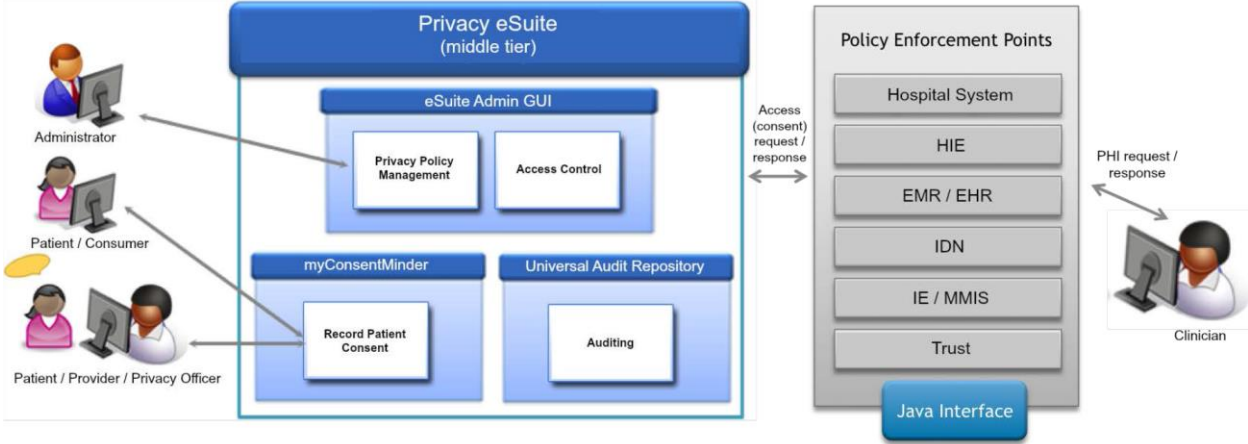


Data Sharing Consent/Privacy Practice Summary

Profile Element	Description
Responsible Entity	HIPAAT International Inc.
Legal Authority	<p>US</p> <ul style="list-style-type: none"> • HIPAA • HITECH • 42CFR Part II <p>Canada</p> <ul style="list-style-type: none"> • Personal Information Protection and Electronic Documents Act (PIPEDA) • Ontario Personal Health Information Protection Act (PHIPA)
Entities Involved in Data Exchange	<p>Sunnybrook Health Sciences Centre, Toronto, Ontario, Canada</p> <ul style="list-style-type: none"> • Services include: cancer, heart and vascular, high risk maternal and newborn, image guided brain therapies, trauma • 1.2 million patient visits per year • 1,200 beds
Problem Addressed	<p>Consent Management</p> <p>Privacy Policy Management</p> <p>Access Control</p> <p>Break the Glass</p> <p>Auditing</p>
Description	<p>The <i>Personal Health Information Protection Act</i> (PHIPA) prohibits a provider organization from using or disclosing personal/protected health information ("PHI") about an individual where that individual has expressly prohibited the provider organization from using or disclosing it for a particular purpose.</p>

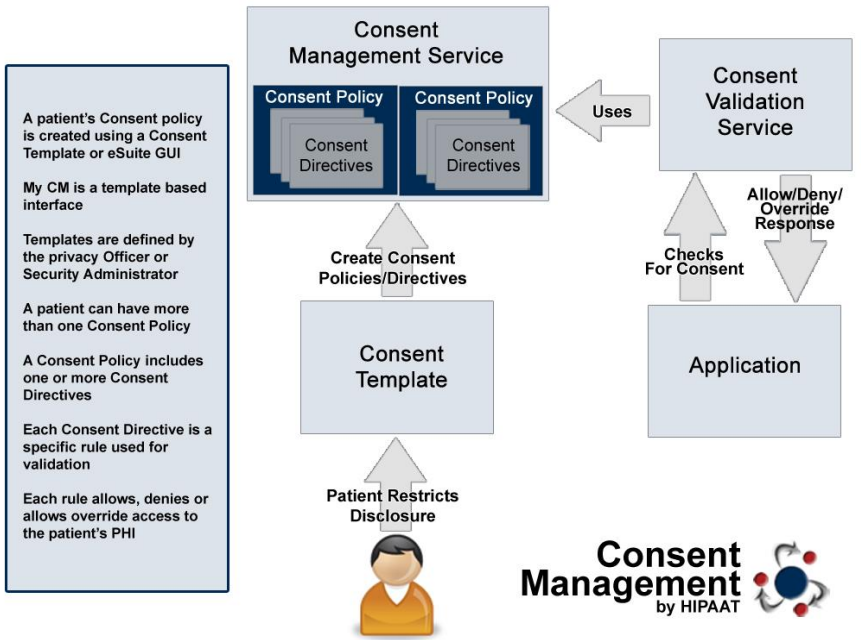
Profile Element	Description
	<p>The express instruction for limiting the use or disclosure is effected within the patient records by means of a consent directive (CD) – the imposition of a logical or physical restriction on access to the records which are the object of the consent directive.</p> <p>Practically, a CD can be imposed on any element of the patient’s record(s), but is typically generalized to, for example, ‘the entire record’, date-to-date ranges of records, or individual or combinations of individual records. Consent directives can also – where feasible – be applicable to restrict specific providers or provider organizations from accessing the object records, such as restricting disclosure to certain third party health care provider/provider organization.</p> <p>To accomplish compliance with regulations, an integration with the HIPAAT Privacy eSuite consent management service and Universal Audit Repository software products to the Sunnybrook Health Sciences Centre’s SunnyCare platform was performed.</p> <p>Consent model supported:</p> <ul style="list-style-type: none"> • Opt-Out with Exceptions • Override/Break-the-Glass <p>Auditing</p> <ul style="list-style-type: none"> • 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

Profile Element	Description
Standards Implemented	IHE-ATNA audit messages HISPC III Intrastate and Interstate Consent Policy Option: <i>Opt-out with Exceptions</i>
Policies Adopted	US <ul style="list-style-type: none"> • Nationwide Privacy & Security Framework for Electronic Exchange of IIHI UK <ul style="list-style-type: none"> • Principles for Implementing Permission to View for the Summary Care Record (v2.0) • “Sealed Envelopes” Briefing Paper (v2.0) • Share with Care: People’s views on Consent & Confidentiality of Patient Information
Legal Agreements	A Software License and Maintenance Agreement bound to a Statement of Work.
Clinical Workflow Impacts	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 which will then trigger an auditable event and provide a notification to a designated individual (ie: Compliance Officer).
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.” <ul style="list-style-type: none"> • Patient Lists • Patient Overview • Results Viewing • Audit and Lockbox [consent management] • Clinical Messaging

Profile Element	Description
	<ul style="list-style-type: none"> • Clinical Documentation • CPOE • Clinician Inbox • Nursing and Allied Health <p>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:</p> <ul style="list-style-type: none"> • Management of consent directives on the behalf of clients to restrict access to their PHI • Evaluation of consent directives to determine appropriateness of access to a client's PHI • Audit logging of all consent directive events for reporting and alert notification  <p>The diagram illustrates the Privacy eSuite architecture. On the left, three user roles are shown: Administrator, Patient/Consumer, and Patient/Provider/Privacy Officer. These users interact with the Privacy eSuite (middle tier), which is divided into two main sections. The top section is the eSuite Admin GUI, containing Privacy Policy Management and Access Control. The bottom section consists of myConsentMinder (with Record Patient Consent) and the Universal Audit Repository (with Auditing). On the right, a vertical stack of Policy Enforcement Points includes Hospital System, HIE, EMR/EHR, IDN, IE/MMIS, and Trust, all connected via a Java Interface. Bidirectional arrows indicate 'Access (consent) request / response' between the middle tier and the enforcement points, and 'PHI request / response' between the enforcement points and a Clinician user.</p>

Profile Element	Description
	<p>It provides the decision point for balancing personal health information (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:</p> <ul style="list-style-type: none"> • Purpose of use <ul style="list-style-type: none"> ○ treatment, research, marketing, etc • Information type <ul style="list-style-type: none"> ○ laboratory results, radiology exam, medication, etc • Specific user(s) <ul style="list-style-type: none"> ○ roles, groups of users, facility, etc • PHI identifiers <ul style="list-style-type: none"> ○ category codes, classification codes, etc <p>Within the Privacy eSuite environment, there are different components that allow for the proper management of information privacy.</p> <p>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.</p> <p>Consent Management Service (CMS). This enables consumer, organizational and jurisdictional privacy policies to be administered and processed into computable access rules.</p> <p>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.</p>

Profile Element	Description
-----------------	-------------



A patient's Consent policy is created using a Consent Template or eSuite GUI

My CM is a template based interface

Templates are defined by the privacy Officer or Security Administrator

A patient can have more than one Consent Policy

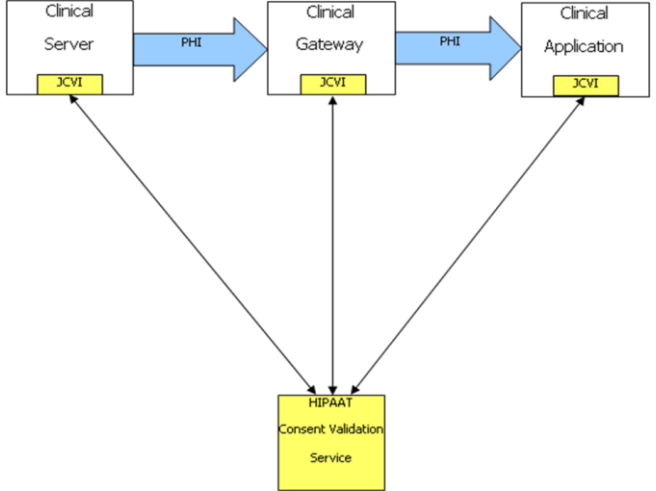
A Consent Policy includes one or more Consent Directives

Each Consent Directive is a specific rule used for validation

Each rule allows, denies or allows override access to the patient's PHI

The Privacy eSuite solution provides two user interfaces for the administration and management of consent directives. The eSuiteAdmin user interface application is for use by system administrators and compliance/privacy officers, and provides full management capabilities to these users based on roles and functions allowed for each. The myConsentMinder is a template based portlet which can be used within any clinical portal. It is intended for use by clients, patients, substitute decision makers, or clinical staff. 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. It is the central audit

Profile Element	Description
	<p>repository that tracks audit events related to updates, queries, and retrievals. The UAR is the primary source for privacy and security reports for all update and access to PHI. Some of the key functional features are:</p> <ul style="list-style-type: none"> • Provides the ability for authorized users to create reports based upon any audit event data as well as to schedule the generation of reports (ie: Accounting of Disclosures) • Provides security notifications based upon the receipt of “Security Alert” audit event messages <ul style="list-style-type: none"> ○ Allows for external Notification Alerts to be utilized • Accepts all (IHE ATNA) audit log messages <p>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</p>  <pre> graph TD subgraph TopRow CS[Clinical Server] -- PHI --> CG[Clinical Gateway] CG -- PHI --> CA[Clinical Application] end CS <--> HCVS[HIPAAT Consent Validation Service] CG <--> HCVS CA <--> HCVS </pre>

Profile Element	Description
Documented Improvements that the practice enables	<p>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.</p> <p>Ensures that the organization manages personal health information in a manner that is consistent with its public commitments and legislative responsibilities.</p> <ul style="list-style-type: none"> • improve the patient experience • mitigate privacy risks • support best practices
Challenges	<p>Nothing beyond normal project management cycles.</p>
References	<p>https://www.youtube.com/watch?v=zeugoStid_4&feature=youtu.be</p>
Contacts	<p>Kel Callahan HIPAAT International Inc. kcallahan@hipaat.com</p>