs and has the ability to replicate and spread to other computers. A virus is generally replicated by inadvertent human action and, when executed, results in undesired effects unanticipated by the user.</td>
</tr>
<tr>
<td>Wireless</td>
<td>Any form of telecommunication or data transmission in which signals are carried by electromagnetic waves as opposed to some form of wire.</td>
</tr>
</tbody>
</table>