- Largest single-site hospital in Canada
- $1B annual operating budget
- 1.2 million patient visits each year
- Teaching hospital at Univ. of Toronto
- $100M breakthrough research each year

Computable Privacy Use Case: Large Hospital Center

Situation

The Ontario Personal Health Information Protection Act (PHIPA) prohibits a provider organization from using or disclosing an individual's personal/protected health information (PHI) where the individual has expressly prohibited such use or disclosure for a particular purpose.

The individual's express instruction for limiting use or disclosure happens within the person's records by means of a consent directive (CD) – a logical or physical restriction on access to the records which are the object of the consent directive.

Practically, a CD can be imposed on any element of the patient's record(s), but is often generalized to 'the entire record', date-to-date ranges of records, or individual or combinations of individual records. Consent directives can also, where feasible, be applied to restrict specific providers or provider organizations from accessing the object records, such as restricting disclosure to certain third party health care provider/provider organizations.

Sunnybrook Health Sciences Centre's challenge was to effectively address those PHIPA requirements with an innovative and comprehensive privacy solution that would complement SunnyCare, Sunnybrook's electronic health record.

Approach

To address the challenge, Sunnybrook integrated HIPAAT's Privacy eSuite consent management service and Universal Audit Repository software with the SunnyCare platform.

Problems Addressed

Consent Management
Privacy Policy Management
Access Control
Break-the-Glass
Auditing

Consent Model Supported

Opt-Out with Exceptions (Implied)
Override
Break-the-Glass

Auditing Functions Supported

Successful and Unsuccessful Logon
Logoff / Timeout
Views
Updates / Saves
Deletes
Access to External Objects, e.g. HIE Interactions
Security Alert of Override / Break-the-Glass Access to PHI

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 EHR ecosystem.

Universal Audit Repository (UAR) – a Java-based, IHE-ATNA compliant, central audit repository that tracks audit events related to updates, queries and retrievals. The UAR is the primary source for privacy and security reports for all updates and access to PHI.

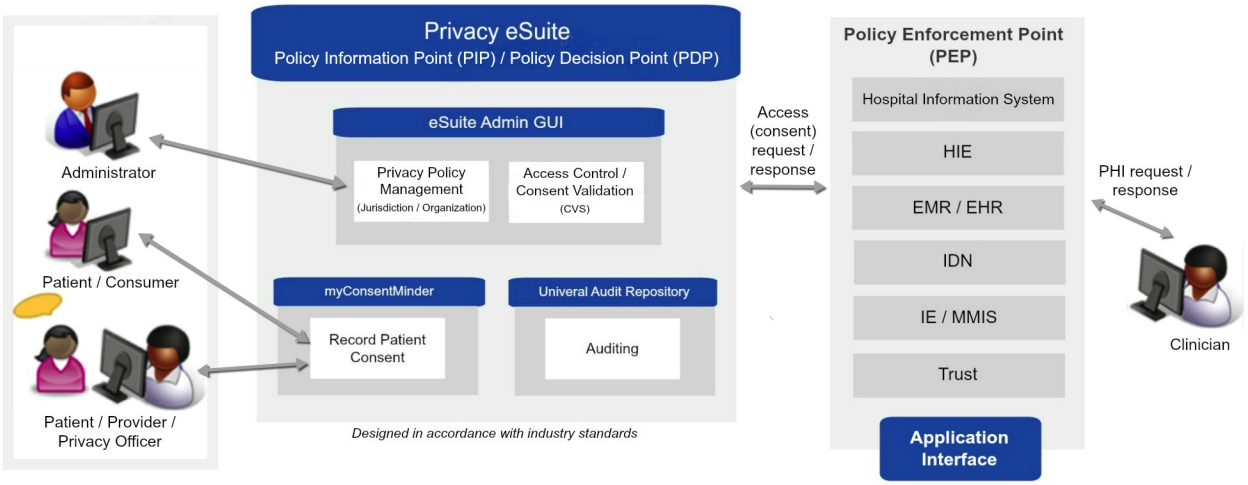
Technical Overview

Sunnybrook Health Sciences Center is the largest single-site hospital in Canada, has a $1 billion annual operating budget, includes a trauma center and achieves $100 million of breakthrough research each year. In 2012, Sunnybrook management performed a market analysis of all the available electronic health record (EHR) COTS products available, and chose to develop their own "SunnyCare" EHR (PC & mobile applications) to overlay all of their existing information systems as a "simple-to-use platform."

- Patient Lists
- Patient Overview
- Results Viewing
- ***Audit and Lockbox [consent management]***
- Clinical Messaging
- Clinical Documentation
- CPOE
- Clinician Inbox
- Nursing and Allied Health

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



PeS 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:

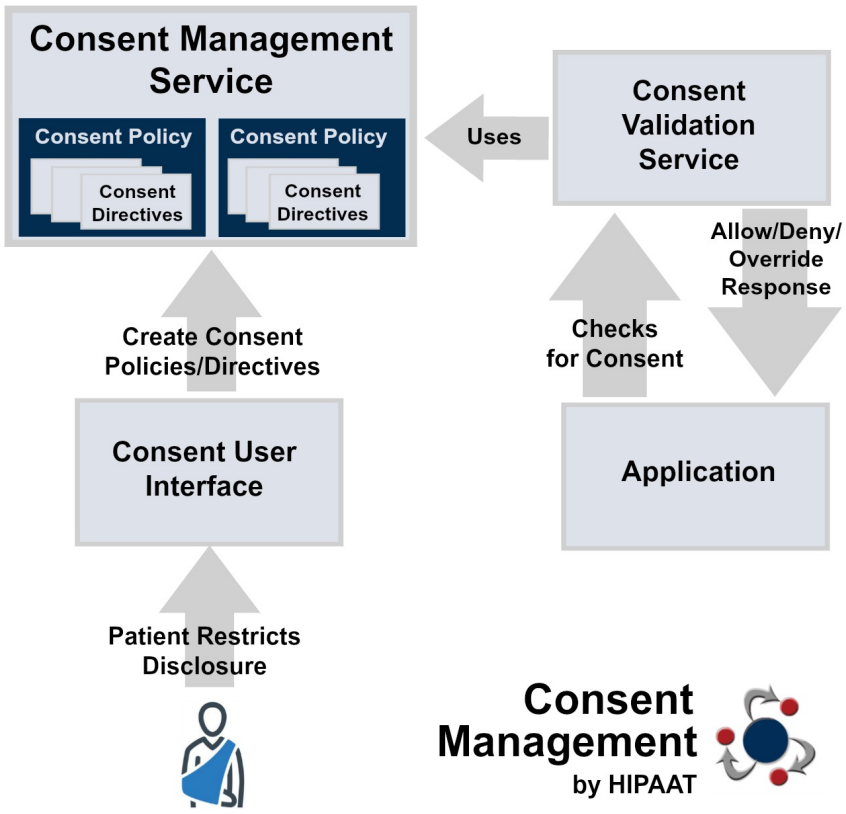
- Purpose of use: treatment, research, marketing, etc.
- Information type: laboratory results, radiology exam, medication, etc.
- Specific user(s): roles, groups of users, facility, etc.
- PHI identifiers: category codes, classification codes, etc.

Technical Overview (cont'd)

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

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.



The administration and management of consent directives is enabled through the eSuite Admin user interface application. eSuiteAdmin 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. The consent validation service evaluates any active directives for a patient and provides a decision of "Permit", "Deny", or "Permit through override" to the requesting system.

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

- 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

Interoperability between the SunnyCare EHR and HIPAAT Privacy eSuite/UAR was achieved through the use of the Java Audit Toolkit (JAT) which facilitates the creation of XML audit messages in accordance with the IHE-ATNA XML schema, and the Java Consent Validation Interface (JCVI) which provides a standards-based integration point between the consumer application and the consent validation service. This interoperability service deals with the creation and response interpretation of Simple Object Access Protocol (SOAP) messages.

Documented Improvements that the Practice Enables

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 (ie: substance abuse), 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.

Impact to Clinical Workflow

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.

Challenges

No challenges beyond normal project management cycles were encountered.

References

https://www.youtube.com/watch?v=zeugoStid_4&feature=youtu.be

Contact

info@hipaat.com