- Jurisdiction provides EHR for all patients
  ~ 16 million people
  ~ 300,000 healthcare professionals
- Annual budget ~ $400 million
- 2 Tier 4 data centers

Computable Privacy Use Case: Large Jurisdiction

Situation

eHealth Ontario is an agency of the Ontario government under the governance of the Ministry of Health and Long-Term Care. The agency is playing a lead role in harnessing information technology and innovation to improve the delivery of care, safety and access in support of the Ontario government's health strategy.

The Identity, Access and Privacy (IAP) Program, part of eHealth Ontario's Cornerstone Information Systems, enables interaction with all of the people and businesses that are participants in the Ontario health system. The IAP Program is responsible for development and deployment of key eHealth Ontario infrastructure components, including enabling the delivery of the following: User Registry, Client Registry, Provider Registry, Data Acquisition and Management, and Monitoring and Control Technology and Consent Management. Specifically, it supports the identification of clients and providers, controls access to information and manages the consent directives of citizens.

The consent management program team is responsible for establishing the strategy, technology, business process and guidelines for use of the core technology assets required to manage consent directives (CDs). The provincial government develops the required consent policies. eHealth Ontario provides the technical components, referred to as consent management technology assets (CMTA), to enable the consent management program.

Challenge

To implement an electronic consent solution that would provide the flexibility to ensure that the implementation would:

- Conform to the Opt-out with Exceptions* consent model
- Support the integration of granular consent
- Enable rules management and validation
- Facilitate consent storage in a single repository
- Alert users when they are about to create consent directives that conflict with existing ones
- Support user access control

** "Implied consent" per Ontario's Personal Health Information Protection Act (PHIPA)*

Software Integrated

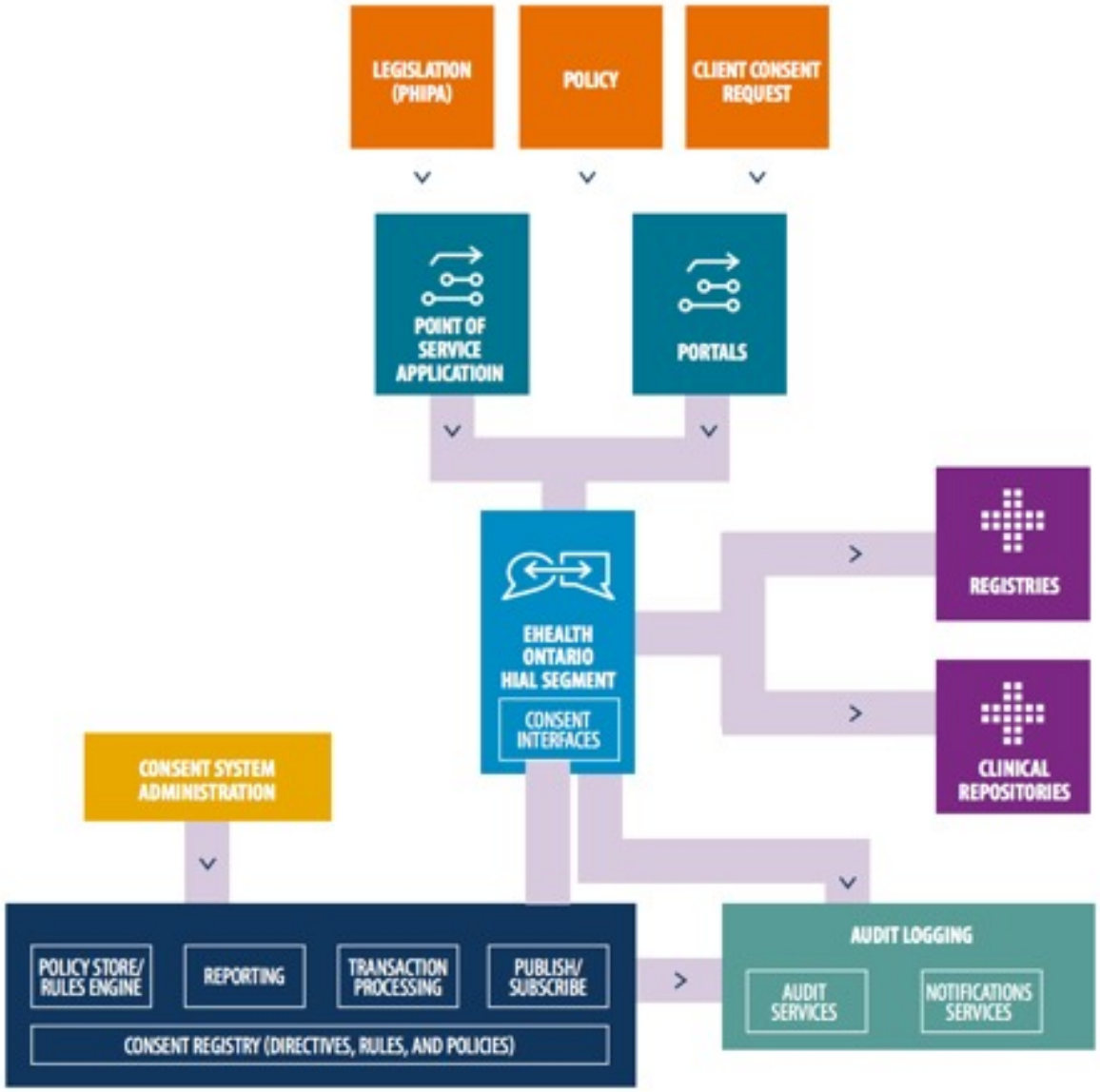
Privacy eSuite (PeS)
A web services-based consent engine developed to enable organizations, HIEs and jurisdictions to electronically manage, enforce and audit complex health information privacy policies in a diverse digital health ecosystem.

Embedded in Privacy eSuite is the **Universal Audit Repository (UAR),** a Java-based, IHE-ATNA compliant audit repository that tracks audit events related to updates, queries and retrievals. The UAR provides the capability for privacy and security reporting for all updates and access to PHI and pushes IHE-ATNA messages to the provincial audit repository.

Approach

To address the challenge, eHealth Ontario selected the Privacy eSuite consent management service with embedded Universal Audit Repository as the CMTA solution.

Architecture

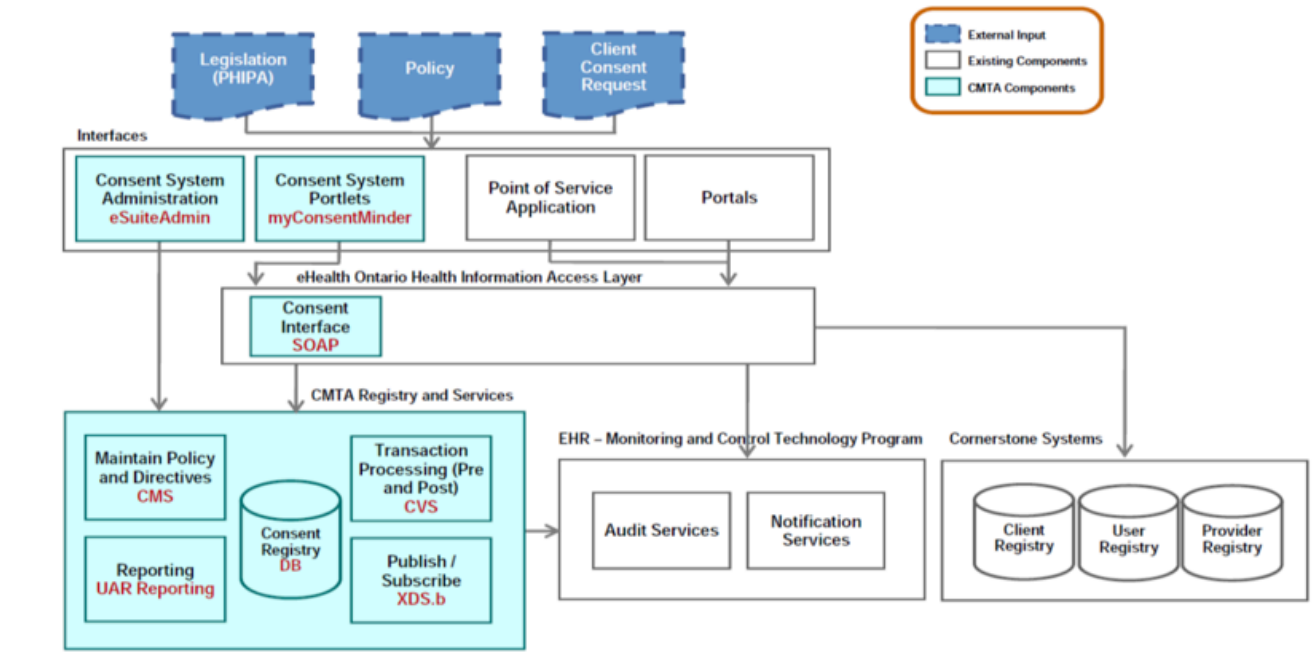


Source: Ontario's Ehealth Blueprint, Fig. 23: Consent Management

CMTA is consent policy neutral, providing the flexibility to ensure that the CMTA solution implementation can follow the consent policy development of the provincial government as the consent policy progresses forward. The CMTA solution provides a privacy-enhanced environment for eHealth Ontario's clinical domain applications by enabling the following:

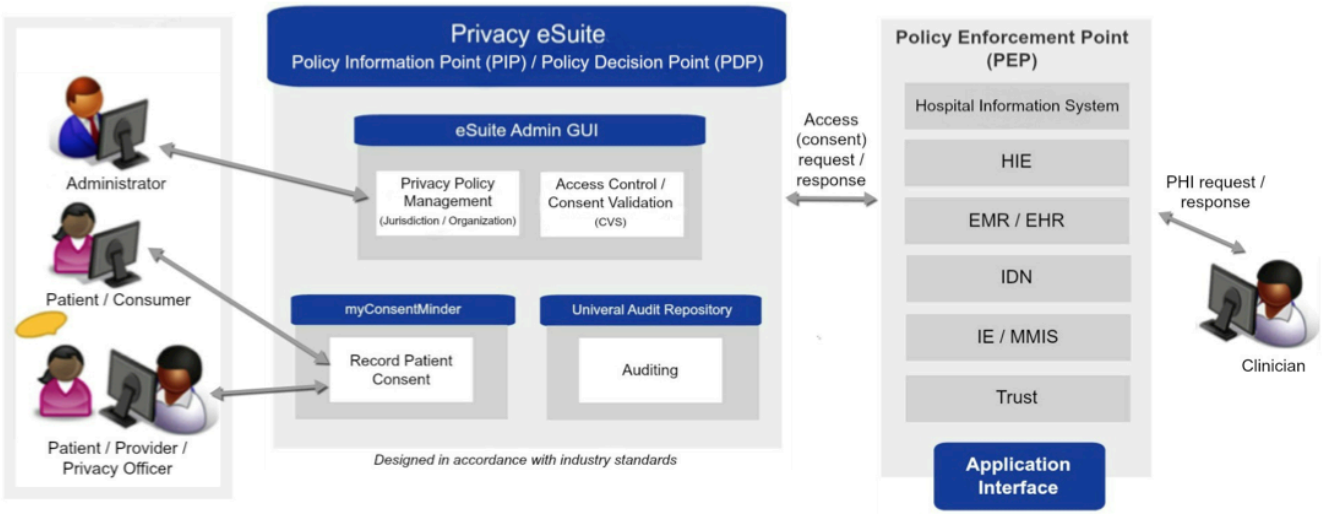
- Standardizing the types of consent directives and the processes by which the consent directives will be implemented
- Logging transactions relating to the implementation, modification or overriding of consent directives
- Providing an interface by which consent directives can be implemented or modified
- A system of record for client EHR consent directives
- Notification to clients regarding override events or updates to client policies
- Privacy officers' management of consent directives on behalf of clients and hospital privacy offices
- Use by all lines of business (domain repositories) to manage and validate client consent
- Use as a province-wide registry for client consent directives

Architecture (cont'd)



Privacy eSuite (PeS) was developed by HIPAAT to centrally manage and help enforce health information privacy preferences (or, consent directives) established by patients, organizations and jurisdictions. It manages directives regarding the collection, use and disclosure of electronic PHI. Authorized users may create, store, update and revoke privacy policies / consent directives on behalf of patients. All of these actions are carried out and audited immediately across the network and enforced by access control mechanisms. This provides functionality for the:

- Management of consent directives on the behalf of individuals to restrict access to their PHI
- Evaluation of consent directives to determine appropriateness of access to an individual's PHI
- Audit logging of all consent directive events for reporting and alert notification



Solution Design

PeS provides the decision point for balancing personal health information (PHI) privacy against clinical access to health information in support of improved quality of care. The eSuite Admin user interface application is used by system administrators and compliance/privacy officers, and provides full management capabilities to these users based on the roles and functions allowed for each. Standards-based privacy policies may be created at various levels of granularity including, but not limited to:

- Purpose of use: treatment, research, marketing, etc.
- Information type: laboratory results, radiology exam, medication, etc.
- Specific user(s): roles, groups of users, facility, etc.
- PHI identifiers: category codes, classification codes, etc.

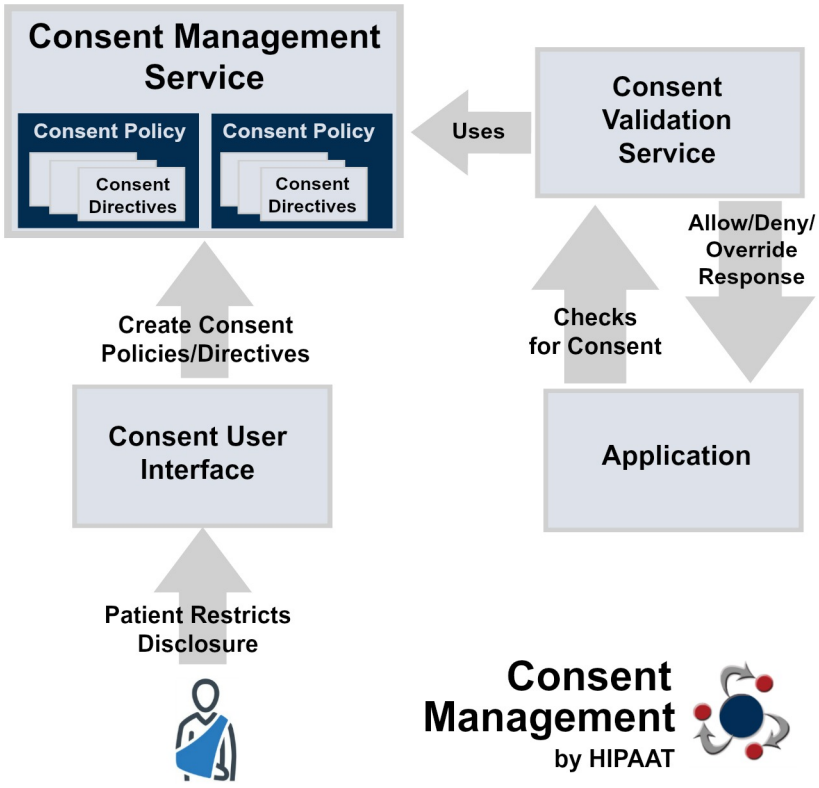
Within the Privacy eSuite environment, there are different components that allow for the proper management of information privacy.

eSuiteAdmin A browser-based user interface (UI) that enables the system administrator to set up business rules for policies, consent directives (within the policies), and report generation.

myConsentMinder (myCM) This GUI is a web-based, end-user-facing application (citizen, patient, clinician or social-services agent) for managing privacy preferences. Users create privacy policies using simple preconfigured web templates created through PeS.

Consent Management Service (CMS) This enables consumer, organizational and jurisdictional privacy policies to be administered and processed into computable access rules.

Consent Validation Service (CVS) This high-speed service (>1,000 tps) determines if a user's access to a patient's PHI is appropriate, based on the rules of the existing privacy policies, and provides a decision of "Permit," "Deny," or "Permit through override" to the PHI-requesting system.



Universal Audit Repository (UAR) This is a Java-based, IHE-ATNA compliant audit repository. As mentioned earlier, it is the audit repository that tracks audit events related to updates, queries, and retrievals and deletions. The UAR is the primary source for privacy and security reports for all updates and access to PHI. Key functional features:

- Provides the ability for authorized users to create reports based upon any audit event data as well as to schedule the generation of reports (e.g. Accounting of Disclosures)
- Provides security notifications based upon the receipt of "Security Alert" audit event messages
    - Allows for external Notification Alerts to be utilized
- Accepts all IHE-ATNA audit log messages

Interoperability

Service-oriented architecture interoperability between the eHealth Ontario enterprise service bus, known locally as the Health Information Access Layer (HIAL), and Privacy eSuite is achieved using direct Simple Object Access Protocol (SOAP) messages. Alternatively, the HIPAAT Java Consent Policy Interface (JCPI) can be used.

Java Consent Policy Interface (JCPI):

- Direct interactions with an enterprise service bus (ESB); manages privacy policies programmatically
- Create/update/revoke/reorder patient policies and system consent directives
    - Supports both single and batch requests

Clinical Value of Privacy Controls

Privacy controls encourage people to seek treatment without fear that by doing so, their privacy would be compromised and they could be subject to negative perceptions and discrimination, criminal legal consequences, or civil legal consequences such as: loss of child custody, employment or housing.

More specifically, these controls protect the confidentiality of the identity, diagnosis, prognosis or treatment of any patient records maintained in connection with the performance of any program or activity relating to sensitive health conditions (i.e. behavioural, mental or sexual) which may result in education, prevention, training, treatment, rehabilitation or research.

Privacy controls also ensure that the organization manages PHI in a manner that is consistent with its legislative responsibilities and public commitments:

- improve the patient experience
- mitigate privacy risks
- support best practices

Clinical Workflow Impact

There is no impact to the clinical workflow unless the clinician encounters a situation where a patient or an organization has enacted a consent directive against a specified PHI artifact. Only at that time does the clinical flow get interrupted with a message generated by the system that the user will need to interact with, to either cancel their query or gain override/break-the-glass access to the PHI artifact. This will then trigger an auditable event and provide a notification to a designated individual, e.g. Compliance Officer.

References

Video: Ontario's Ehealth Blueprint: https://youtu.be/uX5-rcmTpqA
Ehealth Blueprint: Consent & Privacy Audit:
http://www.ehealthblueprint.com/en/documentation/chapter/consent-and-privacy-audit

Contact

info@hipaat.com