Toronto General

Princess Margaret

Toronto Western

Toronto Rehab

Computable Privacy Use Case: Health Information Exchange

Situation

The ConnectingGTA (cGTA) Project is a major clinical integration initiative that encompasses a population of 6.3 million across a large, diverse, and complex set of health care services and health care providers in the Greater Toronto Area (GTA).

The project was initiated to improve patient care delivery by allowing for timely initiation of treatment and increased coordination amongst individual health care providers while creating a robust technical infrastructure that would allow multiple partners and vendors the ability to develop new and innovative functionality in the future.

Challenge

The following EHR privacy considerations and risks are associated with the clinical integration initiative:

EHR Privacy Considerations

- Allow for the collection, use and disclosure of large amounts of health information from diverse sources
- Health care providers do not have sole custody or control of health information in a shared system
- Health care providers have different processes for implementing patient consent models

EHR Risks

- Increases the risk of health care providers using or disclosing health information for unauthorized purposes
- May attract hackers and others with malicious intent
- Easier to remove health information from a secure location and to transfer it to an unsecure device

Stakeholders

cGTA encompasses six Local Health Integration Networks (LHINs), over 700 health service providers (HSPs) and over 12,000 physicians.

From the outset, of the 700+ HSPs, there are 5 Community Care Access Centres (CCACs), 45 hospitals, 28 community health centres, 157 mental health and addiction services, 202 long-term care facilities, and 257 community support services. In addition, there are 60 family health teams as well as over 2,000 individual health care providers in the GTA.

Approach

To address the privacy challenges, cGTA selected the Privacy eSuite consent management solution.

Background

Individual health care providers often have limited access to electronic patient data outside the boundaries of their organization or practice. To make informed diagnostic decisions, providers may repeat laboratory / diagnostic tests or perform administrative tasks to collect the necessary electronic patient data that may already exist at other organizations or practices previously visited by their patients. This is often an inefficient process, increasing the cost to the health care system and negatively impacting the quality of patient care.

The cGTA Project identified the following key objectives:

- Provide individual health care providers with access to relevant electronic patient data at the point of care, thereby improving the patient experience as patients navigate through the continuum of care within the GTA
- Develop and implement a robust, scalable and extensible platform that will allow electronic patient data to be exchanged securely and seamlessly, while fostering innovation where multiple partners and vendors can participate
- Develop the infrastructure and services to support other regional and provincial e-health initiatives
- Foster collaboration amongst health care providers in working towards electronic health records (EHRs) and personal health records

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.

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

Governance

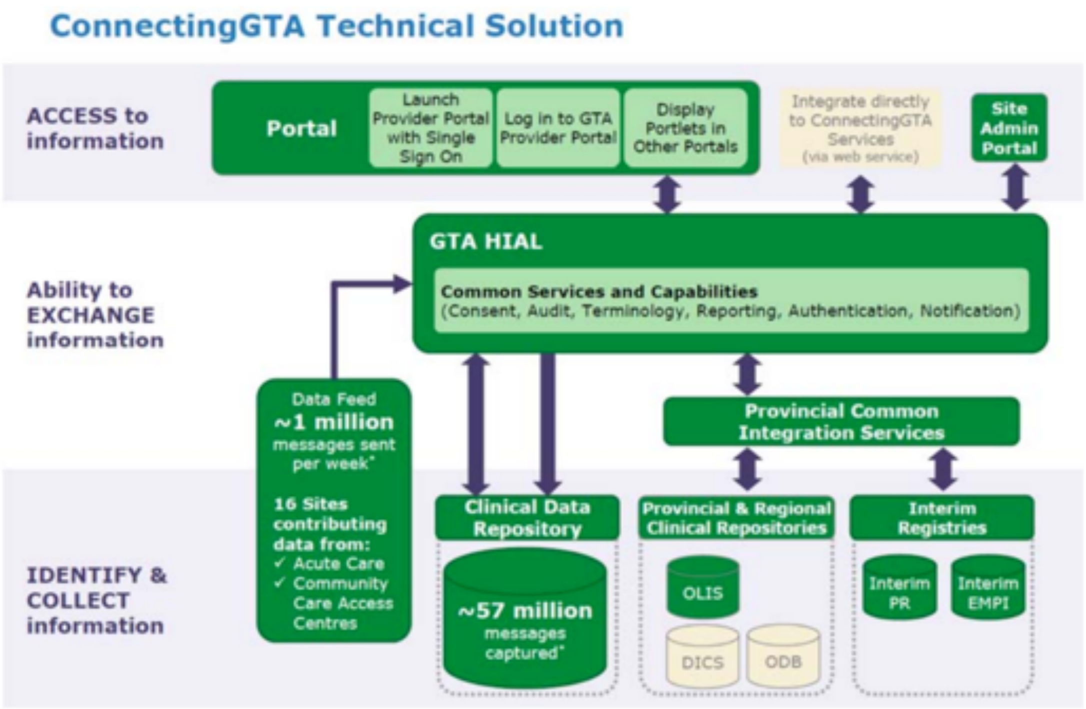
In the cGTA Solution, an individual may make, modify or withdraw the following consent directives in respect of an individual's PHI:

- Global consent directives (Opt-out)
- Domain consent directives (e.g. radiology, labs, etc.)
- Record-level consent directives
- Organizational consent directives
- Clinician-specific consent directives

Architecture

The cGTA Solution is composed of several information system components, and viewed as a single system by any point of service (POS) system accessing it. The cGTA Solution brings together:

- a health information access layer (HIAL) developed on a commercial-off-the-shelf (COTS) platform to enable different types of electronic patient data to be accessed and displayed in an interoperable and trusted manner across the health care providers of the GTA
- a Clinical Data Repository (CDR) with a COTS database designed to store specific electronic patient data
- a Provider Portal and portlets to provide access to cGTA services and available provincial domains through a standard web browser or desktop (e.g. a compliant hospital information system (HIS), electronic medical record (EMR), or other portal)


ConnectingGTA Technical Solution
ACCESS to information
Portal
Launch Provider Portal with Single Sign On
Log in to GTA Provider Portal
Display Portlets in Other Portals
Integrate directly to ConnectingGTA Services (via web service)
Site Admin Portal
Ability to EXCHANGE information
GTA HIAL
Common Services and Capabilities
(Consent, Audit, Terminology, Reporting, Authentication, Notification)
Data Feed
~1 million messages sent per week*
16 Sites contributing data from:
✓ Acute Care
✓ Community Care Access Centres
Provincial Common Integration Services
IDENTIFY & COLLECT information
Clinical Data Repository
~57 million messages captured*
Provincial & Regional Clinical Repositories
OLIS
DICS
ODB
Interim Registries
Interim PR
Interim EMPI

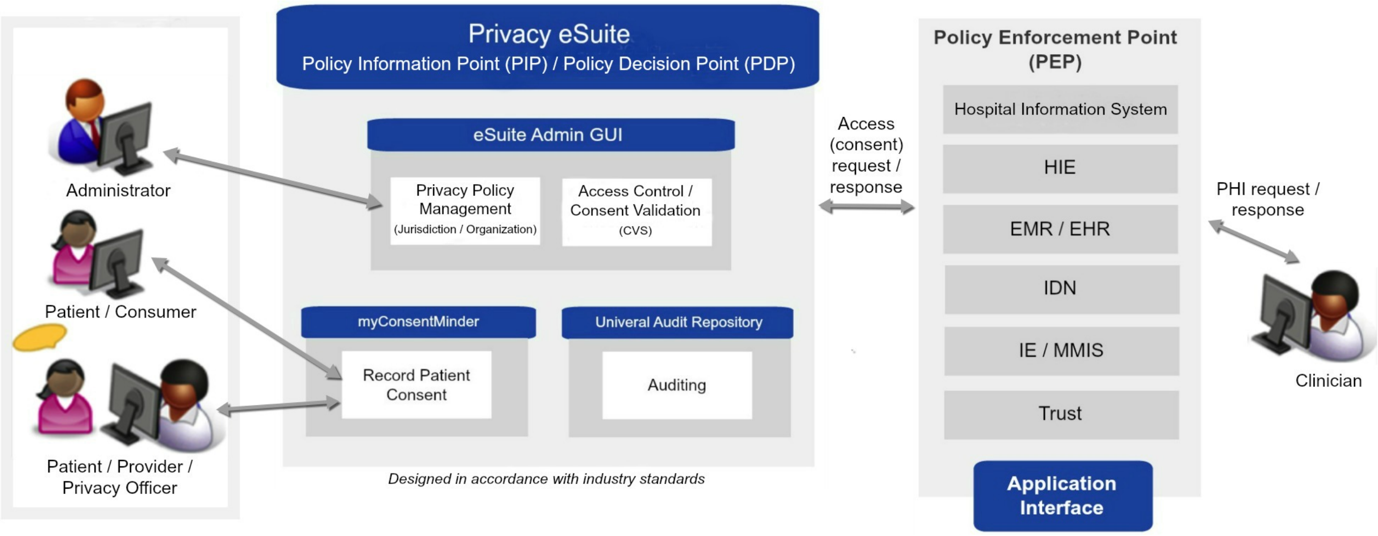
Software Integrated

Privacy eSuite (PeS)
Privacy eSuite is 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.

Privacy eSuite was developed to centrally manage and help control and 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 protected/private health information (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, thereby providing functionality for the:

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

Solution Design (PeS)


Administrator
Patient / Consumer
Patient / Provider / Privacy Officer
Privacy eSuite
Policy Information Point (PIP) / Policy Decision Point (PDP)
eSuite Admin GUI
Privacy Policy Management (Jurisdiction / Organization)
Access Control / Consent Validation (CVS)
myConsentMinder
Record Patient Consent
Univeral Audit Repository
Auditing
Designed in accordance with industry standards
Access (consent) request / response
Policy Enforcement Point (PEP)
Hospital Information System
HIE
EMR / EHR
IDN
IE / MMIS
Trust
Application Interface
PHI request / response
Clinician

Privacy eSuite provides the decision point for balancing PHI privacy against clinical access to health information in support of improved quality of care. 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.

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. It is the central audit repository that tracks audit events related to updates, queries, retrievals and deletions. For this implementation, the UAR pushes all consent-related IHE-ATNA messages to the native platform’s audit repository.

Interoperability

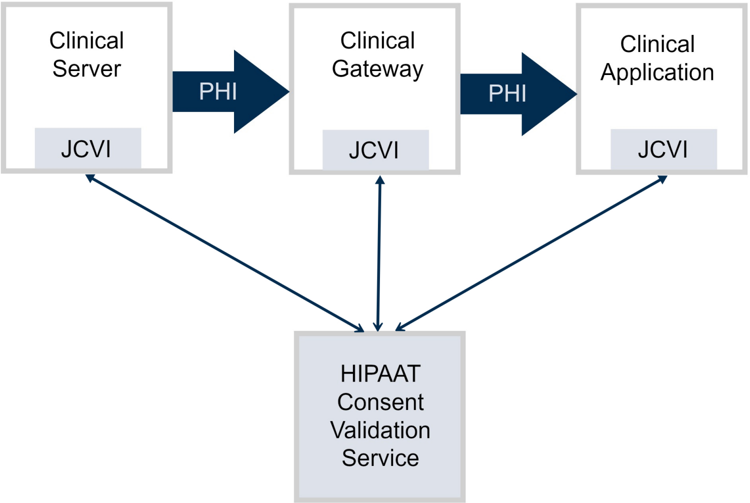
Interoperability between the cGTA technology platform and HIPAAT Privacy eSuite was accomplished using both the Java Consent Validation Interface (JCVI) and the Java Consent Policy Interface (JCPI):

Java Consent Validation Interface (JCVI)

- Provides a standards-based integration point between the consumer application and the consent validation service
- Interoperability service, where requests can be sent and received using Simple Object Access Protocol (SOAP)
    - Deals with the creation of the request and interpreting the response

Java Consent Policy Interface (JCPI)

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



Lessons Learned (provided by Chief Privacy Officer)

- No two organizations are the same
- Be prepared to change
- Agree on common terminology
- Bring privacy into the design of the system
- Separate the policy from the standards
- Policies and standards should focus on patient’s perspective
- Ensure privacy is embedded into the clinical and patient processes
- Align participant's privacy programs
- Test and learn

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

2014 HP-IAPP Privacy Innovation Award Winner-Large Organization: University Health Network
https://www.youtube.com/watch?v=W5POpi5URxw

Contact

info@hipaat.com