TERMS AND CONCEPTS

eHealth Ontario supports the use of health informatics, health information management and information technology industry standard definitions for concepts and terms used throughout the blueprint. This approach keeps eHealth Ontario and other stakeholders aligned with Canadian and international definitional practices as much as possible, and promotes ease of understanding and maintenance for terms and concepts.

Refer to Appendix B: Terms and Concepts for details.

COPYRIGHT NOTICE

Copyright © 2014, eHealth Ontario. All rights reserved

No part of this document may be reproduced in any form, including photocopying or transmission electronically to any computer, without prior written consent of eHealth Ontario. The information contained in this document is proprietary to eHealth Ontario and may not be used or disclosed except as expressly authorized in writing by eHealth Ontario.

TRADEMARKS

Other product names mentioned in this document may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.
Table of Contents

Ontario Ehealth Blueprint Context 1
Perspectives on Health Care .................. 3
  Patient Experience .......................... 3
  Provider Experience ......................... 4
  Health Care Business
  User Experience .............................. 4
  Ehealth Landscape ........................... 5
  Key Challenges ................................ 5
  Transforming Health Care .................... 6
  The Electronic Health Record (EHR) .6

Ontario’s Ehealth Blueprint 7
Why the Blueprint Matters ..................... 8

Business View 9
Benefits of the Business View ............... 10
Governors ......................................... 10
eHealth Ontario Direction .................... 10
eHealth Ontario Capabilities .................. 10
eHealth Services ................................. 11
eHealth Support Services ...................... 11
Partners and Vendors ......................... 12
Health Sector Services ....................... 12
Consumers ....................................... 12

Information View 13
Ehealth Information Architecture ............ 14
Information Management
Framework Principles .......................... 14
Information View Benefits .................... 15
Information Model Overview ................. 15
Health Care Encounters ...................... 16
Health Care Plans .............................. 17
Client Teams ................................. 17
Client Health Profiles ......................... 17
Information Resources ....................... 18
  Knowledge Resources ....................... 18
  Health System Analytics .................... 18

Systems View 19
Key Architectural Principles
and Decisions .................................. 20
Service-Oriented Architecture (SOA) .... 21
  Characteristics of Service Oriented
  Architecture Services ....................... 21
  Enabling a Service-Oriented
  Approach for the EHR ..................... 21
Systems View Components ................... 22
The Ontario health care sector is a complex and multi-faceted environment with a high transaction volume. Hundreds of thousands of health care providers of different types work within a diverse set of health care organizations such as hospitals, rehabilitation centres, continuing care, mental health services, long-term care facilities, Community Care Access Centres (CCACs), as well as private sector services such as dental care, pharmacies, independent health facilities, and laboratories. Interdisciplinary approaches to service delivery include a wide range of health care providers delivering services in a multitude of health care facilities.
The health care system is governed by the Ministry of Health and Long-Term Care (MOHLTC). eHealth Ontario is an independent agency of the MOHLTC, created to promote and implement electronic health records (EHRs) across Ontario.

The province of Ontario is divided into 14 Local Health Integration Networks (LHINs), which are not-for-profit organizations responsible for planning, integrating, and funding health services within their jurisdictional area.

A number of health care disciplines are regulated by bodies, such as the College of Physicians and Surgeons of Ontario, the College of Nurses of Ontario, and the Ontario College of Pharmacists. Other disciplines are not currently regulated.

Health care is a large component of the Ontario government’s budget, and costs are expected to increase due to factors such as population growth, an aging population, increased incidences of chronic and complex diseases, and other changes.
Patient Experience

The patient is the centre of the health care system. Every day hundreds of thousands of patients interact with physicians, nurse practitioner clinics, hospitals, ambulatory care clinics, community services, and pharmacies. As they move through the system, they leave a trail of information about their health care, some of which is recorded and stored by providers. Often, these sources of data are not connected, and data is mostly shareable between authorized health care providers manually through mechanisms such as mail, fax, or telephone.

The patient experience in the current health care system in Ontario is often marked by delay, duplication, limited information availability at the point of service, and frustration. For example, when visiting a provider, a patient may experience one of the following situations.

Scenario 1: the required information is not available due to:

- Slow arrival of test results sent by mail/fax
- Lost results
- Information scattered throughout large paper files
- Required prescription information stored at another physician’s office

Scenario 2: the patient is required to repeat his/her history for each new provider:

- This is an error prone process, which can result in information being stored in multiple places as well as duplicate tests, repeated visits, delay, or missing information through information collection fatigue or forms/processes that make collection difficult.
- Collecting information may not be possible in an emergency department should the patient be unable to communicate.

Perspectives on Health Care

The health care system includes different types of stakeholders:

- Patients (also called health care clients in some health care settings and in this document)
- Providers of health care services
- Business users
- IT professionals

The following section describes the perspective of each of these stakeholders.
Provider Experience

When delivering services, providers need a comprehensive, up-to-date view of a patient’s entire health history. This view should include information from all health care disciplines, regulated and non-regulated, including encounter history, assessments, diagnostic results, consultations, hospital reports, medication history, lab test results, allergies, and immunizations.

Clinical health care data has traditionally been captured and stored across multiple health care organizations, in different physical locations and on different, incompatible computer systems and paper files. It is often stored in different paper and electronic formats, which use different terminology, and are owned and managed by different entities using different standards and technologies. This can have significant impact on the timely delivery of health care, such as:

- Diagnoses and treatment decisions based on fragmented or outdated information
- Having health care providers login separately to multiple systems to input and access data
- Increased health care costs

Providing authorized access to health care information at any time or from any location would significantly benefit both providers and patients, but requires EHR systems to be interoperable. Interoperability refers to the ability of systems to connect to and exchange and process data from other systems – so information sent from one system can be understood by another.

Health Care IT Professional Experience

Electronic health care solutions are based on different standards or no standards at all. Integration of these systems is mainly done using customized mechanisms known as ‘point-to-point’ integration, an approach that is expensive to execute and maintain, making integration difficult or even impossible.

In order to achieve interoperable, secure, private and cross-disciplinary EHRs, IT professionals need a blueprint that includes a common architecture with defined standards, principles, and components for the entire province. This foundation will continue to evolve with the increase in use of electronic health records and improvements to systems, practices and standards.

Health Care Business User Experience

Managers and planners use health care data to monitor resources, build and approve plans and budgets, and create and manage health care policies, standards, and legislation. By analyzing the data they can identify and assess trends and manage health care system costs and the quality of care. Health care researchers use data from the health care system for advancing medical knowledge, identifying best clinical practices, and analyzing treatment results.

Neither of these groups needs personal health information (PHI); they can work with data from which all references to identifiable individuals have been removed, or with data that has been aggregated.

These business users need to find ways to improve the availability, timeliness, quality, and quantity of the data they work with.
Ehealth Landscape

Ehealth or electronic health refers to the delivery of health care services using electronic systems, processes, and information and communication technology, to facilitate the availability and exchange of health information between patients, providers, and other authorized users.

It also includes electronic provisioning of related support services for the effective and efficient planning, management, and delivery of health care.

The term ‘ehealth’ is distinct from ‘eHealth Ontario’, which is an agency of the Ontario Ministry of Health and Long-Term Care.

The diagram represents the relationship between the health care sector, ehealth, eHealth Ontario’s area of focus, and the EHR. It shows that, in addition to eHealth Ontario, other organizations in the province are implementing ehealth solutions and contributing to the EHR.

Key Challenges

Based on these stakeholder perspectives, key challenges can be summarized as:

- Getting the right information at the right time in the right format to the right people with the right access
- Capturing quality data about health care activity and outcomes in a timely manner
- Lack of common standards across the health sectors, health care providers and systems, and a unified approach to building scalable, high performing, interoperable systems
Transforming Health Care

By simplifying information access and sharing, ehealth provides the following benefits:

- **Improved care** through timely, secure, accurate, and complete information shared among all health care providers from all relevant sources. The ability to coordinate and share data among health care systems, such as annual patient physicals, lab reports and test results, medication records, and digital diagnostic images, will help reduce wait times for appointments, procedures, access to health care facilities, laboratory test results, and clinical diagnoses.

- **Improved safety** and reduced potential for adverse effects such as allergies, interactions, and incorrect dosage.

- **Improved security** of confidential health information through modern, encrypted data protection systems, by implementing standards and electronic controls to manage access to data, and to protect the privacy of Ontario citizens.

- **Improved practice efficiencies** from automated workflows and having all patient information in one location, giving providers more time to focus on their clients.

- **Improved support** for health system management by providing the ability to identify program spending effectiveness, and the use and allocation of resources. This will help facilitate the efficient transfer of patients to the appropriate level of care, such as health care facilities, community care, and primary care. It also can help reduce costs through fewer duplicate tests, more efficient use of physician and specialist visits, and more efficient use of emergency room and hospital visits.

- **Improved support** for research through secondary use of rich longitudinal health information spanning a patient’s history. For example, this information can be used to review information on determinants of health, as well as for pure research at health care organizations, universities, and other academic institutions.

The Electronic Health Record (EHR)

The **EHR is a secure and private lifetime record of a person's health history. The record is available electronically to authorized Ontario health care providers anywhere, anytime, in support of high quality care.**

The goal of the EHR is to provide a patient-centric solution to the challenges currently facing the province’s health care sector. It does this by providing the means for diverse health care systems and data sources to securely share information. As a result, authorized users can have a seamless, efficient way to request information from different sources, and input information into designated data sources. For example, through the EHR, an authorized lab will be able to enter a lab test result into the lab data repository, and the provider who requested the test can retrieve the result from the same repository. In this way, a comprehensive health care picture for a patient can be assembled as if it were coming from a single system.

Refer to Appendix C: Scenarios for a comparison of what currently happens when a health care client interacts with the health care system and what will happen when the EHR is implemented.
Ontario’s ehealth blueprint is a foundational artifact that informs EHR planning and delivery for the province. It provides a future state, high-level view of the EHR in Ontario, without specifying when components or capabilities will be available, or who will be responsible for them. It defines the elements required to realize the goals of the EHR, while providing a framework for describing the architectural principles and patterns that will be employed to deliver its solutions. The blueprint is built on key foundational principles including privacy and security compliance, collaborative governance, regulation and policy, standards, and federation.
The blueprint provides multiple views. This document addresses three – the business, information and systems views. Information on standards, a key component of an interoperable EHR, is woven throughout the document.

The business view defines eHealth Ontario’s business services that support health care delivery. The information view defines what information needs to be gathered and managed as part of providing these services. The systems view describes the systems solutions that automate the business services and manage the data, as well as the core infrastructure services required for the EHR.

Example: Health care providers need to be able to order lab tests electronically. The business view describes the requisition service required to support these orders; the information view defines the data that must be captured and used; and the systems view includes the Ontario Laboratories Information System (OLIS), which implements the technical solution.

Why the Blueprint Matters

The blueprint:

- Provides a tool for business and IT stakeholder dialogues
- Establishes a common framework and a set of consistent terminology
- Provides provincial architecture and standards that can be leveraged for local or regional innovation, while supporting province-wide alignment
- Provides information on the types of capabilities that will assist in the enhancement of health program management and operations
- Informs ehealth strategic planning, solution planning, and investment decisions
- Helps shape ehealth governance by clarifying roles, responsibilities, business services
The business view represents eHealth Ontario’s view of the business it is in. It highlights the business services that the agency provides to the health sector, and includes the agency’s mandate, strategic direction, stakeholders, business objectives, and capabilities. It is a technology-neutral and business focused framework; it is not prescriptive and does not specify implementation details for solutions.

While the business view is depicted for eHealth Ontario, this framework can be adapted by any stakeholder. It does not attempt to cover the entire health sector in Ontario, but can be scaled to cover a larger scope.
Governors
eHealth Ontario works with its governors to define its business direction, which includes its mandate, its business strategy, any applicable policies, and its governance processes and structures. Key governors include the Ontario Ministry of Health and Long-Term Care (MOHLTC) and Canada Health Infoway (CHI).

eHealth Ontario Direction
Guides and provides the authority for the business of transforming health care through the use of eHealth. It shapes how the agency’s organization and capabilities are engaged and managed to develop, deliver, and support business services for its stakeholders.

eHealth Ontario Capabilities
Organizational capabilities and internal services/processes that the agency leverages to provide business services to its stakeholders.

Core capabilities: critical capabilities that embody people, process, and technology to realize the eHealth mandate of the agency.

- Health information exchange: the ability to provide a common eHealth platform solutions for integration to support health information exchange in the province
- Infrastructure: the ability to host eHealth solutions and provide access to those solutions
- Health data management: the ability to acquire, manage, and provision health data
- EHealth architecture: the ability to design eHealth models and solutions
- EHealth standards: the ability to ensure interoperability of eHealth solutions
- EHealth privacy and security: the ability to ensure privacy, integrity, and secure access to health information
- Service management: the ability to ensure eHealth service quality and support for eHealth solutions
- EHealth adoption: the ability to support the adoption of eHealth solutions, e.g., through strategic funding

Corporate support capabilities: capabilities that manage and support general operations of the agency—e.g., finance, human resources

Health Services and Support Services
The agency’s service portfolio consists of eHealth services that directly support the health care sector, and support services that support partners and vendors to do the same.
Ehealth Services

Key services that eHealth Ontario provides to the health care sector, directly aligned to the agency’s mandate:

- **Electronic health record services**: support EHR data provisioning and sharing, including the population, maintenance, privacy, and accessing of repositories of clinical health information for health care clients, to actively support health care management and delivery, e.g. content related to laboratory tests, medications, diagnostic imaging, immunizations, shared health records, and consent directives.

- **Health sector identity services**: support identity management, access control, authentication and authorization, including identities for health care clients, providers, and ehealth system users. Examples include the use of provincial registries as authoritative reference sources, and identity federation.

- **Privacy services**: support an individual’s right to control the collection, use, and disclosure of his/her personal health information and/or personal information. Examples: consent directive management, auditing.

- **Communications and collaboration services**: provide communication and collaboration tools and channels to support shared access to health information. Help providers collaborate on client care through point of service system integration, email, instant messaging, portals, information exchange, and other forms of electronic communication or correspondence.

- **Health requisition services**: support creation, sending, and management of health care system requisitions (e.g. orders, referrals, requests for care), including lookup for availability, rejection, wait list management, and scheduling. Examples include lab test orders and referrals.

- **Hosting services**: support the development, acquisition, delivery, and maintenance of datacentre infrastructure for provincial ehealth hosted solutions. Examples include development, testing, and production environments.

- **Health knowledge services**: support the creation, organization, and retrieval of common reference information, for sharing and dissemination across a variety of health care settings. Examples include a repository of standardized clinical protocols, information about coding systems, policies.

- **Health system use data services**: provide electronic information about health and health system activity, in support of the development of business intelligence, analytics, and reporting services throughout the health sector in the province. The data may need to be de-identified (i.e. anonymized), depending on its intended use and the user, to support privacy and legal requirements.

This data will be invaluable for planning, managing, funding, and improving the health care system. It will also contribute to the definition of health care policies, budgeting, and health care performance monitoring.

Ehealth Support Services

Services that eHealth Ontario provides to its partners and vendors to help them develop and deliver health sector services in alignment or cooperation with the agency’s strategy, blueprint, and direction:

- **Strategic planning services**: provide strategic business planning services to partners and vendors who develop and deliver ehealth services, to help them align with provincial direction, strategy, and policies. Provide a province-wide vision and strategy for health and ehealth in Ontario, supported by provincial policies and standards, and a clear understanding of value and accountabilities.

- **Investment management services**: support the making and tracking of ehealth investment decisions, or demonstrate accountability and value through the tracking of outcomes. For example, eHealth Ontario provides and manages funding for delivery partners that is tied to specific deliverables as agreed upon by both parties.

- **Solution delivery services**: provide a standardized solution delivery lifecycle, to streamline development and delivery of ehealth solutions or reusable shared components. These may involve building, buying, and/or reuse.
• **Shared components stewardship services**: promote the development of shareable ehealth components, including providing a repository of reusable components to appropriate delivery partners and vendors

• **Testing and certification services**: support for the testing of ehealth products to assure compliance with expected requirements and standards

• **Standards management services**: support the development, population, maintenance, and accessibility of content that promotes alignment and interoperability across ehealth solutions. Examples include standards, coding systems, nomenclature (terminology), schemas, and other specifications.

### Partners and Vendors

Organizations that partner with, or are procured by, eHealth Ontario to co-develop and deliver solutions and services. An example of a partner is the University Health Network, which is the agency’s lead partner in the ConnectingGTA project.

### Health Sector Services

Services provided within the health industry, which typically include health care delivery and the supporting services:

• **Personal health care services**: provide care to a health care client and enable the hands-on delivery of health care. Examples include services and processes that support accessing a health care client’s health information, and sharing it with other providers caring for the same individual.

• **Public Health services**: provide health support for populations, including population health surveillance, analysis, and reporting; the creation and dissemination of public health communications; the management and investigation of public health issues; and public health promotion

• **Health system analytics and research services**: provide health system intelligence to support management of the Ontario health system and programs, and medical research. Examples include analysis of resourcing, service utilization, health system performance, funding outcomes, trend analysis.

• **Health sector administration services**: support health sector operations, including tracking care delivery costs, human resource management, facility management, training, financial and statistical reporting, and clinical supply management, in order to optimize health care delivery capability

### Consumers

Individuals or organizations that consume the health sector business services. Examples of business view clients include:

• **Health care clients**: people who are eligible to receive, have received, or are receiving health care services in Ontario

• **Health care providers**, who provide the health sector services

• **Health sector managers**, health researchers and others who use ehealth data for uses such as research, analyzing program performance, etc.
The information view provides a model of the information that constitutes an EHR in the Ontario health care system. It offers a structure for managing health information from multiple sources, building a comprehensive record of a health care client’s health. The view defines each piece of information to support a common language between EHR stakeholders, and identifies what information about a health care client is collected, included, and expected at any point in the health care system.
Ontario's Ehealth Blueprint
Information View: Detail

The following diagram shows the detailed view of the conceptual information model.

Ehealth Information Architecture

To support the alignment and integration of the required ehealth initiatives, eHealth Ontario has developed (in collaboration with key stakeholders), Ontario's ehealth conceptual information architecture (CIA).

The CIA is a high-level view of what information constitutes an electronic health record in the Ontario health system, providing broad outlines of how that information should be structured. It is intended for use by all authorized stakeholders for electronic health records in Ontario, including but not limited to eHealth Ontario, the Ministry of Health and Long-Term Care, Ontario health care providers and health care clients, and health care information system vendors.

The CIA provides:
- A common vocabulary to facilitate communication and coordination between parties within eHealth Ontario and across the broader eHealth environment.
- An information structure to guide the planning, design, and data integration of EHR systems.
- A map of information relevant to the business that serves as the basis for information management and governance.
- Conceptual information model (CIM) diagrams and definitions.
- The conceptual information model will be used to enable and fulfill eHealth initiatives in the province of Ontario. Solutions built using the model will have the advantage of a design that promotes and enables integration with other solutions.

Information Management Framework Principles

The following information management principles are used by eHealth Ontario to guide the process of managing information resources. They reflect leading IT practices in managing and using information, forming the basis for relevant policies and practices. All principles are essential in the implementation of a sound information management strategy:

- Information needs are business-driven.
- Information is a public asset.
- Information is shared.
- Information is accessible (for those authorized to use it).
- Information is protected.
- Information is managed using a life cycle approach.
- Information is managed in an integrated manner.
- Information needs to be integrated to support better decision making.
- Information management is everyone's business.
Information View Benefits

This information architecture model provides a common foundation to promote and facilitate integration with other solutions involved in the EHR, enabling stakeholders to leverage a comprehensive set of provincial eHealth information assets. It provides an information structure to guide the planning, design, data integration and governance of health information from multiple sources. It also serves as a reference for organizations building or buying eHealth solutions in Ontario, reducing the time to design a solution, improving the quality of the solution, and ensuring integration with existing solutions.

The model is based on industry standards adapted to reflect Ontario’s health care priorities. Contributing sources include models and standards published by provincial, national and international health organizations, as well as existing eHealth Ontario data model assets. The model can be used by all EHR stakeholders, including eHealth Ontario, the Ministry of Health and Long-Term Care, Ontario health care providers, health care clients, and health care information system vendors.

Information Model Overview

The following diagram introduces the high level subject areas contained in the conceptual information model. Subsequent sections in this chapter will review the model in more detail.

Figure 4: EHR Information Model
Information model definitions:

- **Health client**: a health care client (a person who is eligible to receive, has received, or is receiving health care services in Ontario), or a client supporter (someone who is acting on behalf of or supporting someone receiving health care services in Ontario)

- **Health care provider**: a person or organization providing health care or other health-related services or products

- **Client team**: a group of client supporters and interdisciplinary health care providers working collaboratively with the health care client to support the health care plan. Each client team member is assigned responsibilities to facilitate care for the health care client appropriate to their role.

- **Health care plan**: an integrated care plan, created by a health care client and/or provider(s), to manage the client’s optimal health, to address preventative measures, or to manage existing health conditions. A health care client may have one health care plan, or none. It contains client-centered activities, goals and targets based on best practice guidelines, and is monitored by client team members on a regular basis either directly or through automated and directed notifications.

- **Client health profile**: information about the health care client used to access his/her current health state and potential impacts on future health. It includes a diverse range of information, including, but not limited to:
  - Sensitivities, allergies, intolerances and adverse reactions to substances
  - Health conditions
  - Family history
  - Personal health characteristics
  - Special needs
  - Immunizations
  - Health directives
  - Health concerns
  - Barriers
  - Information consent
  - Emergency contacts

- **Health care encounter**: an event where one or more services or products are provided to assess, maintain or improve a health care client’s health. The service or product may be from a health care provider, or may be self-provided. Any number of outputs may result from a single encounter. Outputs include information categorized by observations, diagnoses, dispense events, intake of substances, clinical procedures performed, requisitions, health care encounter locations, health care products and services provided. Several health care encounters can be linked into an episode of care.

**Health Care Encounters**

- A health care client may have multiple health conditions, which may be transient or chronic. A chronic condition may have co-morbidity with other chronic conditions.

- A health care client may have multiple health care encounters to address one or more health concerns. A health concern may be caused by a life event, and may not necessarily be a health problem, e.g. the need for a medical exam for travel purposes or a pilot’s license.

- Health care providers may be provider organizations or provider persons, and may provide services at a health product location or at other locations such as in-home care or flu shots in a mall or retail pharmacy. Requisitions may include referrals and orders for products or services.

- Two types of health care encounters – those involving a provider person, and self-care encounters – produce health care encounter outputs, although the range of output types from self-care encounters is more limited. Both may involve client supporters, and they occur at encounter locations which may also be a health product location.

- Provider encounters related to the same health condition and the same provider person may be grouped as provider episodes of care, and links between provider episodes of care may also be made. Related episodes may involve the same or another provider person, and may be for the same or different health condition. **Example**: a health care client has separate episodes of care for diabetes and heart disease with different specialists. Each provider contributing to the resolution of the health issue has a set of records to document his/her provider episode of care.

- Health product locations are places where health products are available, and where provider organizations or provider persons operate. A location may be situated within a larger location – e.g. an emergency department within a hospital – or in a separate location such as a clinic or office.
• While the health care encounter represents a care event, the health care encounter output represents the results of that event. There are several different types of outputs, including observations, clinical procedures that may implant devices in health care clients, dispense of devices and medication, requisitions for a health product or a referral to a health care provider, and diagnoses that may identify health conditions.

Health Care Plans

• A plan has one or more plan components to record intended plan health activities, activity goals, and health targets. Fulfilment of these things may come directly from the health care client, or in a health care encounter output.
• A plan component can address one or many health concerns and/or health conditions.
• Clinical guidelines can be used as a base for plan components – for example the Canada Food Guide for developing a nutritional plan, or the Clinical Guidelines for Diabetes Care to help set target test result ranges.
• A health care client can create a plan component with or without input from their client team.
• Client team members may be assigned the right to be involved in the monitoring of plan components.
• Plan health activities may trigger client care notifications such as alerts, reminders or correspondence to the health care client and/or client team members.

Client Health Profiles

The health care client’s health profile consists of six areas relating to his/her health state and health care:

• Health condition, either transient or chronic; a chronic condition may have a co-morbidity with other chronic conditions
• Adverse reaction to a substance such as a drug, food, or other substance
• Sensitivity to a substance (an intolerance or allergy)
• Personal health characteristic: these may be physical, mental, lifestyle, cultural, or behavioural in nature, or may be an immunization, special need, family history item, or health directive
• Barrier to care which may be socio-economic or functional in nature
• Emergency contact: a person to be contacted in the event of a medical emergency involving the health care client

Client Teams

• A client team member is a provider person or a client supporter providing care to a health care client, in one or more client care roles. A client team member may be involved in the development and/or monitoring of plan components.
• A client care role type has one or more standard permissions for specific types of access (e.g. view, update) to different types of health information (e.g. a personal health characteristic or a life event), based on the role played by the client team member. A permission override may be issued by a health care client to supersede an existing permission.
• A health care client may provide information consent for access to their health record.
• Client supporters and health care clients are types of health client from a health system perspective.
**Information Resources**

In addition to the information model for data relating to a health care client’s care, two further categories of information are important parts of the EHR.

---

**Knowledge Resources**

The knowledge resource repositories contain health care reference information for sharing across a variety of health care settings as well as for supporting applications, enabling collaboration and health information integration.

For example, a repository of standardized clinical protocols for surgeries or procedures could be used to support information dissemination to caregivers from an ehealth website portal, but it could also be used by an eReferral data transaction service as part of a referral transaction pathway for a procedure.

Examples of information resources supporting electronic health care issues and implementation include forms, policies, references, coding systems, standards, and links to other organizations playing roles in electronic health care.

Audiences for these resources include the Ontario public, health care workers, vendors, delivery partners, and researchers.

---

**Health System Analytics**

The information electronically captured and recorded about health and health system activity can be used to support the development of business intelligence, analytics, and reporting services throughout Ontario’s health sector. Data used for these purposes may need to be de-identified, to support privacy and legal requirements.

This data will be invaluable in supporting the planning, management, funding, and improvement of the health care system. It can contribute to the definition of health care policies, budgeting, and health care performance monitoring, and can be mined by those conducting clinical research into improved treatment protocols.
The systems view of Ontario’s ehealth blueprint describes the applications, services, and core infrastructure required to build and integrate ehealth solutions in Ontario. It shows how EHR resources and services are integrated and deployed, and how the blueprint is governed.

The view highlights one of the blueprint’s major objectives – developing service-oriented solutions. Using service-oriented architecture, each business function is offered as a standards-based service, which enables it to be repurposed and combined to meet larger business needs, and provides a collection of services that won’t be impacted as technologies evolve.

This section provides an overview of the principles and decisions, technical and implementation views of service-oriented architecture, and the various services and resources that make up the EHR.
Ontario’s Ehealth Blueprint

Key Architectural Principles and Decisions

The systems view has been built using the following architectural principles:

- Integration, interoperability and resiliency: systems will be constructed with methods that substantially improve interoperability and the resiliency of components.
  - Components will be purpose-built to support integration and rapid adaptation.
  - Components are designed using service-oriented architecture concepts and methods, providing persistent and stable EHR capabilities while allowing for flexibility in the selection of new products and services, and the repositioning of existing solutions to maximize value and minimize costs.
  - Components must be replaceable with minimal impact on existing users.
- Standards and open systems: information and technology standards provide the foundation for long-term stability and interoperability. Design choices should be prioritized toward choices should be prioritized toward future stability and interoperability. Design choices should be prioritized toward open systems and the creation of adaptable, flexible, and interoperable, vendor-neutral solutions.
- Availability, scalability, reliability, and maintainability: to ensure high availability of EHR information and services, reliability and availability must be part of their design.
  - EHR components and systems must be scalable in size, capacity, and functionality to meet changing business and technical requirements, and to minimize the application and platform changes required to respond to increased or decreased demand.
- Mainstream solutions: production IT solutions used in the EHR should use industry-proven, mainstream technologies except in those areas where advanced higher-risk solutions provide a substantial benefit.
- Privacy and security: EHR components will be built and/or procured to comply with the privacy and security requirements defined in Ontario law, and will employ adequate safeguards to protect the information they contain and the services they provide and to defend against the broadest possible range of vulnerabilities.
- Service-oriented architecture: EHR solutions should be designed using service-oriented architecture principles, enabling resiliency so that they can be leveraged or extended.
- Technological and operational convergence: EHR solutions should be designed with lower operational complexity in terms of technology, process, systems, and operations, to ensure higher stability, reduced cost, and enhanced delivery and operational capabilities.
- Leverage centres of expertise and build from success: promote the use of best practices and reuse of available artifacts, components, services, and processes.
- Provide multiple ways to interact with services: for example, interaction with EHR services may be provided through portals in a portal, web services, and other means including mobile devices.
- Support versioning and migration: service interfaces are based on standards and long-standing business processes; however, even the most solid standards change over time. By supporting versions of service interfaces, the EHR will allow for new systems to be brought online to consume new features in the EHR without breaking legacy functionality, while legacy features can be phased out in a predictable manner.
- Direct path: when traversing the integrated components of the EHR structure, services should be consumed through the most direct path possible.

The systems view has been built using the following architectural principles:
Service-Oriented Architecture (SOA)

The EHR is built using an architectural design strategy known as service-oriented architecture. The fundamental concepts are that it should be:

- **Service-based**: business functionality is made available in the form of 'services', which can be fairly granular, such as 'get client demographics' (from the client registry (CR)), or 'get lab results for this client' (from OLIS).

- **Specification-based**: each service conforms to a specification describing how to use the service interface specifications or contract.

- **Re-usable**: once a service definition is complete and published, one party can write a program to provide the service exactly as described in the service definition. Another party can use the service by invoking it as described in the service definition. Both the provider and user of the service can independently build the service and implement applications to use it without needing to know how it is implemented or deployed.

- **Combinable**: services can be combined to execute larger business processes, transactions, or applications.

This service-oriented approach allows eHealth Ontario to create and publish a collection of service interfaces for each of its key offerings. As long as the main business elements don’t change, the service interfaces remain the same. By using service-oriented architecture, the technologies that use the EHR can remain independent from the technologies that provide the EHR. Consequently, the technologies underlying the business services can change independently as eHealth Ontario and its partners evolve, providing an effective long-term approach to business interoperability while avoiding technical stagnation.

Characteristics of Service Oriented Architecture Services

- **Reusable**: depending on their granularity, services can be used by multiple processes and other coarse-grained services.

- **Autonomous units of business functionality**: each service provides a business function that is independent of other services.

- **Contract-based**: interface and policies are strictly described by an interface specification.

- **Loosely coupled**: service contracts are designed to be as independent of the service implementation as possible, minimizing the need for service contract changes if the implementation changes. In a tightly coupled system, an implementation change (e.g. a change in a back-end data type) would require a change to the interface and therefore the connecting systems.

- **Platform-independent**: both the consuming and SOA service systems can be on any platform that supports the service transport and interface requirements.

- **Discoverable and location independent**: services are located through a service registry/catalogue and accessed via universal resource locators, and therefore may move over time without disruption to consuming systems.

- **Standards-based**: services are built, consumed, and described using standards such as Web Services Definition Language (WSDL), which provides information about the service, and Simple Object Access Protocol (SOAP), a packaging mechanism.

Enabling a Service-Oriented Approach for the EHR

Using a service-oriented architecture approach for the EHR allows the components to develop independently and organically. The only fixed elements of an interaction are the types of information exchanged and the rules that apply to the exchange between the EHR and the consuming system. For any service that is discovered through the service catalogue, anyone building software or designing solutions can expect consistent behaviour over a long period of time, regardless of technical changes at eHealth Ontario or any of its delivery partners. The Health Information Access Layer (HIAL) is the broker and mediator for these exchanges, ensuring that all parties abide by a common set of rules.

Organizations and vendors will have access to a selection of components with predictable behaviours which can be used as building blocks for innovative solutions that support the health care community.
Systems View Components:

The systems view has four major components:

- **Access points:** includes the point of service applications that access, populate and use the EHR, along with supported channels and examples of device types.

- **HIAL services:** manage secure access to the EHR and provide communication and common services while protecting privacy. They also expose all supported provincial and regional business service interfaces.

- **EHR resources:** includes registries, domain repositories and EHR applications. Will also include de-identified information and analytics capabilities for health sector managers and researchers, as well as knowledge resources including reference information, and educational materials.

- **Core infrastructure services:** infrastructure and services that support the building, implementation and operation of the EHR.

Access Points

Access points include laboratory information systems (LIS), portals, electronic medical record (EMR) systems, hospital information systems (HIS), and pharmacy systems used in labs, clinics, hospitals, pharmacies, home care settings, and community services, all of which provide access to health care information and sources of requests for health care information. Health care clients, providers, health sector managers (end users) and researchers use these access points to automate business, clinical, and information practices and processes, as well as to support program and research functions.

*Access points provide access to the EHR through a data or web access channel. In order to get, put or use EHR data in a secure and interoperable manner, they use standards-based integration tools and interoperable specifications to connect to the HIAL. Access to EHR data is provided by standard messaging formats such as HL7, through provincial and business services exposed by the HIAL.*

One of the EHR principles is to minimize changes to clinician workflows by facilitating access from existing point of service applications, so users can use familiar tools to access health information from EHR sources with minimal disruption to their working environment.

Portals

These are we sites that provide a single point of access to online services for a target group of users, aggregating information from multiple sources and presenting it as a unified whole. Standards-based web portals are a key delivery channel for sharing EHR information.

The anticipated portal landscape will include portals serving user groups or aggregating similar content and services, such as:

- Provincial and regional portals
- Special focus portals run by health care organizations with specific interests, such as Cardiac Care, Cancer Care Ontario
- Provider-managed portals run by hospitals or other health care organizations
- Consumer health portals for the general public to access their health information and services

Individual portals are integrated into a federated, standards-based, province-wide structure, offering shared content and services to stakeholders. All ehealth portals will be technologically...
interoperable, able to use a province-wide authentication and authorization framework, and will follow taxonomy and component construction standards to simplify integration and content sharing.

**Provincial and Regional Portals**

Designed to offer a wide selection of information and functionality from different sources across the province, these portals provide reference implementations of EHR functionality and core infrastructure for applications that will be used by providers and health care recipients.

These portals will:

- Be based on common portal standards, to promote sharing and reuse of portlets. This will reduce development, implementation and ongoing support costs, and will promote a common presentation of clinical data. Individual portlets, e.g. for labs or medications, will be able to share context and be presented together to provide clinicians with a more complete health care client perspective.

- Provide web-based access to all eHealth Ontario core services, such as labs and medication management

- Provide users with local, regional and provincial assets in one location

- Facilitate the rapid deployment of new health applications and information repositories

- Provide contextual references to associated sites, agencies and organizations

**Portlets**

eHealth Ontario will deliver EHR functionality in the form of portlets, each of which will support a line of business, e.g. drugs, labs, diagnostic images, and will provide the user interface capability for viewing and updating data in those systems.

Examples:

- A portlet for finding a health care client in the client registry

- A portlet to retrieve a health care client’s lab results from OLIS
• A portlet to retrieve diagnostic imaging reports from the provincial diagnostic imaging repository

Portlets provide quick and widespread access to data, while ensuring that it is presented in the same way everywhere to all users. This is critical for avoiding misinterpretations of health care client health information.

Delivery partners will be able to implement their own portlets, and leverage standards that promote sharing and consistency across portlets.

Provider-Managed Portals and Web Applications

Since providers have the strongest relationships with health care clients and the deepest understanding of their health issues, organizations such as large hospitals may create their own web-based access channels for communication with staff and health care clients. These portals will also be able provide access to the EHR.

Examples include:

• Hospital portals for internal health care staff
• Hospital web applications for health care clients
• Radiology, labs, or medication web access interfaces
• Primary care web interfaces for health care clients
• Community care health care client and provider web applications
• Pharmacy portals for health care clients

Some providers may be able to access health care client information using local technology such as a connected (local) EMR. Other providers who do not have this capability can access the EHR via a portal.

Web technologies such as portals will allow access to elements of the EHR, enabling eHealth Ontario to deploy features broadly and rapidly as new services are available.

Special Focus Area Portals

Ontario has a number of organizations dedicated to the care and treatment of health care clients with specific requirements, and these organizations’ use of and participation in the EHR is supported. Reusable, standards-based portlets will enable rapid deployment and adoption of appropriate features for the special focus area. Provincial and regional portals can maintain links to these special focus portals, providing context-specific references and extending the continuity of experience for users.

Consumer Health Portals

These are portals accessible to anyone in Ontario. The blueprint allows for the future implementation of consumer health portals, to provide health-related information to any user of the health care system. Consumer-oriented functionality can be provided through consumer portlets presented across multiple delivery partner portals.

The consumer experience will provide users with access to information and services to allow them to be more engaged in their own health care, to better navigate the health system, and to interact with their providers.
Health Information Access Layer (HIAL)

The HIAL is an architectural concept for providing communications services, common services and supporting components to broker data and service requests from point of service applications.

The HIAL does not persist business data. It does not run the database systems that maintain the business and clinical information tied to specific clinical domains, and is generally not responsible for maintaining or applying the business logic that is specific to a line of business. The core business and data processing logic associated with a clinical domain is expected to be handled and processed by the line of business application itself, once the HIAL passes the appropriately-formed service request to it. The HIAL's fundamental capabilities and duties include the following:

- Acting as the central transaction coordinator for all EHR services exposed by the HIAL
- Recognizing and having awareness of all transactions handled by the HIAL
- Coordinating the execution of all EHR transactions from start (service request) to finish (service response sent to requester)
- Monitoring and managing the state of all EHR transactions
- Monitoring, controlling and routing of message exchange between services
- Resolving and managing contention between communicating service components
- Controlling deployment and versioning of services
- Providing commonly needed transaction processing services including event handling, event choreography
- Data transformation and mapping; message and event queuing and sequencing; security; error/exception handling; message parsing and validation; protocol conversion; enforcing proper quality of communication services
- Providing commonly needed and commoditized EHR business services, including: validation of the asserted authentication of the end user involved with a transaction; role-based service access; authorization of the end user involved with a transaction; application of coarse-grained consent directives for disclosure of information
- Validation and resolution of key enterprise reference identifiers for transactions, including client, provider and provider organization involved in clinical transactions
- Catering for the optional application of business logic rules associated with specific business domains

The following sections provide more details on the three major areas of the HIAL services, namely, exposed business service interfaces, communication services and common services.

Example: A point of service system requests the 'get lab result' service for a health care client as part of the larger business service of managing lab results and reports. The system or user requesting the service does not need to know how to interface with the registries, domain repositories and applications; it just needs to know how to request a service that is exposed through the HIAL.
The HIAL exposes business services that provide information from the shared resources layer. By doing this, the HIAL logically decouples the technologies and implementation details that consume EHR services from the technologies and implementation details that provide EHR services.

The benefit of this approach is that decoupled technologies are free to innovate and change without directly impacting each other or the users. Changes can be made to shared resources without impacting the users who are requesting services from point of service systems or portals. Service consumers need only request a service that is exposed through the HIAL – they need not concern themselves with how that service request is implemented.

The services exposed in the HIAL are the external interfaces to be used by point of service applications. The actual domain repositories, registries, and applications are ‘below the HIAL’ in the diagram and expose their native interfaces to it. The HIAL uses these to orchestrate the response back to the requesting system.

The HIAL exposes business services via interface contracts which will be used by point of service systems to access or put information in to the EHR. The implementation of these services will include orchestration that will involve the HIAL calling common services and accessing the registries, domain repositories and other resources in the shared resources layer, using their native interfaces.

- **Registry services**: include client and provider registry services, consent directives, etc. Examples of operations that are supported by these service interfaces include:
  - Identify client, update client, verify client
  - Identify registered provider, update provider, find provider, view provider location
  - Manage health information consent directive, apply consent directive

- **Domain repository services**: include services for the domain repositories such as labs, drugs, clinical data repository (CDR), etc. Examples of operations exposed through these services are:
  - Capture client health data
  - Search client health information, view client health information (summary or detailed, data or document)
  - Create laboratory test requisition, search/view laboratory test result
  - Capture diagnostic image and report, view diagnostic image and report
  - Capture immunization event detail, view immunization history

- **Other services** exposed by the HIAL include EHR application services, regional application services, portlets, and health management and research services.
Communication and Common Services

Communication Services
The HIAL is the integration point between all point of service applications and service providers. Both EHR service consumers and service providers communicate through this layer, removing the need for them to create and maintain their own point-to-point connections with each other. The communication services provide all the necessary services to connect and send and receive messages in the appropriate formats.

These services are the gateway layer that creates the separation between the point of service applications and the registries, domain repositories, applications, and other resources. They allow point of service applications to connect and access, put, or use information in the shared resources layer.

Messaging
Encrypt/decrypt: responsible for encrypting the communication channel between the service consumer and the HIAL, usually via an encrypted Transport Layer Security (TLS) connection with an asynchronous key exchange. Messages passing through the HIAL need to be parsed for processing, so the incoming messages should not be encrypted by the service invoker; the encrypted channel provides sufficient security.

Parser: breaks a data structure into smaller elements according to a set of rules that describe its structure. For example, a phone number consists of an area code, prefix and suffix. In the eHealth Ontario context, examples of standards the parser must support include HL7v2 (pipe delimited and XML), HL7v3 and XML.

Encode/decode: encodes and decodes messages from and to different coding formats such as UTF-8, EBCDIC, and Base64.

Serialization: packages the message in the destination format, e.g. XML, flat file positional, flat file fixed field length.

Context
Caching: manages the cache and provides functions related to cached responses based on configured settings. The purpose of caching is always to drive performance improvements.

Session management: performs security session management so all services and transactions are ‘idempotent’ (i.e. giving the same result no matter how many times they are applied) and thus ‘stateless’ in nature. This means that exposed services do not store ‘stateful’ data that could be reused across multiple consumer service calls. Security sessions are an outcome of the use of the authentication service – applications insert a security token as part of every service invocation and the session management service validates the security token to control the session’s lifecycle.

Protocol
Application protocol: supports the use of application level communication protocols to enable communication channels with point of service applications. Application layer functions typically include identifying communication partners, determining resource availability, and synchronizing communication. This service will support MLLP, HL7v2.x, HL7v3, XML, SOAP 1.1, WS-ADDRESSING, WS-NOTIFICATION, WS-SECURITY, WS-SECURITYPOLICY, WS-POLICY, WSDL, HTTP(S), (S)FTP, Connect Direct (mainframe), SMTP, SNMP, and TLS 2.1 (OSI Layer 6) and others that will be required in the future.

Network protocol: provides communication capabilities over physical networks. The primary network protocols that will be supported are TCP/IP and IP/SEC.

Integration
Interoperability: provides the capability required to support interoperability at various levels within the EHR.

Service catalogue: a central repository or service registry that allows for the cataloguing of eHealth Ontario services. It allows service consumers to search for details about service providers, the functional areas (taxonomies) these services address, and binding details (location, service contract, transport, etc.) for services.

Broker: provides support for brokered HIAL patterns, where several HIAL segments can participate and fulfill services. It allows for service requests to be evaluated and brokered to other HIAL segments or separate transaction processing environments.
Routing: routes messages to internal integration channels. Routing service functionality includes static/deterministic routing, content-based routing, rules-based routing, and policy-based routing.

Mapping: creates a map file that translates a source document format to the destination format, including mapping of fields and mapping using business rules or algorithmic conversions.

Queuing: provides store and forward capabilities. Message queues provide an asynchronous communications protocol, meaning that the sender and receiver of the message do not need to interact with the message queue at the same time. Messages placed into the queue are stored until the recipient retrieves them. The message queuing service provides enhanced resilience functionality to ensure that messages do not get lost in the event of a system failure.

Alert/notification: provides support for handling system alerts. For example, when an alert condition is triggered, the service notifies the corresponding users and/or systems. This service ties into, and works closely with, the publish/subscribe service. An alert notification is triggered by an event that may occur at the HIAL level, at the point of service level, or at the line of business application level. When an applicable event occurs, an alert is pushed out to appropriate recipients via email, fax, phone, SMS or pager.

Publish/subscribe: used to decouple providers and consumers of EHR data. It allows the producers of data to publish information to a topic with no knowledge of the recipients of that data. This service is used for system-to-system communication only.

Management

Management: provides tools to monitor service execution and enforce policies in order to manage the availability and performance of eHealth Ontario services. These tools include dashboards for monitoring, and service level arrangement reporting for application services. They also cover exception and error reporting and management for the HIAL, and transaction processing.

Configuration: provides centrally-established capabilities to manage the parameters of EHR services.

Exception/error handling: provides an interface to raise and manage errors and other business level exceptions. Exceptions can range from system/application level exceptions to exceptions found as a result of corrupt or invalid data and other such conditions.

Logging: allows for the construction of immutable auditable logs for the purposes of traceability, dispute resolution, security, privacy, and compliance with policy (external and internal) and laws. It does not refer to ‘system’ logging that is normally produced for system and application debugging.
Common Services

Common services promote the reuse and consistency of approach in performing common functions. They also relieve clinical domains of the need to build this functionality into their own repository logic.

Since all messaging traffic must go through it, the HIAL is an ideal place to provide these common services – handling tasks that are required across all lines of business and user types. Examples include: logging, auditing, consent management, authentication, authorization, and virus checking.

Providing these services centrally has a number of benefits, including:

- Point of service and line of business systems don’t need to handle these functions themselves; offloading responsibility for these things allows the systems that connect to the HIAL to be more streamlined and effective. It also reduces time to market for new innovative EHR solutions.
- Each of these functions can be applied in a consistent, reliable, predictable manner.
- Management of each of these functions (including maintenance, enhancements) is far easier.

Security

Authorization: ensures that the identified service consumer is allowed to access a controlled resource in a specific way. The HIAL implements a policy enforcement point (PEP) which validates that the service consumer has been authorized for the request that is being made. Authorization is rule based; the rules are defined within the user registry’s policy decision point (PDP), which is a XACML-based rule engine.

Authentication: refers to the policy enforcement point that ensures service consumers are identified. The HIAL implements a policy enforcement point that asserts the service consumer authentication. Services offered through the Ontario HIAL solution leverage a federated identity model.

Access control: the gating of access to secured components, through policy enforcement points at run time

User registry: enables and authorizes providers for access to EHR services. Leverages existing electronic credentials used by providers and health care clients, and binds them to their provincial identities in the provider and client registries. By knowing the real identity of providers and health care clients, the user registry can authorize EHR transactions to ensure their compliance with privacy and security policies, apply coarse- and fine-grained authorization rules, and ensure that only authorized individuals access PI and PHI.

Public Key Infrastructure (PKI): the hardware, software, people, policies, and procedures that create, manage, distribute, use, store, and revoke digital certificates. The PKI is required for digital signature and encryption.

Digital signature: a cryptographically strong electronic signature which typically depends on the PKI.
Privacy

Consent directives management: allows users to block access to their PHI through directives that are checked and honoured during execution of transactions by the HIAL.

Auditing: records events in an immutable log, which can be used for subsequent investigations.

Other Common Services

Portal services: the services required to support portals; includes portlets, the context framework and other related capabilities for portal integration.

Terminology services: provide a consistent interface and set of functions to manage and use terminology for a clinical domain. May include vocabulary lists, value sets, taxonomies, concepts, relationships. An example is translation of vocabulary used in a message to make it understandable to the receiver.

Message transformation: transforms message structure from an input format to an output format by applying a map retrieved from the mapping service.

Policy management: provides an interface to configure, manage and enforce policies for access, auditing, logging, and consent, etc., as required for operation of EHR services.

Line of business orchestration: provides a means to automate and integrate multiple services that execute on heterogeneous platforms into a business process or workflow. Specifically, it invokes activities or services in a particular order; according to a set of rules; manages the complex flow logic and process state, and correlates responses from downstream and upstream systems to a service orchestration instance.

Line of business realization: the HIAL orchestration level activities that are implemented and customized for each line of business service integrated through the HIAL.

Portlet services: help eHealth Ontario portal services facilitate secure and simple access to services provided by eHealth Ontario line of business applications, and integrate into regional and third-party value-add solutions. This enables the aggregation of content and web services from remote sources across many organizational boundaries on numerous application servers.

Example of HIAL Processing

An advantage of a service-based approach is that specialized components can be created and used like building blocks in business processes. The ‘orchestration’ features of the HIAL allow eHealth Ontario and its partners to take advantage of this strategy to enable flexibility and agility.

Orchestration manages the order and operations required to process a composite business transaction. It automates and integrates multiple services, executing on heterogeneous platforms, into a composite business process or workflow. It invokes activities or services in a particular order; according to a set of rules; manages the complex flow logic and process state; manages transactions and error handling; and correlates responses from downstream and upstream systems to a service orchestration instance. Processes are modeled in the abstract, with subsequent specification of technical details for the implementation of individual process steps. Business process interactions are not hard-coded, making it easier to change process definitions to adapt to new business requirements.

Using the example of a service request for data related to lab tests, the orchestration might start with a call to a security service, and then proceed to a transformation, before calling the laboratories repository. Subsequently, the continuing orchestration might check with the consent management service (and any resultant masking of data) and submit a copy of the response to the audit service before returning information. The sequence of orchestration steps can be redefined as necessary, for example to reflect a change in a business policy.

Figure 8 provides a high level process flow of what happens when a request enters the HIAL from a point of service application. At the highest level, the HIAL receives the request and carries out processes on the message (A). It then (B) sends the request to the line of business system which fulfills the request and sends it back to the HIAL.
The HIAL then runs a few more processes on the response and then sends it to the requesting point of service application (C).

Figures 9-11 provide details on what happens once the inbound data request is received.

A: The message is first validated and transformed as required. Authentication and authorization checks are carried out. Then the appropriate orchestration is prepared, which is the process flow developed for the request – this will mostly be generic but at times may contain activities that are specific to a request. This is followed by verification of the client, providers, and terminology. The output is a validated and normalized message.

B: (Figure 12): Once the activities for the received inbound request are carried out, the message is prepared to be sent to the line of business system. The line of business system processes the request sent by the point of service application through the HIAL and returns its response to the HIAL.

C: The HIAL (Figure 13) adds any required information, logs appropriate information for audit purposes, prepares the response message, and sends it to the point of service application.

The process flows show how a request from a point of service application is fulfilled by the line of business system through the integration capabilities of the HIAL. The HIAL transparently and seamlessly integrates the line of business, the various registries, and other services such as logging, auditing, consent etc., and provides a single point of entry for the point of service application. Without the HIAL, the point of service applications would have to know the technical details of each line of business system and all the registries, and how to communicate with them.

The following are the steps taken for a representative EHR service request. In this example, a physician (Dr. Jane) is treating a health care client (Bob). Dr. Jane wishes to use her point of service application (an EMR system) to get a lab test result from the EHR repository of lab test results (OLIS). The HIAL will:

- Receive a message from Dr. Jane’s EMR system for the transaction, via an approved communication channel and interface
- Decrypt, parse, and interpret the envelope surrounding the message
- Identify and launch the appropriate orchestration to fulfill this type of transaction
- Invoke security services to validate Dr. Jane’s identity and her authorization to use this transaction
- Log the transaction and its contents, as required
- Decrypt, parse, and interpret the payload of the message
- Validate identifiers for key entities referenced in the message (Dr. Jane, Bob, any other providers or provider organizations involved)
- Validate conformance with terminology standards (e.g. the code for the lab test)
- Apply any applicable consent directives from Bob
- Prepare a transaction and invoke the provincial lab repository service to fulfill the request
- Receive the response from the lab repository
- Apply consent directives to the response, masking data as appropriate
- Package, encrypt, and send the response back to Dr. Jane’s EMR system
- Throughout, provide overarching services such as session management, system logging, management of alerts and errors, etc.
Figure 8: HIAL High Level Process Flow

Figure 9: HIAL Processing of Input Message

Figure 10: HIAL Processing of Input Message
ASSIGN TRANSACTION ID

PERFORM MESSAGE HYGIENE

VALIDATE THE INPUT MESSAGE

PERFORM BUSINESS LEVEL SOAP HEADER VALIDATION

CONNECTION ESTABLISHED

FROM

LOCATION REQUEST SOAP MESSAGE

Figure 11: HIAL Processing of Input Message

ASSESS CONSENT (PRE-INVOCATION)

PERFORM SERVICE INVOCATION: PREPARE OUTBOUND REQUEST

PERFORM THE INVOCATION: PREPARE SPECIFIC TASKS

INVOKE BUSINESS APPLICATION SERVICE

STANDARD RESPONSE READY

PERFORM POST-INVOCATION: LOB SPECIFIC TASKS

RECEIVE BUSINESS APPLICATION SERVICE REALIZATION

CONTACT SERVICES: LOB REALIZATION

« SEQUENCE FLOWS»

LOG CONSENT SUCCESS

LOG CONSENT SUCCESS

Figure 12: Sending Message to LOB

IN: TRANSIENT DATA

RETRIEVE WARNINGS FROM TRANSIENT DATA

ADD WARNING(S) TO RESPONSE MESSAGE

SEND RESPONSE MESSAGE

FROM

RESPONSE MESSAGE READY

LOG CONSENT SUCCESS

CREATE AUDIT LOG ENTRY FOR SERVICE REQUEST (COMPLIANCE MANAGER)

RESPONSE MESSAGE SENT

Figure 13: Response Message
Records containing identification of health care clients and providers come from multiple sources, some of which may use identifiers that are only valid locally. The provincial registries support the concept of enterprise-wide identifiers to provide a common link for all identifiers for the same person, as required by the line of business. The registries will contain current, trusted information about health care clients, health care providers, EHR users, consent, systems, and terminology. They will serve as definitive reference sources for unambiguous identification and verification. As the EHR and ehealth evolve, requirements for additional types of registries may be identified.

Registries not only include reference data, but also basic functionality that allows data to be managed (e.g. put, get/search) by authorized users in accordance with applicable privacy law.

### Client Registry

Every person who receives care in Ontario, regardless of their eligibility for government funded health services, is to be unambiguously identifiable by a unique identifier, used uniformly across the province.

A health care client is a person who is eligible to receive, has received, or is receiving health care services in Ontario. The client registry is the definitive source for a health care client’s identity, facilitating the unique, accurate and reliable identification of individual clients and others who receive care in Ontario, across the disciplines in the health care sector.

It contains demographic and identification cross-reference data for health care clients registered in one or more Patient Identifier Domains (PID) for which eHealth Ontario, as a result of policy/program/IT decisions, has established a data sharing agreement with the respective organizations.

The registry is fed by a number of data sources, including the registered persons database (RPDB, used by OHIP), systems that are used by hospitals to track admissions, discharges, and transfers (admission, discharge, transfer (ADT) systems), and other systems that participate in health care services. It includes the functionality of the Enterprise Master Patient Index (EMPI), a service that matches records from different sources referring to a single health care client. For example, someone may have been treated in several hospitals, each of which has a record but uses a different, hospital-specific identification number. It is important that the EHR be able to recognize that these records all actually refer to the same individual.

The client registry is designed to address the business need for positive identification of clients.
Examples of services provided by the registry include:

- Validating health care client identity information
- Searching and resolving information from multiple sources that refer to the same health care client identity
- Obtaining summary and detailed demographic information about a health care client
- Adding and updating a health care client record
- Merging and unmerging health care client records (because they either do, or do not, refer to the same individual)
- Reconciling duplicates
- Managing publish/subscribe notifications of adds, updates, merges and splits to downstream systems

**Provider Registry**

The provider registry is the authoritative source of information about providers and health care service delivery locations for use by all EHR solutions. It facilitates the unique and accurate identification of any individual or organization that provides health services in Ontario, or who participates in the collection, use, or disclosure of PHI across the continuum of care.

The registry assigns a unique provincial identifier to each provider and maintains information about them, including professional accreditations (e.g. licences, professions, specialties). It is fed by regulatory colleges, Ministry of Health and Long-Term Care databases, hospitals, and other organizations.

The provider registry is designed to address the business need to:

- Positively identify providers
- Provide information on providers, including credentials, status, documented restrictions of activity, work locations, and relevant health care organization affiliations and local privileges.
- Examples of services provided by the registry include:
  - Searching and resolving a provider’s identity
  - Searching and getting provider organization data and locations

**User Registry**

The user registry provides services to ensure the validation and authorization of user and system access to EHR services (i.e. the right people have access to the right information).

The registry communicates with client and provider registries and other resources (e.g. the system registry) as required, applying business rules and tracking federated users. It allows (or denies) secure electronic access to services and resources by enforcing business rules and policies to determine whether or not a user is entitled to access an EHR service.

The user registry is designed to address the business need for:

- Secure access by providers to EHR services, including federated providers
- Secure access by individual health care clients to PHI
- A simple but secure registration and user verification process
- Single sign-on access – i.e. allowing approved, trusted providers to use their existing identity credentials to access shared eHealth Ontario resources

**System Registry**

The system registry is the definitive source of identity information for all systems which consume services from eHealth Ontario. It enables the tracking of consuming systems as well as any relevant attributes such as system certificates or object identifiers. It also stores application-specific information (e.g. identifiers, limitations, constraints, entitlements) for the applications that a system is consuming from eHealth Ontario. System registration information is captured and maintained by leveraging eHealth Ontario solutions.

Each application determines the authorization rules for its service. Depending on the nature of these rules, the system registry may be invoked by the user registry as part of a run-time service entitlement event.
Consent Registry

A consent directive is defined as express instruction(s) from a health care client (or someone authorized to act on the client’s behalf) to his/her HIC, regarding the collection, use, or disclosure of the client’s PHI. The consent registry is a repository that stores and manages the consent directives issued or withdrawn by health care clients, with an accompanying policy store/rules engine to enable enforcement based on roles and access rules.

Health care clients will be able to create, modify, and revoke their consent directives, which will be enforced to restrict the use and disclosure of PHI. Providers may override consent directives under certain conditions, i.e. with a health care client’s express consent or under conditions permitted by applicable law. All consent-related updates and overrides will be logged, and notifications of override transactions will be provided according to business rules.

Terminology Registry

Health care systems may use different local names, codes, or wording for the same clinical concepts – for example, labs may have different names or numerical codes assigned to a lab test. When health care data from different sources is being shared, it is essential to be able to translate or resolve these differences, to ensure correct interpretation by both people and systems.

These naming schemes are called vocabulary or terminology, and commonly originate and are governed by terminology authorities with editorial rules and licensing rights. Rules for mapping/translating from one set of terminology to another must be established and stored in accord with terminology best practices. Authoring and mapping tools will be used by terminology specialists to support the creation and maintenance of the terminology value sets and associations that are ultimately stored in the registry.

EHR Applications

EHR applications are a class of systems that provide data taken from multiple domain repositories and registries in the EHR for more sophisticated and specialized use.

These are more function-rich than the domain repositories, which consist in general of data stores for a single clinical domain with only basic services to enter or retrieve data or perform simple operations (e.g. get, put). Some examples of these EHR applications include:

Chronic Disease Management

This may include data about health care clients with targeted chronic diseases. Application features may include rules for identifying ‘at risk’ individuals, or mechanisms for health care clients to enter self-test results or monitor their own progress.

Personal Health Management

This provides the tools that allow health care clients to leverage the personal health repository to store, retrieve, and manage information about their own care – e.g. a record of appointments, email correspondence with providers, information about medications, and interactions with online patient groups.

Resource Matching and Referral (RM&R)

A referral is when one provider requests a service, care, support, and/or advice from another, on behalf of a health care client. It may or may not result in a transfer of care. Resource matching and referral (RM&R) is an electronic information and referral system that matches health care clients to the earliest available services that best meet their needs.

This solution queries a directory of facilities, programs and services that meet the client’s needs within an identified level of care. Once an appropriate facility and service have been identified, an electronic referral, or eReferral, directs the health care client from a source caregiver to a target caregiver (health
professional or institution), recommending the required type and level of care. For example, users could locate a suitable long-term care facility for a health care client who is currently waiting to be transferred from a hospital.

The RM&R solution will support:

- Resource matching: determines which facilities/providers offer the programs and services required to meet the health care client’s needs within the identified level of care
- Referral management: creates, sends, revises, updates, and responds to a referral
- Reporting: provides reporting capabilities on referral processes, patterns, wait times, and gaps in programs/services
- Communication with external systems: communicates with external systems such as EMRs, hospital information systems (HIS), Community Care Access Centres (CCACs) information systems, provider information systems, and external reporting and registries, to complete the referral process

Public Health

This is a class of EHR applications designed for use by public health units. An example is the Panorama application, which includes a pan-Canadian public health immunization and infectious disease surveillance solution. Panorama is designed to revolutionize public health surveillance, improve preparedness for health emergencies, and support improved protection of Ontarians (and Canadians) against emerging and ongoing threats to public health. Having access to timely information will help public health professionals efficiently manage cases and outbreaks of infectious diseases, improve delivery and tracking of immunizations, and better manage vaccine inventories.

The immunization-related functionality in Panorama will initially be used by all 36 public health units across Ontario, as well as the Public Health Division (PHD), the Public Health Ontario Agency, Ontario Government Pharmaceutical and Medical Supply Service (OGPMSS), and eventually First Nations and Inuit communities.

The full list of core function modules planned for eventual implementation in Ontario is:

- Immunization management
- Inventory management
- Surveillance analytics – business intelligence
- Investigations management
- Outbreak management
- Notifications management
- Work management

Wait List Management

These are applications providing services related to the establishment of lists of health care clients waiting for services, deriving geographic, service, procedure or population-based wait time statistics.

eScheduling/Booking

These are services related to resource and time management for the organization, locations, and services of the broader health sector. They will involve the use of standards for publishing free/busy information from existing scheduling systems, but this is not intended to suggest that a common scheduling system will be implemented province-wide. Some of these services are already offered through HIS, EMR, and private sector vendors. eHealth Ontario may not implement any such systems, but may provide standards and guidelines for vendors.
Access to, use of, and entry/modification of information in the repositories is managed through service interfaces exposed by the HIAL. Using the HIAL creates an important level of abstraction, so that consuming systems can exchange data with these domain repositories without needing to interact with, or know the details of, their native interfaces – the consuming systems simply use a published service end point that is exposed at the HIAL.

These applications are designed to ensure that high quality data pertinent to a line of business is properly managed and adheres to the rules of that line of business. They are provincially owned and are accessible to authorized requestors.

Data exchange with these repositories can be two-way. For example, laboratory information systems may populate lab results into the laboratory domain repository, and health care clients and providers may view lab results from the same repository. Access to the various clinical repositories, in combination, enables the user to compose a multi-disciplinary clinical picture of a health care client.

**Drug Repository**

The EHR drug system will include a comprehensive drug profile system (CDPS) and a prescription service.

The CDPS supports the centralized storage and retrieval of dispensed health care client medications, and provides application services supporting dispensing activities. A knowledge repository of clinical support tools and information will be provided, for informed decision-making. The CDPS will provide related services like performing drug utilization reviews (DURs) and viewing health care client profiles. The DURs identify any conflicts between the medication being prescribed and what is known about the health care client, including previously prescribed medications, allergies, intolerances, drug interactions.

The prescription service will support electronic authorization and transmission of prescriptions from primary care prescribers to community pharmacists.

**Diagnostic Imaging Repository**

Diagnostic imaging repositories contain health care client diagnostic imaging reports and digital images such as x-rays, MRIs, and ultrasounds. There are four diagnostic imaging repositories in Ontario (known as DI-Rs), each serving a different geographical area in the province.

Diagnostic Imaging Common Services (DICS) will provide a way of searching and exchanging diagnostic images and reports from across all the repositories. DICS will leverage common services, such as a terminology service, an XDS-I registry and repository, consent, and audit.

**Domain Repository Services**

Disciplines in the health sector are referred to as clinical domains or line of business systems.

**Domain repositories are applications that collect, store, and support the use of clinical data about health care clients for a clinical domain. They also provide business services for accessing and managing the data. Examples of domain repositories include drugs, labs, diagnostic images, immunizations, and clinical data repositories.**

**Laboratory Repository**

The laboratory repository, implemented as OLIS, is a single provincial domain repository that allows all laboratory test order and result information on people in Ontario to be exchanged electronically and securely between authorized practitioners and laboratory service providers. It also provides the Ministry of Health and Long-Term Care with de-identified program management information.

The repository is responsible for managing and storing all laboratory test orders and reports. Data is currently transmitted to OLIS when lab technicians submit lab test results. In future, data will also be transmitted to OLIS when providers order lab tests.
Immunizations Repository

Another key type of data required in the EHR is information about immunizations. Immunization data is entered and reviewed by physicians, clinical staff, and public health providers, using point of service applications in hospitals, Community Care Access Centres, public health locations, and primary care clinics. This information will be assembled, stored, and managed as part of a public health surveillance application, known as Panorama.

Clinical Data Repository (CDR)

EHR initiatives in Canada have initially focused on sharing electronic information in the clinical lines of business, especially labs, drugs, and diagnostic images. This focus was adopted to fulfill the immediate needs of clinicians through information sharing. However, clinicians want to share and access other types of information when providing care. These will be stored in the clinical data repository.

Examples include adverse reactions, sensitivities, allergies, intolerances, health concerns, health conditions (a health state that persists over time and requires intervention or management as opposed to a point-in-time observation), personal health characteristics, health care plans, client teams, episodes of care, encounters, etc. The CDR will also store information such as hospital discharge summaries, consultation reports, emergency department reports, medication and drug profiles reports, cardiovascular, neurophysiology or respiratory reports, community care reports, etc.

Access to the CDR information will be subject to consent directives. Information will be fed from a variety of heterogeneous, non-interoperable sources, which will be heavily dependent on the definition and use of standards for clinical data types, including terminology standards and common metadata. Services will allow users to search, list, retrieve, enter, and update information. As far as possible this information will not overlap with that in other repositories, e.g. the authoritative source for lab data will still be OLIS.

Personal Health Repository

No decision has been made at a provincial level regarding the approach to having health care clients access their own PHI. The blueprint recognizes that as consumer ehealth services evolve, health care clients may wish to manage and update some kinds of data for themselves, such as a record of appointments or self-recorded blood pressure readings.

Knowledge Resources

These are classes of information related to tacit and explicit knowledge supporting health care delivery, health system management, health self-management, collaboration, knowledge management and eLearning. Knowledge resources are primarily consumed by users of ehealth portals to support communications, collaboration and knowledge work, and generally do not contain personally identifiable health information.

Some examples include:

- Forms: electronic forms (including computerized versions of paper forms) for a variety of health care delivery and administration activities
- Policies such as health care policies
- Reference libraries: health and health care-related reference material (e.g. Compendium of Pharmaceuticals, drug interactions, medical dictionaries) and best practices or protocols for treating certain conditions
- Approved standards and other interoperability specifications: information relating to all ehealth-related standards (pan-Canadian, international etc.)
- Education: training on various ehealth-related topics, using elearning or other media
Health System Analytics

The electronic collection and sharing of health care data will yield a wealth of information for health system managers and planners – those responsible for planning and managing health care in Ontario. The electronic data captured, once anonymized to remove personal identification information, can support the following:

- Population demographics: studying the population of Ontario and health care client cohorts of interest, to support system planners, service integrators and program managers
- Population health data: studying the health status of population groups/cohorts
- Service utilization data: analyzing the type and number of health services consumed by Ontarians across the health care sector
- Health human resources data: analyzing the number, types and location of health human resources (e.g. doctors, nurses) available and working in the health system
- Financial data: analyzing the financial expenditures associated with the delivery of health services
- Performance data: analyzing performance indicators for tracking the performance of the health system and for supporting reporting requirements

The analytics can provide a wealth of information for those who:

- Analyze population health trends (e.g. public health)
- Budget and plan health care resources
- Identify catchment areas with specific needs
- Monitor services and data requirements
- Monitor systems for performance
- Conduct research into ways to improve health care
- Define health care policy in Ontario
Core Infrastructure Services

Other core technologies are required to interconnect stakeholders, services, and resources for the EHR:

- **Portal**: based on a common platform (hardware, software and basic configuration), portal infrastructure provides a point of aggregation for EHR stakeholders to access reference materials, access and share PHI, and collaborate.

- **Secure messaging**: technology and infrastructure supporting the secure and private exchange of information among EHR stakeholders and components (e.g. HL7 segments, repositories, registries, point of service systems).

- **Directory services**: repositories of people, organizations and places with standards-based interfaces for access (e.g. Lightweight Directory Access Protocol (LDAP), Active Directory).

- **Hosting**: secure facilities and services required to physically house information and information technology assets for the EHR.

- **Network**: as a result of increased reliability and bandwidth, as well as application security, the internet is suitable for the secure sharing of PHI, providing health care clients with more choice and cost savings. eHealth Ontario manages a secure private network for service classes or network requirements that the internet cannot address, or for health care applications that cannot be securely accessed via the internet.

- **Security services**: technologies and facilities providing information and technology safeguards for the EHR, including authentication and authorization, Public Key Infrastructure (PKI), immutable logging, network and security (firewalls, intrusion detection), and malware detection (virus scanning).

- **Support**: provincial and integrated EHR solutions must be properly managed, operated, maintained, and supported. Effective end user support infrastructure must be in place.

- **Operations**: ongoing services to operate the application or system following the design and build of a solution.

- **Enterprise availability services (EAS)**: as more EHR services are deployed, service delivery becomes more critical and the right technology, operations and people must be in place to sustain it. EAS will enable the delivery of health care services with an availability level to meet current and future service levels. This may include the use of continuous operations, high-availability techniques, and continuous availability services, as well as disaster recovery and business continuity capabilities.

  » Continuous availability is an approach to system and application design that protects users against downtime, whatever the cause, and ensures that users remain connected to their applications.

  » Systems with high availability are designed and operated so that systems and components remain available for a defined period of time, avoiding unplanned outages. Planned outages may occur. High availability involves sufficient redundant components so that a failure of one (or more) does not prevent the system from continuing to provide services.

  » Systems running continuous operation are designed to avoid planned outages (unplanned outages may still occur). By having multiple systems capable of performing each service, they can be maintained and upgraded while still providing services.

  » Disaster recovery is the ability to resume operations after a disaster and consequential loss of service to end users. It uses IT-focused plans to restore applications, systems or data centres during or after a disruption. Once a disaster is declared, a business continuity process is invoked, providing alternate ways for business services to function. Manual methods may be employed to facilitate business functions until services resume. During recovery, the reintegration of any manually processed transactions may be required.
Core Infrastructure Standards

The core infrastructure services include hardware and software based on standards, including standards for computing platforms (hardware architecture, software and applications).

Platforms generally include a computer architecture, operating system, programming languages and related user interface (run-time system libraries or graphical user interface). Hardware standards may include:

- Server performance standards (minimum response time, number of concurrent users, maximum load)
- Storage standards (minimum read/write speeds, file formats, size, cache, data storage schemes such as redundant array of independent disks (RAID))
- Software standards including operating systems (e.g. Linux, Windows), programming and scripting languages (e.g. Java, C#), and databases (e.g. Oracle, MySQL)
EHR Deployment

The province is divided geographically and jurisdictionally into three regions, along Local Health Integration Network (LHIN) boundaries. These are ConnectingGTA (cGTA – six LHINs encompassing the Greater Toronto Area and North Simcoe Muskoka), ConnectingSouthWestOntario (cSWO – four south west LHINs) and ConnectingNorthernandEasternOntario (cNEO – four northern and eastern LHINs).

Regional integration involves leveraging local, regional and provincial assets and connecting existing information technologies in ways that improve health care client care and clinical efficiencies for a region. The initiative revolves around developing the three eHealth regions to implement regional integration hubs, which will enable effective delivery of regional and provincial eHealth solutions.

Ultimately the goal is to connect these regions so that users in any region will be able to access a health care client’s EHR information across Ontario, no matter where the care was provided. Use of a regional approach also incorporates local and regional sources of information, allowing for regional flavour and innovation.

eHealth Ontario expects that many of its partners will deliver access to health care information through internet technologies. The delivery approach that the agency has adopted, using portals and web applications, supports broad deployment. In this way, the web is not a single channel, but rather a technology that supports many different access points. Some providers use web technology for remote access to their EMR, and all major HIS vendors already provide web viewers for their solutions – which can be leveraged regionally. Hospitals have deployed web infrastructure to help their staff in their day-to-day work and to help health care clients understand their own health care. eHealth Ontario supports these efforts with standards-based portlets that can be deployed in partner portals to quickly deliver comprehensive EHR capabilities.

The basic strategy is to build a central point of integration for (and within) each region. This is called a regional hub, defined as a set of integrated EHR services and infrastructure for a defined region of Ontario, which includes a HIAL, a provider portal, clinical repositories, and applications for that region. Furthermore, the three regional HIALs, along with a provincial HIAL owned by eHealth Ontario, will be interconnected to form a federated Ontario HIAL solution, for data exchange.

This section describes key solution components, how they will be deployed and how users will access and store information in the EHR.
Deployment Principles

- **HIAL-to-HIAL patterns and service consumption paths:** while traversing the HIAL, EHR services should be consumed via the most direct path possible.

- **Regional HIAL segments should not provide simple pass-through proxy services for provincial services:** regional integration services provide material support to regional point of service applications that are not capable of consuming provincial services directly. Conversely, point of service applications that are able to consume provincial services directly should do so without going through the local regional HIAL segment.

- **Business context propagation:** components may need to know about the original business context of a call to apply fine-grained authorization and consent policies.

- **Data messaging interactions authenticated and authorized:** this guarantees that only valid, recognized, and authorized users access EHR data messaging services, and enables the traceability and auditing capabilities required to support the protection of PHI.

The Ontario HIAL Solution

The Ontario HIAL solution is comprised of a number of distinct instances of the HIAL concept — HIAL segments — which are similar in purpose and function. Each of the three regions will implement an integration hub, including a regional HIAL segment, a regional provider portal, and local repositories of clinical data (belonging to and pertaining to that region alone).

A fourth HIAL segment, owned by eHealth Ontario, will serve as the integration point for access to provincially owned assets (provincial registries, clinical repositories, applications, knowledge resources). All HIAL segments will work together in a secure, well-governed, service-oriented manner to provide the foundation for the provincial EHR.

**eHealth Ontario HIAL Segment**

The eHealth Ontario HIAL segment will integrate all shared EHR resources and present their services to service consumers. The shared EHR resources (registries, repositories, applications) are provincial in scale, containing information for the entire provincial population of health care clients, and accessible by all health care providers in Ontario in accordance with provincial regulations related to the disclosure of PI and PHI.

**Regional HIAL Segments**

While all HIAL segments are similar in purpose and function, regional segments are focused on integration of more local/regional assets into the common province-wide HIAL resources and services infrastructure. The Regional HIAL segments will be used in a number of key ways:

- They will expose regional ehealth services (belonging to, and pertaining to, a region). HIAL communication and common service capabilities will be used in each regional HIAL segment to integrate health information within the region.

- They will expose regional variations of provincial ehealth services via a connection to the eHealth Ontario HIAL segment. The regional HIAL segment will use its integration capabilities to expose regional versions of eHealth Ontario services. For example, it could process (e.g. transform or translate) a request before relaying it (this is referred to as ‘last mile integration’). This facilitates the adoption of provincial ehealth services by allowing regional legacy, non-standard systems to indirectly consume standards-based ehealth services.

- Some regionally-supplied ehealth services may be of interest to other regions. One
way to provide access to these services could be to have an associated central service (hosted by the eHealth Ontario HIAL segment). The following diagram shows the regional and eHealth Ontario HIAL segments and how service consumers connect and get access to information about a health care client. Note that while service consumers can connect directly to the segment that presents a region’s ehealth services, eHealth Ontario services may also be consumed via another HIAL segment. This will be transparent to the point of service application.

- In cases where no last mile integration is required, a regional service consumer may connect directly to the eHealth Ontario HIAL segment to access shared EHR resources, without going through the corresponding regional HIAL segment. The path taken depends on the service consumer and the service requested. Service consumers do not need to know which path (provincial or regional) to use. They simply request a service from the service catalogue which defines the location and routing for service fulfilment.
A federated approach enables the regions and eHealth Ontario to work seamlessly and collaboratively, so that health care applications and data can be accessed across the province by authorized users. This approach leverages regional assets, systems, and referral patterns already in place or planned, and fosters local innovation.

The federated HIAL approach incorporates:

- Standards to govern technical interoperability between HIAL segments
- Common characteristics, features, and specifications for HIAL segments
- Agreements governing security and privacy (e.g. sharing of data among HIAL segments)
- Mechanisms to recognize and trust user identities and service requests from other HIAL segments
- A shared governance structure, including a common framework for governing the service oriented architecture to ensure a consistent approach to designing and managing provincial EHR services
- A common service registry that defines each EHR service and where it is accessed

Federating the HIAL segments facilitates the extension of eHealth technologies across the province. Each HIAL segment brokers requests and responses between point of service applications and EHR services. Common services (e.g. privacy, security) are provided to ensure consistent processing and to remove the need for line of business applications to build and support these functions.

Regional point of service systems can access provincial services in two ways:

- Directly through the eHealth Ontario HIAL segment
- Through the eHealth Ontario HIAL segment via their regional HIAL segment if ‘last mile integration’ is required

The HIAL will use web services based on the simple object access protocol (SOAP) and the WS* suite of supporting protocols to address security, policy, federation and other higher level functionality. Many EHR web services will contain HL7 message payloads based on the appropriate pan-Canadian standard for the EHR component they address. In alignment with WS-I, interfaces offered by eHealth Ontario on the HIAL will have established web services definition language.

All transactions that use the HIAL must provide strong credentials to prove their authenticity. The eHealth Ontario HIAL segment will rely on mutually authenticated SSL connections to establish entitlement to communicate with the EHR infrastructure, based on certificates from a trusted PKI Certificate Authority.
EHR Integration

The cornerstone of clinical integration is the ability to consume ehealth services from the HIAL. The HIAL supports complex integration requirements and a variety of EHR-enabling technologies with differing application interfaces, while the regional HIAL segment components must support integration with, for example, hospital information systems (HIS) that are typically not designed out of the box to integrate with an EHR.

Connecting systems must be able to communicate using SOAP-based web services secured with Secure Sockets Layer (SSL) and HL7 or the appropriate standard. They must also comply with terminology standards adopted by Ontario (such as LOINC or SNOMED CT). Security and privacy are handled differently in different organizations, and these must be considered when connecting to the EHR. The goal of the HIAL is to provide flexible integration capabilities to support current and future EHR systems.

Regional implementations of the HIAL have a higher dependency on flexibility in their services layer. Very few clinical systems are designed to integrate into an HL7 v3/SOAP-based EHR. Some services may not be applicable to the entire province, and these will also need to be integrated into the regional services model.

Integration Principles

- EHR services provide different types of service modes: these support external/public services including synchronous transactional data messaging services, asynchronous transactional data messaging services, synchronous business function services, portlet services, and batch services.

- EHR services have contracts based on web services and are discoverable: service contracts shall be stored in a single, well-known, accessible location, including contextual information (the service catalogue). Their names will describe their business functions and they will clearly define the expectations of service providers while providing service consumers a service infrastructure that is predictable, reliable, and managed.

- EHR services are based on established standards and interoperability specifications: standardization (e.g. messaging, data types, terminology, communication) is associated with increased interoperability, reduced complexity and reduced operational and support costs, and so should be strongly encouraged. Messages are encapsulated into industry standard web services, and web services level features are used to control communication, reliable messaging and security.

- EHR Services use a consistent set of interfaces and behaviours: the collection of external/public EHR services is offered as a consistent set of interfaces and behaviours, providing data and business services to organizations and application systems that consume its portlets and services.

- Services to eHealth Ontario’s internal systems are abstracted from external service consumers: through this abstraction, the provincial EHR hides the complexity and heterogeneity of all its components (e.g. shared EHR resources). Consequently, these components can be upgraded, modified, or replaced with minimal or no impact to the applications that rely on them.

- External/public services are secured: any service exposed to external access is vulnerable to attacks/penetration by unauthorized users, and must be protected through a series of security measures to identify and prevent malicious use.
Transaction Patterns

Transaction patterns establish a common set of interoperability processes and behaviours that can be applied to line of business applications invoked within the EHR. This creates predictable system behaviours by relying on a limited number of ways to connect to and use EHR services. Patterns also inform the interoperability requirements for point of service applications and EHR components, defining the responsibilities of the sending and receiving components, and how they should interact.

The patterns are founded on three common types of interactions between point of service applications and the Ontario HIAL Solution (and the services offered through it), including data, portlet, and publish-and-subscribe interactions.

- Data interactions: the exchange of EHR data between point of service applications and the Ontario HIAL Solution through exposed data services
- Portlet interactions: build on the data interactions with the use of portals at the point of service by exchanging EHR data through portlet services
- Publish and Subscribe interactions: a pattern in which a person or application publishes information, triggering an event notification (with or without payload) to all authorized subscribers. An example would be where a line of business application uses this pattern to publish data to other line of business or point of service applications.

These common patterns are divided into processing phases, including the external and internal (regional and provincial) activities to satisfy external requests:

- Point of service patterns: the sequence of activities that point of service applications perform to interact with and consume EHR services
- EHR services patterns: the flow of activities to fulfill service requests invoked by point of service applications or other internal components
- Federated Health Information Access Layer patterns: build on EHR services patterns by defining processing behaviours for the provincial and regional HIAL segments

Integration Service Modes

The Ontario HIAL Solution has established the service modes that it will support. This is crucial to the standardization of external/public services for the EHR. External service consumers select the category types they need to support their business requirements.

EHR services support the following integration service modes:

- Synchronous transactional data messaging services: for example, an EMR requests a lab test result for a health care client from OLIS, and waits for acknowledgement
- Asynchronous transactional data messaging services: for example, a laboratory information system submits a lab test result to the HIAL to be posted to OLIS at the end of the day. In the meantime, the laboratory information system can continue with its own processing.
- Synchronous business function services: for example, a drug utilization review, which provides decision support to health care professionals (such as pharmacists or physicians) by identifying drug contraindications
- Portlet services: for example, a nurse practitioner views a health care client’s lab results via a portlet that may be distributed on a number of portals across the province
- Batch services: for example, regulatory colleges send batch files of provider license numbers to the provider registry
Information/Data Standards

Information/data standards are an essential part of achieving interoperability, allowing point of service applications and all EHR services to exchange information seamlessly and reliably.

An EHR standard is an agreed-upon rule, format or process that is applied to support the definition, exchange, and use of EHR data and services.

For the EHR to work, everyone must agree on and use common processes, technology, data definitions, semantics, and formats for data exchange. Information/data standards are an essential part of interoperability, and are therefore critical to the design, support, and operation of the EHR.

These standards must be selected carefully for applicability, durability, consistency and sustainability, allowing for the effective build and design of EHR components and avoiding unpredictable changes resulting in rework. The use of standards minimizes the cost of new implementations, and allows new solutions and systems to participate in the EHR more easily.

The selection of standards is critical to the communication of business functionality. The standards selected by eHealth Ontario to support the EHR have clearly articulated business models to enable providers to understand how the standards support clinical activities. This is particularly important during early design stages, to ensure that functional and non-functional requirements are complete.

For more information on standards, refer to eHealth Ontario’s web site, or the website for a particular standard.

There are several types of standards required for the EHR:

Message and Document Standards

When systems need to communicate with the EHR, they will usually use an integration pattern called messaging, transferring information frequently and immediately. The term message refers to a unit of information that has to be moved between systems. Messaging standards define the format and construction of the message that will be used to convey the information.

Messaging and document standards include:

**HL7 v2 Messaging**

The HL7 version 2 messaging standard, perhaps the most widely implemented standard for health care in the world, allows for the simple exchange of clinical data between systems. It defines both the transport and messaging standards to convey information.

Support for terminology standards also exists but is not rigorously defined. Although not as complex or complete in functionality as other standards used in healthcare, legacy systems using this very common standard will be around for a while.

**HL7 v3 Messaging**

In response to difficulties with lack of clarity in the HL7 v2 standard, HL7 created a new standard based on a strict modeling methodology and XML encoding, with robust built-in support for terminology. HL7 v3 uses a single information model – the Reference Information Model (RIM) – providing a consistency lacking in HL7 v2. Unlike HL7 v2, it is less a framework for negotiation, and more of a solid specification, reducing the amount of custom work needed to connect two systems.
HL7 v3 Clinical Document Architecture (CDA)
A clinical document can be described as anything found in a health care client’s medical record that describes something about their health or their care. They are used extensively throughout health care to provide two main functions – to communicate information between clinicians about the health of the client, and to maintain a permanent record of their care to support compliance with local regulations and laws. The clinical document architecture is a framework based on the HL7 version 3 RIM, vocabularies and data types that allow one to express clinical documents in a human-readable and machine-readable form.

Digital Imaging and Communication in Medicine (DICOM)
Medical imaging generates vast amounts of data, using a very large array of imaging technologies. DICOM is the standard to create, store and transmit medical images and associated information between systems. The DICOM standard is comprehensive and defines all standards necessary to exchange images, including hardware specification, transport protocols, messages, content and document standards, and vocabulary and terminology sets.

Web Services Standards
Web Services are a standardized way of integrating applications over the internet. The two most common standards for web services are Simple Object Access Protocol (SOAP) and Representational State Transfer (REST).

Simple Object Access Protocol (SOAP)
The SOAP web services standard permits arbitrary complex business operations to be accessed over the internet. It is more complicated to implement than REST, but it can handle more difficult operations and is useful if more flexibility is required.

Representational State Transfer (REST)
REST is used to send and retrieve individual units of data, or objects, over the internet. It doesn’t handle complex operations, but it is lightweight and fast – useful in cases where bandwidth or processing power is limited. Most mobile applications, such as iPad apps, use REST.

Terminology Standards
Other types of standards address terminology and other vocabularies used in various clinical contexts, allowing physicians and other health care providers to communicate with each other in predictable ways and to provide consistent results across record sets and jurisdictions. Examples include Logical Observation Identifiers Names and Codes (LOINC) and Systematized Nomenclature of Medicine Clinical Terms (SNOMED-CT). HL7 uses external terminology standards like LOINC and SNOMED CT, as well as its own terminology for HL7 v2 and v3.

For example, if a type of lab test is given a different name by other labs in Ontario, errors in searching for and interpreting a health care client’s lab tests can result. It is necessary to determine what the standard set of terminology should be and secure agreement on how to adopt it, while making the required changes in local systems or mapping to the terminology in the EHR.

Standards bodies work with subject matter experts on all aspects of the EHR to assure stakeholders that their needs will be met by the technologies being procured and implemented. This provides a strong channel of planning and communication between system developers and system consumers. The following terminology standards provide some examples.

Logical Observation Identifiers Names and Codes (LOINC)
LOINC is a terminology standard that provides standardized means of identifying medical observations. It has two main parts: laboratory and clinical LOINC. LOINC is often used to provide standardized names for lab tests, which is essential for clinicians and labs to exchange requests for tests and results electronically. Clinical LOINC contains a subdomain of document ontology which captures types of clinical reports and documents. Clinical LOINC codes are sometimes used in Clinical Document Architecture (CDA) implementations to represent the types of sections of a document. Canada Health Infoway maintains a Canadian extension to LOINC called the Pan-Canadian LOINC Observation Code Database (pCLOCD), which OLIS is adopting.
Systematized Nomenclature of Medicine Clinical Terms (SNOMED CT)

SNOMED CT is a reference terminology standard that provides standard codes, descriptions and synonyms for over 311,000 clinical concepts. A clinical concept is a representation of clinical idea, which can range from body parts and drugs to services such as medical procedures and assessments. The clinical concepts are organized into groups called hierarchies. Medical procedures, clinical findings, body structure, and pharmaceutical products are examples of SNOMED CT hierarchies. Each concept is given a unique code to support functions such as algorithms for clinical decision support, alerts and reminders. Each concept has a description (a human-readable explanation) and a precise name (a fully specified name), as well as synonyms which can be other commonly used names. The use of fully specified names and synonyms helps with situations where a user wants to see a particular name in their application that is different from its fully specified name.

Transport Standards

Standards are also required to describe the transport of information and protocols to convey EHR data. A set of standards that enables network, communication and transport protocol interoperability is sometimes referred to as Transport Level Interoperability (TLI). These standards describe the network and transport protocols, as well as communication and interaction models (e.g. synchronous/asynchronous). Some messaging standards are restricted to using a particular type of transport standard (for example, REST can only be used with HTTP, and HL7 v2 can only be used over TCP/IP), but many can be transmitted over different channels (for example, SOAP can be transmitted over HTTP, but also can use the Java messaging service, or Simple Mail Transfer Protocol (SMTP)).

Example Relationships between Types of Standards

All of the types of standards listed above work together, and all are required in order for information to flow through the EHR. Document or content standards need messaging standards to describe how they will be transported between systems as well as terminology standards to accurately convey the information they contain in a way that can be interpreted and used by the other system. Messaging standards need transport standards to describe how they will be moved over the network. And all need privacy and security standards to ensure that information only goes to the places it's meant to go, and is accurate and complete when it gets there.

For example, Integrating the Healthcare Enterprise (IHE) is an international initiative by health care professionals and industry to improve the way computer systems in health care share information. IHE does not create standards. Instead, it produces implementation guidance in the form of Integration Profiles, which describe a clinical information need or workflow scenario and document how to use established standards (e.g. HL7, DICOM, LOINC etc.) to accomplish integration of systems.
This section provides high-level examples of the functions and supporting standards for a few of the EHR registries and repositories.

### Registries

<table>
<thead>
<tr>
<th>Name</th>
<th>Example Standards</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client</td>
<td>HL7 v2 and v3 messages and terminology to support management and query/results for client identifiers and demographic data (e.g. adding a client, revising client demographic data, querying for a client record)</td>
</tr>
<tr>
<td>Provider</td>
<td>HL7 v3 messages and terminology to support query/results for provider identifiers, profession, specialties, and demographic data (e.g. querying for a provider’s identifiers or specialization)</td>
</tr>
<tr>
<td>Consent</td>
<td>HL7 v3 messages and terminology to support management of consent directives</td>
</tr>
<tr>
<td>Audit</td>
<td>IHE ATNA based messages and terminology to support the automated collection of transaction logs associated with the collection, use and disclosure of PHI within eHealth Ontario systems</td>
</tr>
</tbody>
</table>

### Repositories

<table>
<thead>
<tr>
<th>Name</th>
<th>Example Standards</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clinical Documents</td>
<td>HL7 v2, v3 messages and CDA, and terminology to support the management and query/response for many different types of clinical documents and reports (e.g. discharge summaries, assessments, consults)</td>
</tr>
<tr>
<td>Drug</td>
<td>HL7 v3 messages and terminology to support prescribing, dispensing and management of medication information</td>
</tr>
<tr>
<td>Lab</td>
<td>HL7 v2 messages and terminology to support the ordering of lab tests, provision of lab test results, and management of lab orders and results. LOINC is used to represent lab test result names.</td>
</tr>
</tbody>
</table>
**Relationships between Standards Development and Management Organizations**

Many of the organizations responsible for standards development and management are collaborating to align their standards and/or make it easier to adopt them as well as maintain them. For example, the World Health Organization and the International Health Terminology Standard Development Organization (IHTSDO) have developed maps between ICD-10 and SNOMED CT. HL7 is working closely with IHTSDO to provide guidance on the use of SNOMED CT in HL7 v3 and to coordinate HL7 vocabulary submissions to IHTSDO.

**Vendor and Clinician Support**

A strong commitment to standards and careful standards selection are important for vendor and clinician support of the provincial strategy. If vendors understand that their development costs in the long run will be low, they will be more inclined to invest in standards, which will help ensure a richer, more competitive procurement environment which benefits implementers as well as users. Similarly, clinicians and other stakeholders need to be engaged in the standards selection and implementation to ensure their needs are met, which will contribute to their willingness to use and contribute EHR data.

**Canada Health Infoway (CHI) and the Standards Collaborative**

eHealth Ontario has a strong commitment to working on a national level with Canada Health Infoway, the federal not-for-profit corporation working as a strategic investor to transform health care through health information technology across all provinces and territories in Canada.

Launched in 2006 by Canada Health Infoway and the Canadian Institute for Health Information, the Standards Collaborative’s objective is to integrate the Canadian health information standards community into a single, cohesive, coordinated forum, and provide a single point of contact for health information standards in Canada.
Integrating with the EHR

Two main approaches allow information to be exchanged between point of service applications and the EHR:

- System-to-system communication through the HIAL using web services – the information flow is in both directions (e.g. service requests and responses, inbound storing of data, and outbound notification to a provider of a new report)
- Through a portlet in a portal – portlets also access web services, but provide a user-friendly, task-oriented interface which lends itself to use in combination with other portlets inside a portal, using a web browser

Both methods must be based on industry standards. Portlets rely on standards such as Web Services for Remote Portlets (WSRP), while web services are based on industry-recognized standards and may use data messaging standards such as HL7 and DICOM. Portlets are generally more easily integrated with point of service applications because they do not require the same direct system-to-system connectivity. However, they can only present data in a prescribed manner, which means that accessing data via a portlet gives less flexibility. Accessing a web service gives users raw data so they can display it as desired.

The health care industry has established business activities and workflows as well as guidelines and standards of practice. eHealth Ontario has no requirement or intent to alter the normal flow of business in the health care setting. The goal of the EHR is to enhance the quality and quantity of information available to users, while minimizing the impact and disruption to critical systems. With this in mind, eHealth Ontario provides no direct instruction on where and how to use the EHR, but makes information available and provides integration patterns and data delivery channels, with the expectation that the community will best understand how to use the information in their daily tasks. eHealth Ontario also works with the provider community and their authoritative bodies to enable transformative technology.

Hospital Information Systems (HIS)

Hospital information systems refer to application suites deployed institutionally. These suites are functionally rich and provide internal consistency, and the hospitals that run them are technically mature. They do not generally comply with all Ontario and pan-Canadian standards required to consume EHR services directly.

eHealth Ontario’s integration strategy for hospitals centres around identity federation and integration with the HIAL. The federated approach relies on trusting assertions from hospitals about the identities of their users of EHR services. Essentially, a hospital is entitled to request information from the EHR under its own recognizance as a health information custodian (HIC, as defined under PHIPA), but it must assert the identity and strength of authentication of the user requesting the information, for further authorization, audit and consent purposes. Hospitals sign agreements with eHealth Ontario referencing its policy and standards and establishing their responsibilities. Once this is done, eHealth Ontario will ensure that its policies and standards are followed.
Hospital systems have user management mechanisms which are often based on older, proprietary or internal naming standards and other integration mechanisms which may not meet the EHR’s user identity management requirements. These solutions may integrate using HL7v2 over MLLP or other standards. It is expected that a local interface engine or a regional HIAL segment will provide any necessary ‘last mile’ integration services before sending the systems request to the eHealth Ontario HIAL segment. For example, issuing required Security Assertion Markup Language (SAML) assertions, mapping local users to provincial identities for proper authentication and authorization, or transforming/translating messages to and from provincial standards.

In practice many hospitals may choose to use a hybrid solution, incorporating both the HIS and a hospital portal, with the HIS acting as a data source and potentially feeding information to the EHR. Users can be presented with a composite view of information (from the HIS, other local solutions, and the EHR) via context-sensitive portlets on the portal. Users can access their portals through their HIS with single sign-on enabled, or through a separate browser session using suitable context management mechanisms.

Other hospital systems supporting core functionality in the EHR such as lab or radiology information systems are expected to follow either the general HIS integration pattern or the patterns specific to the solution space in which they act.

**Electronic Medical Record (EMR) Systems**

EMR solutions are used in many health care settings. When used in a hospital ambulatory care setting, an EMR may be integrated with the broader hospital information environment, which provides common provisioning, identity, security and other services. These EMR systems may connect directly with the EHR components at eHealth Ontario via the eHealth Ontario HIAL segment, or through a regional HIAL segment; they will likely also integrate with local systems at the
hospital. EMR systems in community care settings are typically used by primary care physicians and specialists in the community.

eHealth Ontario, with OntarioMD, publishes specifications for EMR systems to work with EHR components. Users who purchase EMR systems that comply with these specifications qualify for funding from us. Clinical EMR systems at hospitals may or may not necessarily be specification-compliant. Those that are not compliant will need to rely on a local integration facility or the regional HIAL segment to leverage EHR services. Those that are compliant will have more flexibility and ease in using this integration pattern.

There are two models for the provincially funded EMRs:

- A local model – deployed, managed and operated at the clinic
- An application service provider (ASP) model – deployed in a central location; services are accessed by providers in remote locations

The major distinction between these two models, from an integration perspective, is the scale of operations. The following diagram depicts the two models.

Figure 17: EMR Integration Pattern
Since the local EMR pattern is able to continue providing many services with the network down, it is often deployed to small practices or those without adequately reliable network availability. However, this pattern requires local technical skills and resources (for maintenance, operation, upgrades, patches, support, disaster recovery, backup, etc.).

The application service provider (ASP) pattern provides a centrally managed and highly-available service for providers. It has a light local footprint and can be rapidly deployed to new environments. It is highly dependent on high-quality network services being available to the provider, and therefore network instability is a critical operational issue. Local EMRs will connect directly to a HIAL segment, while shared EMRs in an ASP model will have the ASP’s system connect to the HIAL segment.

**Radiology Systems**

The integration pattern for diagnostic imaging has some unique characteristics:

- There are different kinds of data of interest – actual images (e.g. x-rays) and documents – specifically, reports and manifests (documents that indicate the images that are part of a study and their location). Images are far bigger in terms of file size than documents.

- Currently there are four diagnostic imaging repositories (DI-Rs) in place across the province, each of which stores images, reports, and manifests for a different part of the province. These repositories are built with different technologies which support interoperability between systems within their respective regions. Users are currently limited to accessing diagnostic imaging data from within their regional diagnostic imaging repository. With the proper credentials a user in one repository could access data in another via a supported access channel. However, to provide consolidated view of data across all four repositories, a common service approach is required (see below).

- Data comes into these repositories from radiology systems (picture archiving and communication systems (PACS), or radiology information systems), but needs to be accessible not only by radiologists but also by other types of providers who do not use these systems.

- The vision for diagnostic imaging integration is to provide diagnostic imaging common services (DI-CS), through the eHealth Ontario HIAL segment, to allow for searching and retrieval of diagnostic imaging data for a health care client across the province at once. Reports and images will be accessible via various channels.

The following diagram shows the anticipated integration pattern to put images and documents into the EHR.

---

**Figure 18: Diagnostic Imaging PUT Integration Pattern**
There will be multiple ways to retrieve DI data. The ‘Other’ category may include, for example, EMRs, and PAC systems.

Laboratory Information Systems

Currently, hospitals, community labs, and public health labs are populating OLIS with lab orders and reports. They are doing so using the OLIS interface specification; OLIS SOAP messages carry a HL7 V2 compliant payload, travel over an SSL mutually authenticated channel, and are digitally signed. At present, most OLIS clients (users or systems) connect directly to OLIS. When the eHealth Ontario HIAL segment is ready, OLIS services will be accessed through it and the integration pattern will be similar to that used for integration of other point of service systems.

Systems in Community Care Settings

Entitled community health care providers with a clinical system can access the EHR through one of following three paths:

- Connecting through local integration tools provided by the regional HIAL segment or an interface engine
- Connecting to a segment of the Ontario HIAL Solution directly using web services
- Connecting to a portal service provider and consuming EHR services through another affiliated organization
- The integration pattern is similar to the ones described in this section for direct connections via web services or as described in the section below describing integration using portals.

Systems in Home Care

Home care can involve a chain of providers that deliver a wide array of services. These can extend from in-home visits by nurse practitioners through to meal delivery. The individuals that deliver these services may need access to the EHR depending on their profession and their relationship with the client. The patterns associated with this model are particularly applicable to work done by the Community Care Access Centres (CCACs), as well as Public Health.

eHealth Ontario supports community organizations that have case management solutions and field workers that provide health care visitation. For example, the CCACs are significant regional coordinators of home health care services. They have developed a case management system, the Client Health and Related Information System (CHRIS), and they use an assessment system called an Integrated Assessment Record (IAR). In addition, they are foundational users of resource matching and referral systems for acute-to-community care referral patterns. In this model, case workers help health care clients identify resources available to them and then coordinate the delivery of the applicable services. This structure is particularly
helpful in health care client transition from acute care environments to the home.

The health care client and the case management team arrive at a care plan that is appropriate for the client’s condition. This may be done via computer-based communications or by telephone. The health care client may or may not be using an online service containing personal health records. The visiting provider, for example a nurse practitioner, receives information from the case worker and the case management system but may augment this information by communicating with the EHR either through a portal or through a mobile interface to an EMR (or other EHR-connected system).

Other Systems Connecting to the EHR
There are a number of other non-clinical systems that can benefit from connectivity with the EHR. These include systems belonging to the Ministry of Health and Long Term Care, the Ministry of Community and Social Services, the Agency for Health Protection and Promotion, and health research groups. These participants do not have direct access to the personal health records of health care clients but they typically get de-identified or summary data for system management purposes.

Integrating Web Applications and Portals
Web applications and portals play a significant role in the dissemination of functionality and information associated with the EHR, as well as providing an important channel for rapid deployment and early adoption.

In settings such as hospitals, with multiple hard-to-integrate legacy systems, local portals play a critical role in presenting EHR functionality to providers.

Web delivery channels will play a key role in disseminating information to health care clients and their supporters. Web access is the most common way for individuals to get information from the institutions that they deal with, and will become a standard tool for individuals involved in their own care or the care of others.

Three EHR integration models for portlets in remote partner portals are supported. In two cases the partner portal owner is responsible for deploying the eHealth Ontario portlets, and in the third the portal owner is responsible for designing all aspects of the EHR integration.

Remote Portlet Model
Remote portlets (specifically WSRP v2.0) will be leveraged to deploy provincial content in a consistent manner across multiple portals (e.g. provincial, regional, and institutional portals). This approach enables the central management of versioning and implementation, while supporting distributed deployment of functionality through the reuse of provincial portlets. Refer to the figure below.

Figure 20: Remote Portlet Model
In this scenario, a partner portal is managed and maintained locally. User accounts, security, audit logs and other administrative details are the responsibility of the portal owner. Using OLIS as an example, the portal is configured to display content from eHealth Ontario using WSRP to access the eHealth Ontario OLIS portlet. This portlet is responsible for ensuring that laboratory reports are displayed in alignment with appropriate standards and best practices. It ensures that all aspects of the lab report are displayed in the correct order on the screen, with the right details as well as correct links to other documents. The portal owner does not need to understand the lab line of business or its display requirements to use this portlet; they only need to allocate a portion of the portal screen to display the pre-formatted HTML from the eHealth Ontario portlet producer server.

When a user connects to the portal and is authenticated, a secure connection is made (using SSL), via the eHealth Ontario HIAL segment, to the portlet producer, which manages and maintains all of the logic for the OLIS portlet component. The portlet producer then sends back the appropriate markup for the portal to show the user an interface that can display OLIS lab results. At this point, no query to OLIS has been performed, and the portlet does not display any PHI.

Should the user choose to search, he/she fills out the appropriate input fields in the portlet and submits a request containing the form data, which is then sent via the HIAL to the portlet producer. The portlet producer then connects to the OLIS web services interface (again via the HIAL) and makes a properly formatted OLIS request on behalf of the user. It receives and formats the OLIS response appropriately, including both HTML display information and the data returned by OLIS, and sends it back to the portal. The portal displays this content to the user as part of the aggregated portal page.

At no point does the portal designer need to understand the details of the OLIS transaction; that information is within the OLIS portlet. All that is needed is an understanding of how to configure the portal to use the OLIS portlet.

**Local Portlet Model**

The second scenario is very similar to the first, except that all of the business logic built into the portlet runs locally in the portal. This could be local code, or code provided by eHealth Ontario; in either case, for this scenario, there is no need to access the portlet producer every time. The application then consumes eHealth Ontario web services via the HIAL, using the appropriate protocol (e.g. CeRx) and security. Refer to the figure below.

---

**Figure 21: Local Portlet Model**

1. **Portal owner** is responsible for all user interface operations including security, portal layout and user identification. The portal runs a portlet designed by eHealth Ontario or another organization and is responsible for displaying content in a manner consistent with policies of each of the content types (correct formatting for labs, drugs, etc.).

2. **Services layer** is responsible for responding to web services requests containing appropriate HL7 (or another protocol) requests.

3. **EHR “Lines of Business”** have policy control over how the portlet producer formats content for portlets funded by them.
Continuing with the OLIS example, in this case, the user connects to a local portal, which runs the portlet code to display content. The user then fills out the appropriate fields in the portlet and submits the request. The portlet code connects to eHealth Ontario via the eHealth Ontario HIAL segment, and submits a properly formatted OLIS request containing the details provided by the user. OLIS returns the information to the portlet which formats the data for presentation to the user.

As in the remote services example, the portal owner does not need to understand the workings of OLIS in order to use the portlet, only how to deploy and configure it.

Local Implementation Model

In the last scenario, all of the development and design work is done by the portal owner. This is the most technically challenging and complex scenario. The portal developer simply consumes the underlying EHR web services directly.

This approach requires the portal developer to properly understand the business details of the EHR and the application (in this example, OLIS). It requires the developer to understand what should be displayed, where it should be displayed and how it should be displayed. This is a matter of medical functionality that requires specialized knowledge. It also means that ongoing maintenance of the functionality and presentation is the responsibility of the portal owner.

Figure 22: Local Implementation Model
Privacy and Security

Privacy refers to an individual’s right to control the collection, use, and disclosure of his/her personal health information (PHI) and/or personal information (PI) in a manner that allows health care providers to do their work. Security is about ensuring the information gets to the right person in a secure manner.

The privacy and security of information is a stringent requirement for the EHR, and eHealth Ontario is committed to delivering EHR services with privacy and security as foundational design principles. The PHI in the EHR is intended as a clinical tool, but its misuse or inappropriate disclosure could lead to issues ranging from public embarrassment to loss of employment, and threats to personal safety could arise from tampering with information or service outages.

The PHI Protection Act, 2004 (PHIPA), governs the collection, use and disclosure of PHI in Ontario. eHealth Ontario is creating an Information Security Management System based on ISO 27001:2005 and ISO 27799:2008 standards to ensure that PHI is properly protected.

The EHR Landscape from a Privacy and Security Perspective

PHI exists in doctors’ offices, pharmacies, hospitals, labs and other locations throughout Ontario. The data custodians of these locations (and their agents and security providers) must ensure that the information is properly protected as required by PHIPA. Providers are responsible for the privacy and security of the records stored on their premises or elsewhere on their behalf.

With paper-based records, a security or privacy breach could jeopardize only those records held by a single health care provider. In a small clinic with several providers, the number of jeopardized records would be somewhat larger. In a hospital the impact would be larger still. With the introduction of the EHR, the potential impact of a breach is increased, both in terms of the breadth of distribution and the amount of sensitive information available.

This places greater emphasis on the need for strong security and privacy controls and applicable standards. The EHR will provide the architecture for the widespread sharing of clinical data, coupled with strong controls for registration, identification, authentication, authorization, and auditing. Consent-based privacy mechanisms will allow health care clients to block access to any or all of their PHI.

In the context of information security, data ‘integrity’ means assurance that the information is accurate and complete. Accuracy is critical to the effective delivery of health care, as diagnoses, prescriptions, treatment plans and other clinical activity depend on the correctness of the information with which health care providers work. The accuracy of EHR data is critically dependent on the quality of identification, which is itself dependent on the identification of sources and users of data. This puts particular onus on the creation and maintenance of accurate provider and health care client identity, from record creation through storage and retrieval.

This requirement for accuracy has implications for the technologies used to analyze, store and report on information in the EHR. It underpins the need for effective testing, including data quality, change management and audit strategies, and puts emphasis on the quality of procurement and operations activities in support of the EHR. It should also be noted that, while EHR solutions can employ controls to help ensure accuracy, health care providers are ultimately responsible for ensuring that the data is correctly input.

The EHR must be reliable and highly available in order to be successful and widely adopted. Health care providers must be able to access information when and where they need it, which has a huge impact on the design and deployment of EHR services, driving the need for stable, high-availability infrastructure and applications.

EHR solutions also must be protected from malicious attacks from both outside and within the health community. The EHR infrastructure (hardware, software, networks, data centres) will have appropriate security controls.
Privacy

Privacy Principles

The Canadian Standards Association’s Model Code (CSA Model Code) is a national standard for privacy protection and is widely used across Canada as the basis for health information privacy legislation, including Ontario’s PHI Protection Act, 2004 (PHIPA). Detailed information is available at www.ehealthontario.on.ca in the Privacy section.

eHealth Ontario adheres to the CSA Model Code’s privacy principles in the implementation of the EHR as follows:

- **Accountability**: an organization is responsible for PHI under its control and has designated an individual or individuals who are accountable for the organization’s compliance with privacy principles.

  eHealth Ontario’s Board of Directors is accountable for the protection of privacy at the agency. It delegates this authority to the Chief Executive Officer who designates and appoints a Chief Privacy Officer to act on his or her behalf in this capacity.

- **Identifying purpose**: the purposes for which PHI is collected shall be identified by the organization at or before the time the information is collected.

  eHealth Ontario does not collect PHI directly from health care clients, but is permitted under PHIPA to use PHI received from Health Information Custodians (HICs – e.g., hospitals, labs, pharmacies) to create and maintain the electronic health record. Information about the purpose of the eHealth Ontario-managed data repositories can be found on eHealth Ontario’s website under Privacy. HICs, as the collectors of the PHI, are responsible for identifying the purpose for the collection of PHI at or before the time it is collected.

- **Knowledge and consent**: the knowledge and consent of the individual are required for the collection, use or disclosure of PI, except where inappropriate.

  When health care clients receive health care services from HICs, their express consent to share information between HICs who are involved is not required. According to PHIPA, HICs may rely on the implied consent of the health care client to collect, use, disclose and retain PHI in the EHR, for the purpose of providing or assisting in the provision of healthcare services, unless the health care client has expressly withheld or withdrawn consent. Consent should be meaningful and health care clients should be able to understand how their PHI will be used and disclosed in the EHR, as well as the fact that they are entitled to withdraw consent at any time.

  eHealth Ontario’s role is to implement a consent management system for provincially managed assets. Health care client consent directives regarding how their PHI can be shared through the EHR are processed to respect and protect the health care client’s privacy. If a consent directive has been overridden by a HIC, a notification in writing shall be sent to the health care client, unless otherwise directed by the health care client.

- **Limiting collection**: the collection of PHI shall be limited to that which is necessary for the purposes identified by the organization. PHI shall be collected by fair and lawful means.

  When eHealth Ontario is creating or maintaining EHRs, it is not collecting PHI as defined by PHIPA. eHealth Ontario is permitted to receive the PHI collected by HICs for the purpose of creating or maintaining EHRs. When acting as an agent for a HIC, eHealth Ontario collects PHI only as directed by the HIC and only on behalf of the HIC.

- **Limiting use, disclosure and retention**: PHI 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.

  eHealth Ontario does not use or disclose PHI, as those terms are defined in PHIPA, for its own purposes. PHI is only used, disclosed and retained as directed by the HICs to which it is providing services when acting as an agent under PHIPA, or in accordance with the legislation to provide and assist in the provision of healthcare services, and for no other purpose unless permitted by the legislation and approved by the Commissioner. According to PHIPA and its regulations, when PHI is provided to eHealth Ontario by a HIC for the purposes of creating and maintaining one or more EHRs, the HIC is not considered to be disclosing the PHI to eHealth Ontario as the term is defined in PHIPA. eHealth Ontario does not disclose PHI to HICs when it is creating or maintaining one or
more EHRs; it receives PHI from and sends PHI to authorized HICs for the purpose of providing or assisting in the provision of healthcare services.

PHI is retained within eHealth Ontario's data centre(s) and systems only as long as necessary for the fulfillment of those purposes, to the extent that is reasonable and practical.

To prevent misuse and lack of consistency of the privacy protocol among HICs and eHealth Ontario, there are agreements stipulating the permitted disclosure and uses of PHI.

Where a HIC provides PHI for the creation and maintenance of the EHR, and such PHI is stolen, lost or accessed by an unauthorized person, eHealth Ontario notifies the HIC at the earliest opportunity.

- **Accuracy:** PHI shall be as accurate, complete and up to date as is necessary for the purposes for which it is to be used.

The HICs who collect the PHI are responsible to ensure the accuracy of the source PHI. Corrections or changes to PHI must be completed by the HIC who has custody and/or control of the PHI. eHealth Ontario, where possible, provides mechanisms to HICs to support the accurate entry of PHI into the EHR (such as input validation controls). eHealth Ontario implements the security controls (e.g., encryption and digital signatures) to make sure the information sent to eHealth Ontario by HICs has not been intentionally modified or accidentally corrupted, and that it can be relied upon.

- **Safeguards:** PHI shall be protected by security safeguards appropriate to the sensitivity of the information.

eHealth Ontario consistently identifies and classifies its information assets and implements the commensurate security safeguards to protect the information and systems from the perspectives of confidentiality, integrity and availability (refer to the Security section below). Specifically, eHealth Ontario implements administrative, technical and physical safeguards, including but not limited to: encryption of PHI in transit or mandatory required on mobile devices; threat and risk assessments; privacy monitoring, immutable logging, auditing and reporting; access control; and privacy and security training.

In addition, for every eHealth Ontario service that involves PHI, a privacy assessment must be conducted, and identified risks and issues must be addressed prior to go-live.

- **Openness:** an organization shall make readily available to individuals specific information about its policies and practices relating to the management of PHI.

eHealth Ontario maintains a high degree of transparency with respect to its policies and practices relating to the management of PHI in the EHR. eHealth Ontario publishes this information to the public at www.ehealthontario.on.ca/en/privacy

- **Individual access and correction:** upon request, an individual shall be informed of the existence, use and disclosure of their PHI and shall be given access to that information. An individual must be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

eHealth Ontario is not a HIC and does not directly deal with a health care client's request to access or correct PHI. If eHealth Ontario receives an access or correction request, it will direct the individual to the appropriate HIC(s) to respond to the request.

- **Compliance challenge:** an individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

eHealth Ontario has a well-established process that allows individuals to contact its Chief Privacy Officer for compliance concerns. For more information, refer to the eHealth Ontario Privacy Data Protection Policy, PHI Privacy Policy, and Personal Information Privacy Policy at www.ehealthontario.on.ca/en/privacy

**Privacy by Design**

The approach taken to protect privacy is to build the capability to make PHI widely available, but to tightly manage the access to it. The approach needs to be dynamic to ensure clients can access health care anywhere in Ontario and providers will be able to access their health care information. The key is to ensure that access to PHI is only granted to those who are authorized, and that the health care client's consent directives are applied.
To ensure that the privacy of Ontarians is respected at all times when data is being accessed, collected, used or disclosed through the EHR, the principles of Privacy by Design (a concept developed by the Information and Privacy Commissioner of Ontario) have been embedded into the EHR blueprint (see www.privacybydesign.ca/index.php/about-pbd/7-foundational-principles).

Privacy by Design consists of seven principles which, when operationalized, will permeate all aspects of the creation and management of EHRs. It advances the view that the future of privacy cannot be assured solely by compliance with regulatory frameworks, but that privacy assurance must become an organization’s default mode of operation (Information and Privacy Commissioner, Ontario, Canada, 2011). Privacy by Design seeks to embed privacy and accountability into every aspect of the EHR’s business practices, information technologies and physical infrastructure.

An example of how privacy has been built into all aspects of the EHR by default, specifically business processes supporting the use of PHI, is Privacy Common Understandings (PCU). These establish a shared approach to privacy practices between eHealth Ontario and the regional hubs, and ensure compliance with PHIPA by identifying specific roles and responsibilities for privacy across users of the EHR.

Privacy controls built into the EHR include:

- Privacy training for users of the EHR
- Use of anonymized data for testing purposes
- Logging and monitoring of access
- Maintenance of audit logs
- Encryption of all data in transit
- Specific purposes for the access, collection, use or disclosure of PHI in the EHR
- Segregation of repositories of data for specific identified purposes
- Access controls for users of the EHR
- Consent rules applied by default to all transactions crossing the eHealth Ontario HIAL segment that require access to PHI
- Agreements outlining the roles and responsibilities for protection of PHI
- Transparent privacy practices

**Privacy Governance in the EHR**

The common privacy policies and procedures developed and approved by the ConnectingPrivacy Committee (CPC), a provincial forum of representatives from Ontario’s three regional healthcare hubs (cGTA, cSWO, cNEO), eHealth Ontario, the Ministry of Health and Long-Term Care, the Office of the Information and Privacy Commissioner of Ontario, Canada Health Infoway and other stakeholders from across the province, allows for a consistent approach to privacy provincially. Adoption of harmonized policies by Ontario’s regional healthcare hubs ensures a consistent privacy experience for providers who use ehealth systems and individuals whose information is stored in those systems, and it enables a common privacy governance framework throughout organizations participating in the EHR.

**Privacy Standards**

Privacy standards tend to describe sequences of activities and the roles, rights, responsibilities, benefits and risks associated with the collection, use, and disclosure of information. Legislation, policies, best practices, guidelines, and process/management standards produced by standards development organizations (SDOs) that focus on the privacy of information – in electronic and paper formats – may fall under this general category. From a privacy perspective the EHR must comply with the following key legislative and policy drivers:

- PHI Protection Act, 2004 (PHIPA)
- Freedom of Information and Protection of Privacy Act (FIPPA)
- eHealth Ontario Privacy and Data Protection Policy
- eHealth Ontario PHI Privacy Policy
- eHealth Ontario Personal Information Privacy Policy
- Other relevant eHealth Ontario internal policies
Consent and Privacy Audit

Consent Directives

A consent directive is defined as express instruction(s) from a health care client (or someone authorized to act on the client’s behalf) to his/her HIC, regarding the collection, use, or disclosure of the client’s PHI.

When a request for PHI disclosure comes through eHealth Ontario’s HIAL segment, a check is made for consent directives against release of the data. The degree of control available to individuals is determined by provincial policy.

The components of the consent management solution are shown in figure 23.

Consent Management components are:

- **External inputs:** include legislation, regulation, and policy direction from MOHLTC and eHealth Ontario, and consent requests from health care clients
- **Consent system administration:** an administrative application restricted to a small group of authorized users for reporting and configuration purposes
- **Point of service (POS) applications:** clinical systems requiring interaction with the consent management solution
- **Portals:** websites providing a single point of access to online services for a target group of users, aggregating information from multiple sources and presenting it as a unified whole
- **eHealth Ontario HIAL segment:** the key interface point for all access to PHI in eHealth Ontario’s clinical repositories. Service orchestration through this segment requires that consent management is invoked for any request for PHI access.
- **Audit log:** provides PHI auditing services and generates notifications to privacy officers in eHealth Ontario when specific transactions occur (e.g. consent override)
- **Registries:** used in the application and evaluation of consent directives – for example to normalize client identifiers from POS applications to the corresponding provincial identifiers
- **Domain repositories:** the provincial stores of clinical data that contain PHI for a domain

- **Consent management registry and services:** the core of the consent management solution. Services include:
  - **Consent management directory:** stores health care client consent directives, as well as legislation-based rules and policy-based rules that control consent directive processing
  - **Transaction processing:** the main processing engine invoked by the consent interface to apply consent, allowing or blocking a transaction or masking its content
  - **Reporting:** reports on the management of consent directives, which can include information on the directives in force for a health care client at a point in time
  - **Publish/subscribe:** allows partner clinical systems to be notified of consent directives collected by eHealth Ontario

Planned features of the consent management solution include:

- Health care clients will be able to create, modify, and revoke consent directives, withdrawing or withholding consent for the use or disclosure of their PHI via the EHR, as directed by policy and/or the law. They will also be able to reinstate this consent if required.
- The solution will have the flexibility to implement more finely detailed degrees of access control, as determined by the MOHLTC through regulation or provincial policy.
- Standards will be applied for both the types of consent directives that can be created, and the processes by which they are implemented and managed.
- Transactions relating to the implementation, viewing, modification, revocation, or overriding of consent directives will be logged.
Privacy Audit

PHI audit trails are an important part of the EHR privacy compliance and security implementation. All transactions relating to PHI that consume EHR-related services through the eHealth Ontario HIAL segment will be logged in a centralized audit repository for privacy purposes. This repository is maintained separately from the system and other logs managed by the other EHR components. The solution is based in part on requirements set out in PHIPA O. Reg. 329/04, requiring the ability to respond to requests for information on accessed PHI in eHealth Ontario’s systems and who has accessed the information.

The components of the privacy audit solution are shown in figure 24. Many of them are similar to those in the consent management solution (HIAL segment, registries, domain repositories).

Authorized users will access the solution through an interface for administration, management of business rules, and reporting. The core functionality of the solution will include:

- Logging of all PHI-related transactions, for privacy auditing purposes
- Reporting and analytics: tools to present information in standard format
- Monitoring and alerting: detection of inappropriate use based on configurable business rules and system configurations. Includes the ability to correlate audit events and the generation of intelligent, context-based alerts, for suspicious events or behaviour.
- Security mechanisms to prevent unauthorized access to, and unauthorized use of, audited information

Figure 23: Consent Management
Figure 24: Privacy Audit
Security

Security is about ensuring the confidentiality, integrity and availability of information and systems. It is achieved through a risk management process and assures the public that risks are adequately managed. Information security management is integrated into the blueprint and considered in every aspect of developing and operating EHR systems.

eHealth Ontario's information security management system will be based on ISO 27001:2013 and ISO 27002:2013 standards, industry best practices that will ensure the protection of EHR assets in eHealth Ontario. eHealth Ontario is committed to delivering EHR services with privacy and security as foundational design principles, which are embedded by default across the solutions that provide services.

Security Principles

eHealth Ontario uses the following principles to secure EHR assets:

- **Leadership:** Top management shall demonstrate leadership and commitment with respect to the information security management system by:
  - Ensuring the information security policy and the information security objectives are established and are compatible with the strategic direction of the organization
  - Ensuring the integration of the information security management system requirements into the organization's processes
  - Ensuring that the resources needed for the information security management system are available

- **Planning:** eHealth Ontario shall plan the information security management system by considering the issues and the requirements to determine the risks and opportunities that need to be addressed, by:
  - Defining and applying an information security risk assessment process
  - Establishing information security objectives at relevant functions and levels

- **Supporting:** eHealth Ontario shall determine and provide the resources needed for the establishment, implementation, maintenance and continual improvement of the information security management system by:
  - Maintaining a competent staff
  - Ensuring staff are aware of security policies and need to comply with them
  - Documenting information necessary for the functioning of the organisation

- **Operating:** eHealth Ontario shall plan, implement and control the processes needed to meet information security requirements by:
  - Performing information security risk assessments at planned intervals or when significant changes are proposed or occur
  - Implementing an information security risk treatment plan

- **Evaluating performance:** eHealth Ontario shall evaluate the information security performance and the effectiveness of the information security management system through:
  - Audits and compliance checks
  - Management review of the information security management system

- **Improving:** eHealth Ontario shall improve the implementation of the information security management system by:
  - Taking corrective action of non-conformities
  - Continually improving the suitability, adequacy and effectiveness of the information security management system

Information Security Standards

Information security standards describe sequences of activities and the roles, rights, responsibilities, benefits and risks associated with the security of information. Policies, best practices, guidelines, and process management standards produced by standards development organizations (SDOs) that focus on the security of information
– in electronic and paper formats – may fall under this category. From a security perspective, eHealth Ontario must comply with the following key policy drivers:

- eHealth Ontario internal policies
- eHealth Ontario information security policies
- ISO 27001 & 27002 standards adhered to by eHealth Ontario

### Security Control Objectives

Security controls are means of managing risk, including policies, procedures, guidelines, practices, or organizational structures, which can be administrative, technical, management, or legal in nature.

ISO#27002 is a widely recognised and accepted information security standard which defines the level of information security rigor appropriate for provincial scale assets. Its guidelines and principles should be followed by all systems that are part of the EHR structure in eHealth Ontario.

ISO#27002 covers the following topics:

- Information security policies
- Organization of information security
- Human resource security
- Asset management
- Access control
- Cryptography
- Physical and environmental security
- Operations security
- Communications security
- System acquisition, development and maintenance
- Supplier relationships
- Information security incident management
- Information security aspects of business continuity management
- Compliance

### Security Services

In the EHR, security is provided in the form of services. The following security services are described in the Canada Health Infoway (CHI) EHRS blueprint and the privacy and security architecture document:

- Identity protection services
- Digital signature services
- Encryption services
- General security services
- Identity management services
- Access control services
- Secure auditing services
- User authentication services

These services map to the privacy and security services described in the common services section of this document. eHealth Ontario’s privacy and security services map to those listed by Canada Health Infoway as follows:

- **Authorization**: maps to CHI’s Access Control
- **Authentication**: maps to CHI’s User Authentication Services
- **Access control**: maps to CHI’s Access Control
- **User registry**: maps to CHI’s Identity Management Services
- **Digital signatures**: maps to CHI’s Digital Signature Services
- **Public Key Infrastructure (PKI)**: maps to CHI’s Encryption and Digital Signature Services
- **Auditing**: maps to CHI’s Secure Auditing Services
**Identity and Secure Access**

Associating a user's real world identity with an electronic credential helps ensure that only authorized people can access PHI. The following key identifiers are used in the context of the EHR.

**Health Care Client Identity**

Current, accurate, and trustworthy health care client identity information is central to the integrity of the EHR. This identity is used to access all related records for a client, both current and historic, from any source. Incomplete or incorrect identity records could lead to inaccurate association of all data pertaining to a client. Identity management procedures will therefore be critical to quality of care in the EHR.

The goal is to create a complete identity record for all individuals receiving care in Ontario, including:

- People who have a health number but have not received care in Ontario
- Health care clients who are not from Ontario
- Ontarians who do not have health numbers
- Health care clients who do not have identification that can be electronically verified by providers

The client registry will work with these restrictions, as well as with medical record numbers (MRNs) and other health care system identifiers for a client. Enterprise Master Patient Index (EMPI) capabilities in the client registries, active integration with point of service systems such as admission/discharge/transfer (ADT) systems, and approaches such as the enterprise client ID (ECID), help manage these identifiers and the provision of a longitudinal electronic health record for the health care client, irrespective of the type and number of identifiers linked to his/her health information.

**Provider Identity**

eHealth Ontario’s provider registry is a sharable province-wide repository of providers to help manage access to health care applications. Some providers, such as physicians, nurse practitioners, and dieticians, are regulated by colleges or similar bodies. The provider registry will contain both regulated and unregulated providers.

Electronic credentials uniquely identify the provider who is accessing the health care application, and are used to ensure that the provider has authorized access. These credentials are stored as part of the EHR transaction logs, providing traceability throughout the EHR.

To ensure accountability, all EHR transactions must be traceable to a responsible individual. Due to the distributed nature of access to the EHR, this responsibility is shared by eHealth Ontario and its federation partners. Prior to disclosure of information from the EHR, the requesting care provider will always be strongly identified and authenticated. The strength of the identity process is taken into account during the entitlement evaluation. If the requested EHR or data domain service has a policy that requires users to have a particular strength of identity or authentication, then requests that do not meet these requirements will be rejected.

Two patterns are typical for disclosure of EHR data to a user. In the first a provider system presents a PKI certificate as part of an SSL mutually-authenticated session. The system owner will have proven their identity to the appropriate Certificate Authority (eHealth Ontario) to obtain the credential (PKI certificate) that enables them to submit a request to the EHR. Businesses seeking this type of access are bound contractually through agreements with eHealth Ontario, and must meet the requirements outlined in the appropriate policy.

The second disclosure pattern requires identification of the individual user. The level of assurance associated with user identification needs to be commensurate with the sensitivity of information being disclosed. Users can be identified through eHealth Ontario's ONE ID mechanism, or through other recognized and federated identity providers and federation partners.

**Identity Federation**

EHR transactions are traced to the individuals who performed them, and to the organization under whose authority they acted. Electronic credentials link users to their real world identity and to their regulatory college, if applicable. They also map to an organization that has authorized the user’s access to specific applications and health care client
records. By contrast, system-generated tokens describe the authority for an electronic transaction which can be associated with agreements between contributing parties.

As a consequence of the broad use and need for EHR functionality, eHealth Ontario must support the activities of hundreds of thousands of health care providers and millions of health care clients at thousands of locations throughout the province, while keeping information available, accurate and secure. Providers wanting to access the EHR need to be assigned digital identities – i.e. they need to be securely identified, so that they can be authenticated when they make service requests. They also need to be assigned access privileges so that their requests can be properly authorized. Accurate identification of the requesting provider is also critical to allow consent features to work effectively.

The identity federation concept takes advantage of the fact that many providers have already fulfilled similar requirements in the organization where they work. For example, clinicians in a hospital must satisfy internal criteria in order to access its systems. This provides an opportunity to partner with such organizations, by trusting and sharing their digital user identities. Organizations that are trusted in this way are ‘federated’ with respect to identity.

Federation partners sign agreements to follow relevant federation policies and standards. The agency will ensure that these policies and standards are followed.

Federation can be considered a network of organizations providing access to services based on user identity assertions made by trusted identity providers. For example a clinician’s hospital credentials, (asserted by an identity provider), are used to authenticate to provincial applications presented by eHealth Ontario.

Benefits of federation include:

- More effective use of provincial assets through consistency of business processes/operations, technical infrastructure and policies, standards, and agreements
- Increased efficiency by minimizing duplication of effort among federation members and reducing/offloading some administrative responsibilities to the federation operator (defined below). For example, gathering, validating and maintaining identity information locally, as providers have clear and established relationships with their organizations.
- Improved privacy and security by enforcing common policies, standards and agreements
- Applications (EHR components, hospital and LHIN-based solutions) developed by one organization are easier to adopt by other organizations, since they recognize each other’s credentials
- Users from a federated partner can use the same login credentials for both their local system and broader EHR services (this is called single sign-on). Credentials from federation members can be used to access provincial services, including eHealth Ontario assets like OLIS, which can rapidly increase the number of users with secure electronic access to clinical applications.

![Figure 25: Access through Identity Federation using Trust Relationships](image-url)
The eHealth Ontario federation model defines 4 roles for federation members. A federation member may play one or more of these roles:

- **Federation operator**: sets policies, standards and agreements; provides business processes and technical infrastructure to facilitate federation operations

- **Identity provider**: provides credentials to users based on real world identities; captures and passes verified data required for federation (e.g. professional designations), and authenticates users when requested by the federation operator

- **Delivery channel**: provides a conduit to an EHR service. A good example is a portal that deploys eHealth Ontario portlets.

- **Application provider**: provides services for consumption by federation members, and defines the rules by which users are entitled to access the services. Users with credentials from recognized identity providers can access services using a recognized delivery channel.

An organization wanting to be an identity provider, (i.e. issue health care providers with electronic credentials to access EHR applications), or a delivery channel, (i.e. provide an entry point such as a portal, for EHR applications), must sign an agreement with eHealth Ontario to abide by the policy and standards applicable to their role in the federation.

**ONE ID as an Identity Provider**

To support providers not affiliated with a hospital that can issue them a user ID and password, such as pharmacists, dentists, dieticians, midwives, occupational therapists, psychologists, administrative staff, and sole practitioners, eHealth Ontario’s ONE ID service acts as a province-wide identity provider, issuing electronic credentials for access to EHR applications. These applications may be hosted by eHealth Ontario or by other organizations. ONE ID is a member of the identity federation and also plays the federation operator role.

The service uses a network of Local Registration Authorities (LRAs) employed by their own organization and acting on behalf of eHealth Ontario to simplify the registration process.

A number of organizations also use ONE ID as their identity provider for access to their applications. Note that they may not necessarily consume any other eHealth Ontario services. By partnering with these organizations, the ONE ID service will reach a critical mass of users so that future applications or systems adopting ONE ID will be accessible to more users who are already registered.

**Secure Access to the EHR**

The elements of the EHR are stored with eHealth Ontario and its regional partners, some of which are large, well-established organizations with mature IT processes and security/privacy controls, while others are smaller and less mature. The EHR may be accessed through large systems, EMR systems or portal implementations. All of these accesses occur through a secure mechanism.
eHealth Ontario has adopted a layered approach to access control:

- The operators of health care provider systems restrict access to those with valid user identities and a specific need to access the data.
- Only systems with an eHealth Ontario PKI certificate issued through a ONE ID registration event can communicate directly with provincial EHR assets through the eHealth Ontario HIAL segment.
- ONE ID works with other EHR systems to evaluate service requests in the context of the requesting system, the identity of the requesting user, the user’s roles, and the service being requested.
- The solution implementing the business service (the application owner) applies fine-grained access control based on business rules and the transaction the end system is requesting.
- Applicable consent directives are applied against all transactions that require access to PHI.
- All accesses and transactions to PI/PHI through eHealth Ontario are logged for audit purposes.

**Accessing Diagnostic Imaging Repositories**

Diagnostic imaging information may not always be in a central repository, but in locations distributed around the province. These federated service providers will be supported by facilities developed by eHealth Ontario, e.g. if a certain type of diagnostic image or report is distributed across multiple regional repositories, eHealth Ontario can build common services to search across them all.

**Accessing through Portals**

Content from many sources, including the EHR, can be presented to users through a web/portal interface using portlets. Hospitals and other large provider organizations wanting to consume eHealth Ontario portlets in their portals can qualify to be trusted by eHealth Ontario to control access to and use of EHR components, based on existing security and privacy controls and their HIC status.

The identity provider is responsible for authenticating and authorizing the user, and for controlling access to the pages hosting the portlets. Audit records will be kept of all transactions, and integration with the eHealth Ontario audit service will ensure appropriate reporting.

All user interactions with portals use Transport Layer Security (TLS) between the browser and the portal at the strongest cipher level available from the browser, or in the worst case, in compliance with minimum requirements set by policy. Communications from the portal to the eHealth Ontario infrastructure also use TLS, but they are authenticated by both ends of the communication channel.

The following diagram shows the high level user and system actions performed by solution
components for the ‘remote portlet’ model. The user securely logs on to a partner portal which displays a page containing one or more portlets. The user interacts with the portlets which then communicate with one another in the browser via the eHealth Ontario shared context manager portlet. The context manager provides event management and also manages attributes that specify the current activity context, such as the health care client health number or other health information.

1. The partner portal provides the user web experience, as well as the attributes for user context for service authorization and entitlement. The users implicitly rely on the partner portal to address their privacy and security concerns. The partner portal also establishes the communication channel to the eHealth Ontario portlet producer.

2. HIAL portlet access processing validates the partner portal.

3. The eHealth Ontario portlet producer provides the portlets with a common set of interfaces (the WSRP interfaces). The portlets obtain the user and activity context from the WSRP messages sent from the partner portal. They convert the user context to SAML assertions that are inserted into the line of business services requests.

4. HIAL service access processing engages ONE ID to check the user’s entitlement, based on the SAML assertions.

5. Line of business services process information based on the service request.

The eHealth Ontario portal is complemented by regional portals providing similar services and using common technologies, components and standards. Regional portals have integrated security and a strong trust relationship with eHealth Ontario, allowing them to offer the same services as the eHealth Ontario portal. However, they have different governance structures and a mandate to expose additional content and services that only apply to their regional providers.

**Access to the Public**

For health care clients to have access to their own records, their identities must be managed and authenticated. Leveraging a model of federated identity and authentication similar to that for clinicians may be the best approach. Addressing the security and privacy of individuals under these circumstances requires considerable attention to identity, appropriateness, and audit verification. eHealth Ontario’s advanced registration authentication systems can be leveraged where needed to support stronger identification and authentication of users.

Giving the public access to their health information also provides strong security benefits. For example, providing users with a list of organizations that have accessed their records allows them to validate appropriate use and request investigations for perceived violations. Individuals will be able to provide and manage consent directives which guide the use and disclosure of their PHI.

**Access ‘Under the Authority Of’**

Any provider accessing the EHR is considered to be acting under the authority of a Health Information Custodian (HIC), as defined in legislation. The HIC could be a large organization (e.g. a hospital), or it could be a sole practitioner’s clinic. eHealth Ontario records the HIC associated with each transaction.

Some providers may work for more than one HIC. When interacting with the EHR, they must specify under which HIC’s authority they are acting.

---

**Figure 27: Action steps in the Remote Portlet Model**

- **LOB SERVICES**
  - Provides: Information based on service request

- **HIAL SERVICE ACCESS**
  - Checks: Entitlement

- **EHEALTH PORTLET PRODUCER**
  - Provides: Portlets

- **HIAL PORTLET ACCESS**
  - Validates: Partner Portal
  - Provides: Credentials
  - Context attributes
  - Web experience

- **PARTNER PORTAL(IES)**
  - Declares: Context

- **PORTAL USER**
  - Uses: Portal
Governance

The following diagram illustrates the EHR architecture and standards governance committee structure.

- The gating portfolio/project review committee and the business and architecture review committee focus on the governance of projects either executed within eHealth Ontario or funded by eHealth Ontario.

- The strategic committee and the business and technical committee focus on the governance of Ontario EHR architecture and standards.

**Business and Architecture Review Committee (BARC):** responsible for ensuring architectural compliance and quality assurance for the EHR Blueprint. Conducts in-depth reviews of project management, architecture, standards, security, privacy, quality assurance, and operations artifacts submitted as part of the gating and checkpointing processes. Provides all checkpointing approvals and gating endorsements to GP/PRC.

**Gating Portfolio/Project Review Committee (GP/PRC):** responsible for reviewing and approving project gates as outlined in the gateway policy and based on the business and architecture review committee’s endorsements. Is accountable for portfolio management of programs and projects.

**Ontario EHR Architecture and Standards Strategic Committee (SC):** consists of external stakeholders providing strategic decisions and direction on the development, maintenance, conformance and adoption of Ontario EHR architecture and standards. Approves Ontario EHR development, maintenance, conformance and adoption of Ontario EHR architecture and standards. Approves Ontario EHR architecture and standards for eHealth Ontario standards-based solutions and services based on the Business and Technical Committee’s recommendations.

**Ontario EHR Architecture and Standards Business and Technical Committee (BTC):** consists of external stakeholders that ensure that business and technical requirements for Ontario EHR architecture and standards are clearly and accurately scoped, documented and met. Recommends Ontario EHR architecture and standards for Strategic Committee (SC) approval.

Figure 28: EHR Governance Structure
### Appendix A: Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADT</td>
<td>Admission, Discharge, Transfer system</td>
</tr>
<tr>
<td>ASP</td>
<td>Application Service Provider</td>
</tr>
<tr>
<td>BARC</td>
<td>Business and Architecture Review Committee</td>
</tr>
<tr>
<td>BTC</td>
<td>Business and Technical Committee</td>
</tr>
<tr>
<td>CA</td>
<td>Certificate Authority</td>
</tr>
<tr>
<td>CCAC</td>
<td>Community Care Access Centre</td>
</tr>
<tr>
<td>CDA</td>
<td>Clinical Document Architecture</td>
</tr>
<tr>
<td>CDR</td>
<td>Clinical Data Repository</td>
</tr>
<tr>
<td>CDPS</td>
<td>Comprehensive Drug Profile System</td>
</tr>
<tr>
<td>cGTA</td>
<td>Connecting the Greater Toronto Area</td>
</tr>
<tr>
<td>CHI</td>
<td>Canada Health Infoway</td>
</tr>
<tr>
<td>CHRIS</td>
<td>Client Health and Related Information System</td>
</tr>
<tr>
<td>CIA</td>
<td>Conceptual Information Architecture</td>
</tr>
<tr>
<td>CIM</td>
<td>Conceptual Information Model</td>
</tr>
<tr>
<td>cNEO</td>
<td>Connecting Northern &amp; Eastern Ontario</td>
</tr>
<tr>
<td>CR</td>
<td>Client Registry</td>
</tr>
<tr>
<td>cSWO</td>
<td>Connecting South-West Ontario</td>
</tr>
<tr>
<td>DICS</td>
<td>Diagnostic Imaging Common Services</td>
</tr>
<tr>
<td>DICOM</td>
<td>Digital Imaging and Communications in Medicine</td>
</tr>
<tr>
<td>DUR</td>
<td>Drug Utilization Review</td>
</tr>
<tr>
<td>EAS</td>
<td>Enterprise Availability Services</td>
</tr>
<tr>
<td>EBCDIC</td>
<td>Extended Binary Coded Decimal Interchange Code</td>
</tr>
<tr>
<td>ECID</td>
<td>Enterprise Client ID</td>
</tr>
<tr>
<td>EHR</td>
<td>Electronic Health Record</td>
</tr>
<tr>
<td>EHRS</td>
<td>Electronic Health Record Solution</td>
</tr>
<tr>
<td>EMPI</td>
<td>Enterprise Master Patient Index</td>
</tr>
<tr>
<td>EMR</td>
<td>Electronic Medical Record system</td>
</tr>
<tr>
<td>FIPPA</td>
<td>Freedom of Information and Protection of Privacy Act</td>
</tr>
<tr>
<td>FTP</td>
<td>File Transfer Protocol</td>
</tr>
<tr>
<td>GP/PRC</td>
<td>Gating and Portfolio/Project Review Committee</td>
</tr>
<tr>
<td>HIAL</td>
<td>Health Information Access Layer</td>
</tr>
<tr>
<td>HIC</td>
<td>Health Information Custodian</td>
</tr>
<tr>
<td>HIS</td>
<td>Hospital Information System</td>
</tr>
<tr>
<td>HL7</td>
<td>Health Level Seven</td>
</tr>
<tr>
<td>IAR</td>
<td>Integrated Assessment Record</td>
</tr>
<tr>
<td>IHE</td>
<td>Integrating the Healthcare Enterprise</td>
</tr>
<tr>
<td>IHTSDO</td>
<td>International Health Terminology Standard Development Organization</td>
</tr>
<tr>
<td>IP/SEC</td>
<td>Internet Protocol Security</td>
</tr>
<tr>
<td>LDAP</td>
<td>Lightweight Directory Access Protocol</td>
</tr>
<tr>
<td>LHIN</td>
<td>Local Health Integration Network</td>
</tr>
<tr>
<td>LIS</td>
<td>Laboratory Information System</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Full Form</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------</td>
</tr>
<tr>
<td>LOINC</td>
<td>Logical Observation Identifiers Names and Codes</td>
</tr>
<tr>
<td>LRA</td>
<td>Local Registration Authority</td>
</tr>
<tr>
<td>MLLP</td>
<td>Minimal Lower Layer Protocol</td>
</tr>
<tr>
<td>MOHLTC</td>
<td>Ministry of Health and Long-Term Care</td>
</tr>
<tr>
<td>MRN</td>
<td>Medical Record Number</td>
</tr>
<tr>
<td>OGPMESS</td>
<td>Ontario Government Pharmaceutical and Medical Supply Service</td>
</tr>
<tr>
<td>OLIS</td>
<td>Ontario Laboratories Information System</td>
</tr>
<tr>
<td>PACS</td>
<td>Picture Archiving and Communication System</td>
</tr>
<tr>
<td>pCLOCD</td>
<td>Pan-Canadian LOINC Observation Code Database</td>
</tr>
<tr>
<td>PCU</td>
<td>Privacy Common Understanding</td>
</tr>
<tr>
<td>PDP</td>
<td>Policy Decision Point</td>
</tr>
<tr>
<td>PEP</td>
<td>Policy Enforcement Point</td>
</tr>
<tr>
<td>PHD</td>
<td>Public Health Division</td>
</tr>
<tr>
<td>PHI</td>
<td>Personal Health Information</td>
</tr>
<tr>
<td>PHIPA</td>
<td>PHI Protection Act</td>
</tr>
<tr>
<td>PI</td>
<td>Personal Information</td>
</tr>
<tr>
<td>PID</td>
<td>Patient Identifier Domain</td>
</tr>
<tr>
<td>PKI</td>
<td>Public Key Infrastructure</td>
</tr>
<tr>
<td>PR</td>
<td>Provider Registry</td>
</tr>
<tr>
<td>RAID</td>
<td>Redundant Array of Independent Disks</td>
</tr>
<tr>
<td>REST</td>
<td>Representational State Transfer</td>
</tr>
<tr>
<td>RIM</td>
<td>Reference Information Model (part of HL7 V3)</td>
</tr>
<tr>
<td>RM&amp;R</td>
<td>Resource Matching and Referral</td>
</tr>
<tr>
<td>RPDB</td>
<td>Registered Persons Database</td>
</tr>
<tr>
<td>SAML</td>
<td>Security Assertion Markup Language</td>
</tr>
<tr>
<td>SC</td>
<td>Steering Committee</td>
</tr>
<tr>
<td>SDO</td>
<td>Standards Development Organization</td>
</tr>
<tr>
<td>SMTP</td>
<td>Simple Mail Transfer Protocol</td>
</tr>
<tr>
<td>SNMP</td>
<td>Simple Network Management Protocol</td>
</tr>
<tr>
<td>SNOCTED - CT</td>
<td>Systematized Nomenclature of Medicine – Clinical Terms</td>
</tr>
<tr>
<td>SOA</td>
<td>Service-Oriented Architecture</td>
</tr>
<tr>
<td>SOAP</td>
<td>Simple Object Access Protocol</td>
</tr>
<tr>
<td>SR</td>
<td>Systems Registry</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Sockets Layer</td>
</tr>
<tr>
<td>TCP/IP</td>
<td>Transmission Control Protocol/Internet Protocol</td>
</tr>
<tr>
<td>TLI</td>
<td>Transport Level Interoperability</td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security</td>
</tr>
<tr>
<td>UTF</td>
<td>Unicode Transformation Format</td>
</tr>
<tr>
<td>UR</td>
<td>User Registry</td>
</tr>
<tr>
<td>WSDL</td>
<td>Web Services Description Language</td>
</tr>
<tr>
<td>WSRP</td>
<td>Web Services for Remote Portlets</td>
</tr>
<tr>
<td>XACML</td>
<td>eXtensible Access Control Markup Language</td>
</tr>
<tr>
<td>XDS</td>
<td>Cross-Enterprise Document Sharing</td>
</tr>
<tr>
<td>XML</td>
<td>eXtensible Markup Language</td>
</tr>
</tbody>
</table>
Appendix B: Terms & Concepts

The following key terms and concepts are used throughout this document:

**Certificate**: used for authentication, this is an electronic file in a format in accordance with ITU-T recommendation X.509, containing the public key of a registrant and related information, digitally signed with the private key of the Certificate Authority (CA) issuing it, and including the ID for the certificate policy. A certificate identifies its registrant, contains a public key corresponding to a private key under the control of the registrant, identifies its operational period, contains a certificate serial number, and is digitally signed by the Certificate Authority issuing it.

**Certification**:

**Certificate Authority (CA)**: a trusted entity responsible for verifying the identity of a certificate registrant and issuing certificates.

**Certificate Chain**: a sequence of certificates, each signed by the previous one, forming a chain that leads to a trusted root certificate.

**Certificate Policy**: a set of rules that defines when and how a certificate can be used.

**Certificate Signing Request (CSR)**: a request for a digital certificate sent to a Certificate Authority, containing information about the applicant and their public key.

**Certificate Revocation List (CRL)**: a list of certificates that have been revoked due to compromise or other reasons.

**Certificate Revocation List (CRL)**: a list of certificates that have been revoked due to compromise or other reasons.

**Conceptual information architecture (CIA)**: a complete high-level view of information constituting an individual's EHR in the Ontario health system, and an outline of its structure.

**Consent and consent directive**: consent is the explicit or implicit granting of access to specified information. A consent directive is defined as express instruction(s) from a health care client (or someone authorized to act on the client’s behalf) to his/her HIC, regarding the collection, use, or disclosure of the client’s PHI.

**Data exchange**: the process of taking data structured under a source schema or standard, and transforming it into a target schema or standard so that it is an accurate representation of the source data.

**Data standard**: a standard that enables functional interoperability by defining the required content and format in which particular types of data are to be exchanged.

**Domain repositories**: disciplines in the health sector are referred to as clinical domains. Domain repositories are applications that collect, store, and support the use of clinical data about health care clients for a domain, and also provide business services for accessing and managing data. Examples include lab, drugs, and diagnostic imaging domain repositories.

**Electronic medical record (EMR)**: a partial health record under the custodianship of a health care provider(s) holding a portion of the relevant health information about a person over their lifetime. This is often described as a provider-centric or health organization-centric health record of a person. The EMR represents a point of service application used by providers in their practice management and patient care, for storage, retrieval and manipulation of (for example) patient health records, clinical encounter notes, medications, orders, test results and a cumulative patient profile.

**Electronic health record (EHR)**: secure and private lifetime record of key health history and care within the Ontario health system. The record is available electronically to authorized health care providers and the individual anywhere, anytime in support of high quality care.

**Electronic health record (EHR) application**: a system that provides health care client data from multiple domain repositories and registries in the EHR for specialized use. EHR applications are more function-rich than the domain repositories. An example would be Public Health.

**Electronic health record solution (EHRS)**: Canada Health Infoway defines EHRS as “a combination of people, organizational entities, business processes, systems, technology and standards that interact and exchange clinical data to provide high quality and effective health care”.

**Federation**: an association whose trusted members have agreed to share information across organizational boundaries. Identity federation refers to an association whose trusted members have agreed to share user identity information.
Freedom of Information and Protection of Privacy Act (FIPPA): Ontario legislation that applies to information that institutions collect, the rights of access to that information by individuals, and the protection of privacy of individuals with respect to their personal information (PI). eHealth Ontario must adhere to all regulations addressed in FIPPA.

Governance: seeks to establish clear chains of responsibility to empower oversight bodies in their decision making, set in place measurements to gauge effectiveness, establish policies to guide the organization and stakeholder community to meet its goals, and allow control mechanisms to ensure compliance, and communication to keep all required parties informed.

Health care client: a person who is eligible to receive, has received, or is receiving health care services in Ontario

Health care provider: a person or organization providing health care or other health-related services or products

Health Information Access Layer (HIAL): a single logical interface for EHR interoperability, facilitating the exchange of information between point of service applications and shared information resources. The HIAL abstracts the interfaces, security mechanisms, internal technical specifics, and topology (locations and partitioning) of these systems, and provides common services.

HL7: Health Level Seven International, a not-for-profit, ANSI-accredited standards developing organization dedicated to providing a comprehensive framework and related standards for the exchange, integration, sharing, and retrieval of electronic health information that supports clinical practice and the management, delivery and evaluation of health services.

HL7 v2: an HL7 standard supporting hospital workflows. Originally created in 1987, it defines a series of electronic messages to support administrative, logistical, financial, and clinical processes.

HL7 v3: an HL7 standard supporting health care workflows. Development of version 3 started around 1995, resulting in an initial standard publication in 2005. The HL7 v3 standard, as opposed to HL7 version 2, is based on a formal methodology (the HDF – HL7 Development Framework) and object-oriented principles.

Integration: the process of linking computing systems and software applications physically or functionally, to work with each other.

Integrating the healthcare enterprise (IHE): an initiative by healthcare professionals and industry to improve the way computer systems in healthcare share information. IHE promotes the coordinated use of established standards such as DICOM and HL7 to address specific clinical needs in support of optimal patient care. Systems developed in accordance with IHE communicate with one another better, are easier to implement, and enable care providers to use information more effectively.

Interoperability: the ability of systems to connect to, accept services from, exchange data with, and process data from, other systems, and the extent to which information or instructions sent from one system can be understood by another.

Longitudinal health record: health care client-centric electronic health information, from the earliest event to the most recent client encounter.

Personal health information (PHI): information about an individual in oral or recorded form, if the information, (a) relates to the physical or mental health of the individual, including information that consists of the health history of the individual's family, (b) relates to the providing of health care to the individual, including the identification of a person as a provider of health care to the individual, (c) is a plan of service within the meaning of the Home Care and Community Services Act, 1994 for the individual, (d) relates to payments or eligibility for health care, or eligibility for coverage for health care, in respect of the individual, (e) relates to the donation by the individual 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, (f) is the individual's health number, or (g) identifies an individual's substitute decision-maker.
Personal information (PI): information about an identifiable individual

Personal Health Information Protection Act (PHIPA): an act to a) establish rules for the collection, use and disclosure of PHI about individuals that protect the confidentiality of that information and the privacy of individuals with respect to that information, while facilitating the effective provision of health care b) provide individuals with a right of access to PHI about themselves, subject to limited and specific exceptions set out in this act, c) provide individuals with a right to require the correction or amendment of PHI about themselves, subject to limited and specific exceptions set out in this act d) provide for independent review and resolution of complaints with respect to PHI e) provide effective remedies for contraventions of this act

Portal: a website providing a single point of access to online services for a target group of users, aggregating information from multiple sources and presenting it as a unified whole

Portlets: pluggable software components that can be configured and displayed in a portal (or multiple portals based on the same standard), to provide access to information sources or applications

Point of service (POS) application or system: a system employing EHRs in a clinical setting (e.g. an EMR system in a health care provider's office, a laboratory information system, or a hospital information system)

Privacy: an individual's right to control the collection, use, and disclosure of his/her PHI and/or PI

Regional Health Information Access Layer segment: one instance of the HIAL architectural concept, owned by one of ConnectingGTA (cGTA), ConnectingSouthWestOntario (cSWO), or ConnectingNorthernandEasternOntario (cNEO) and used as the access point to that region's EHR resources as well as provincially owned shared EHR resources

Regional hub: a set of integrated ehealth services and infrastructure for a defined region of Ontario, which includes a HIAL segment, a provider portal, clinical repositories, and applications for that region

Registry: the authoritative source of reference information for an ehealth entity (e.g. clients, providers, systems). It also provides services to allow authorized users to access applicable functionality (such as search, retrieve, add, update, and merge), while protecting the privacy of the entity. Registry information is often consolidated information from multiple authoritative sources.

Security: the protection of the confidentiality, integrity, and availability of information

Service-oriented architecture (SOA): a business-driven IT architectural approach that supports integrating the business as linked, repeatable business tasks, or services. At a technical level, it is a component model interrelating functional units of an application, called services, through well-defined interfaces. The interface is standards-based and independent of the hardware platform, the operating system, and the programming language implemented for the service.

Simple Object Access Protocol (SOAP): a protocol specification for exchanging structured information in the implementation of web services in computer networks. SOAP uses XML technologies to define an extensible messaging framework providing a message construct to be exchanged over a variety of underlying protocols. The framework has been designed to be independent of any particular programming model and other implementation-specific semantics, and is specified by the W3C recommendation.

Standard(s): accepted rule or format used to establish uniformity or consistency, including documented agreements containing specifications, or other precise criteria to be used consistently as rules, guidelines, or definitions

Terminology standard: a standard that enables semantic interoperability by defining comprehensive clinical language terms and their relationships to other terms that health care providers can use to observe diagnose and treat clients
# Appendix C: Scenarios

The scenarios below compare what currently happens when a health care client interacts with the health care system with what will happen when the EHR is implemented.

## Scenario #1 – Health Care Client Visits a Physician

A health care client’s care involves several providers, each using a different clinical system.

<table>
<thead>
<tr>
<th>Steps</th>
<th>Current Situation</th>
<th>With the EHR</th>
</tr>
</thead>
</table>
| **Health care client visits physician with a problem and requires a procedure or treatment** | • Support staff locates client’s paper chart  
• Physician reviews information received from procedures or treatments ordered (information from other providers may not be available). Client forgets to mention a relevant visit to another health care facility.  
• Physician documents visit in paper chart; information will be available for review in subsequent visits | • Physician reviews client’s clinical information in the EMR system. May also access client’s province-wide health information electronically (e.g. using a portal accessing data through a HIAL, or through an EMR connected to a HIAL).  
• Before accessing data created by other providers, physician’s identity and access rights are validated and health care client’s instructions regarding use of his/her health information are checked, to make sure he/she has not blocked access (performed through provincial registries, accessed via eHealth Ontario HIAL segment)  
• Physician reviews all client’s procedures and treatments, including information from all data sources and providers across the province  
• Physician documents visit in the EMR. This information will be available for review by all authorized providers across the province (for example, via a clinical document repository). |

**Possible outcomes:**

- Probability of errors in data due to manual data entry
- Probability of errors due to delayed or misplaced information in paper chart
- Health care client responsible for providing much of full clinical history
- Unnecessary or redundant procedures and consultations ordered
- Avoidable costs incurred

**Outcomes:**

- Procedures and consultations not repeated unless required
- Information available to authorized providers in real time, regardless of location
- Client does not need to remember full clinical history
<table>
<thead>
<tr>
<th>Steps</th>
<th>Current Situation</th>
<th>With the EHR</th>
</tr>
</thead>
</table>
| **Physician identifies need for an intervention / procedure** | • Physician generates paper requisitions for interventions/ procedures such as lab tests or diagnostic images. Physician may not be aware of previous interventions and procedures, since paper reports were either not forwarded or are delayed.  
  • Requisition taken by client or sent by fax for processing  
  • Copy of requisition added to client’s paper chart  
  **Possible outcomes:**  
  • Data errors with manual/paper-based processes | • Physician checks in the EHR for previous interventions and procedures  
  • Physician reviews results and orders new interventions/procedures electronically (using OLIS via eHealth Ontario HIAL segment)  
  • Physician orders additional interventions/procedures complementing previous orders  
  • Physician may access online references if additional information is required during treatment process (using integrated knowledge resources with information on best treatment practices and medical reference materials)  
  **Outcomes:**  
  • Results available online for authorized review in the EHR regardless of who ordered intervention/procedure and their location  
  • Interventions and procedures not duplicated  
  • More timely initiation of treatment |
| **Health care client presents for follow-up visit** | • Paper copies of interventions/procedures are sent to physician and added to paper chart  
  • Follow-up visit must account for delays in receiving information  
  • Physician reviews information and compares with other information in paper chart  
  **Possible outcomes:**  
  • Access to information is limited (local) and not available across continuum of care  
  • Delays in starting treatments | • Results of interventions and procedures available for review by physician shortly after being completed (using domain repositories, via eEHealth Ontario HIAL segment)  
  • Physician compares results against information collected from other providers  
  **Outcomes:**  
  • Comprehensive picture of client’s results  
  • Treatments can be started without delay |
<table>
<thead>
<tr>
<th>Steps</th>
<th>Current Situation</th>
<th>With the EHR</th>
</tr>
</thead>
</table>
| **Health care client referred to a specialist** | • Referral sent by fax or mail. Office staff or health care client schedules referral with specialist by telephone  
• Copy of information from paper chart sent by fax or mail (only tests and treatments physician is aware of)  
• Additional information sent with client to specialist  
• Fragmentation of information available for specialist to review  
• Available information includes data from local physician’s paper chart  
**Possible outcomes:**  
• Delays in service delivery  
• Duplication of interventions/procedures | • Physician office completes online referral (using EHR electronic referral application)  
• Possible dates made available electronically to physician’s staff  
• Specialist reviews information electronically from all sources (all data is integrated through a HIAL)  
• Specialist’s identity and access rights are validated, and client’s consent directives are checked (using provincial registries via eHealth Ontario HIAL segment)  
**Outcomes:**  
• Referral not delayed  
• Information available for specialist to review electronically in timely fashion (may include digital information)  
• Treatment initiated without delay |
| **Health care client treatment plan established and follow-up arranged** | • Treatment plan developed and documented in paper chart and forwarded to primary care physician  
• Client documents some of the treatment plan  
• Paper prescription written by specialist and handed to client  
**Possible outcomes:**  
• Potential adverse drug event if critical medication information from other health providers not available, or if client omits information on medication history  
• Consultation summary sent to primary care physician for client’s paper chart  
• When the pharmacist transcribes the paper prescription, possible error in drug dosage, or refill instructions, which may result in inappropriate dispense | • Treatment plan when entered is available to authorized providers  
• A copy of plan is printed for client  
• Electronic prescription is created and sent to the pharmacy (using the ePrescription service)  
• Pharmacist checks for potential drug interactions (using the Comprehensive Drug Profile System (CDPS), via the eHealth Ontario HIAL segment)  
**Outcomes:**  
• Easier for client to follow printed treatment plan and document personal activities  
• Information is available electronically in timely fashion to all providers subject to confirmation of identity, access rights, and consent directives  
• Treatment initiated without delay  
• Mitigated risk of prescribing inappropriate medications |
### Scenario #2 – Unknown Health Care Client goes to Emergency Department

<table>
<thead>
<tr>
<th>Steps</th>
<th>Current Situation</th>
<th>With the EHR</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Throughout the scenario</strong></td>
<td>• No record of who has accessed the Client’s PHI.</td>
<td>• All accesses to client’s PHI in the EHR are logged</td>
</tr>
<tr>
<td><strong>Health care client presents alone at emergency department requiring urgent acute medical care (client unknown to emergency department)</strong></td>
<td>• Assessment history obtained during interview with client. If client is incapacitated, critical information may not be available.</td>
<td>• Emergency department views client’s health information electronically (information sources are integrated through the EHR)</td>
</tr>
<tr>
<td></td>
<td>• Limited information about client available</td>
<td>• Previous information is available for comparison purposes</td>
</tr>
<tr>
<td></td>
<td>• Client may not have medications or list of medications</td>
<td>• All accesses to client’s PHI logged</td>
</tr>
<tr>
<td></td>
<td>• Other providers must be contacted to obtain health information</td>
<td>• Drug dispensing history from this encounter is available for any other providers who treat this client in future (using the CDPS, via the eHealth Ontario HIAL segment)</td>
</tr>
<tr>
<td><strong>Possible outcomes:</strong></td>
<td></td>
<td><strong>Outcomes:</strong></td>
</tr>
<tr>
<td></td>
<td>• Potential for adverse event due to incomplete information</td>
<td>• Interventions and procedures not duplicated</td>
</tr>
<tr>
<td></td>
<td>• Duplication of interventions/ procedures</td>
<td>• Treatments initiated in timely fashion</td>
</tr>
<tr>
<td></td>
<td>• Avoidable costs are incurred</td>
<td>• Mitigated risk of inappropriate treatment</td>
</tr>
</tbody>
</table>
Work with us

We all have a role to play in building Ontario’s EHR.

Only a collaborative effort will result in a scalable system that can securely share the right information, with the right people, at the right time to support the myriad decisions required to improve health care for Ontario’s 13 million citizens.

Our role is providing guidance to help you implement your ehealth solutions and / or integrate existing ones.

Using Ontario’s ehealth blueprint, we can all work towards a fully interoperable EHR – one that provides a lifetime record of an individual’s key health history and care.

Get us involved

From advisory consultations on blueprint alignment to standard selection and stakeholder engagement, we can help you align, adopt and implement the blueprint.

Book an appointment with us today and discover how we can help you develop your ehealth solutions.

Architecture, Standards and Planning
Tel: 416-591-8046
Email: architecture@ehealthontario.on.ca

www.ehealthblueprint.com