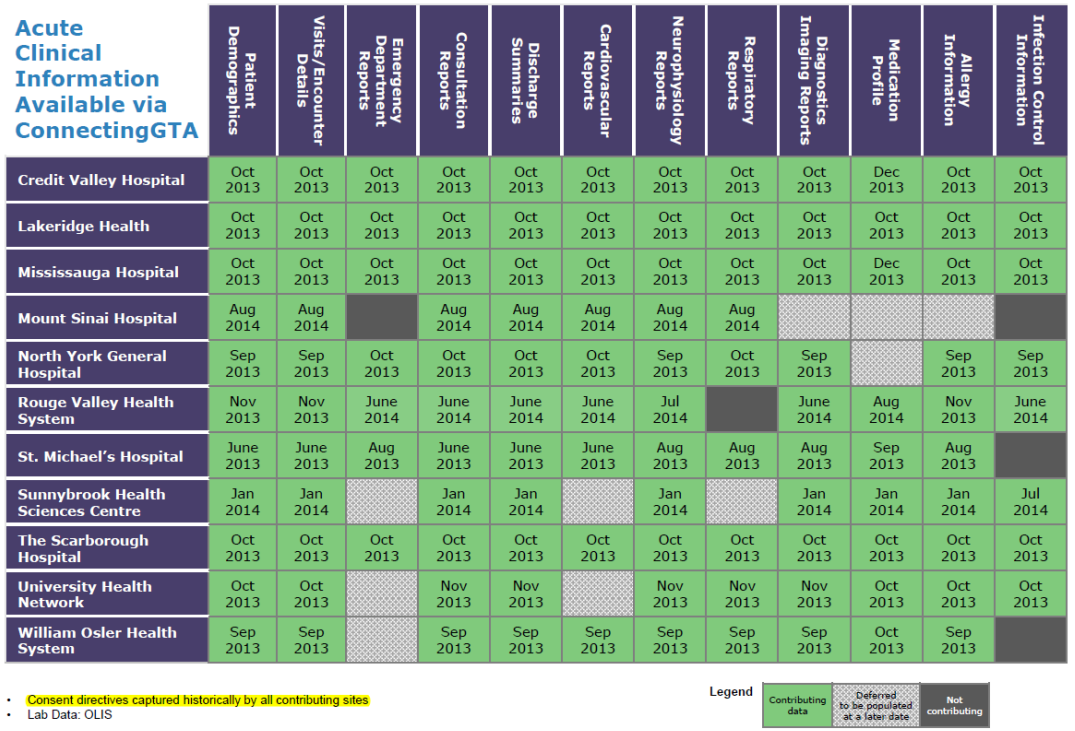
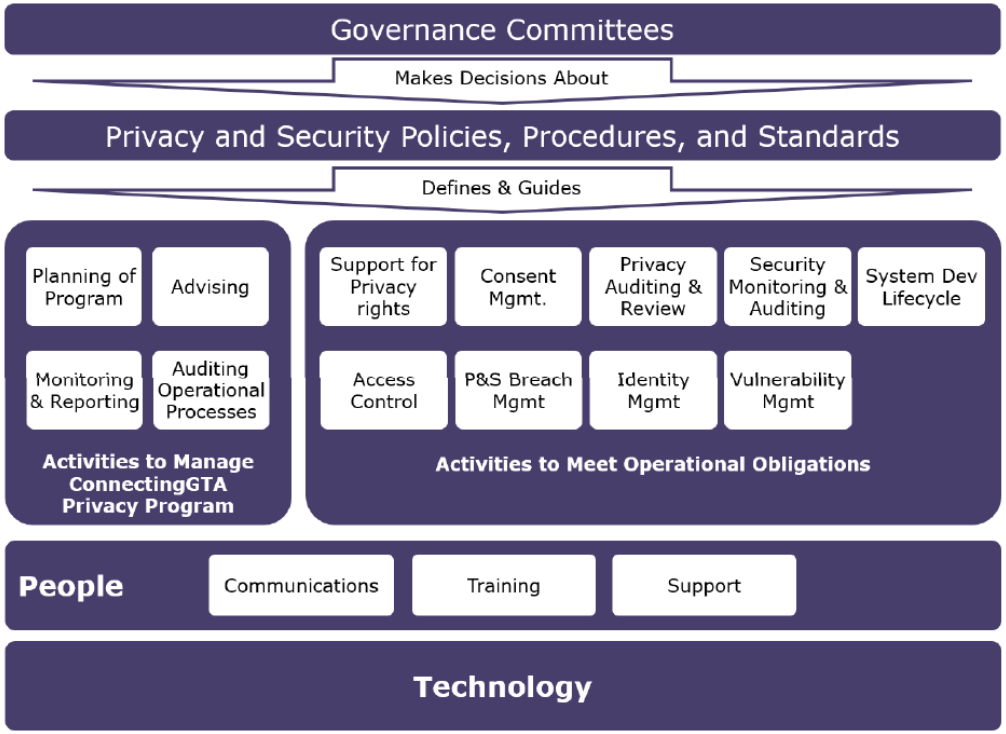
Data Sharing Consent/Privacy Practice Summary

Profile Element	Description
Responsible Entity	HIPAAT International Inc.
Legal Authority	US • HIPAA • HITECH • 42CFR Part II Canada • Personal Information Protection and Electronic Documents Act (PIPEDA) • Ontario Personal Health Information Protection Act (PHIPA)
Entities Involved in Data Exchange	HIE: Connecting the Greater Toronto Area (cGTA) • 6 local Health Integration Networks • 750 healthcare organization • Over 12,000 physicians • Services include: acute care, community support services, complex continuing care, long term care, mental health and addiction, primary care, rehabilitation Many more added since, but as of October 2014:

	
Problem Addressed	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



Data Governance: (Personal Health Information Protection Act – PHIPA)

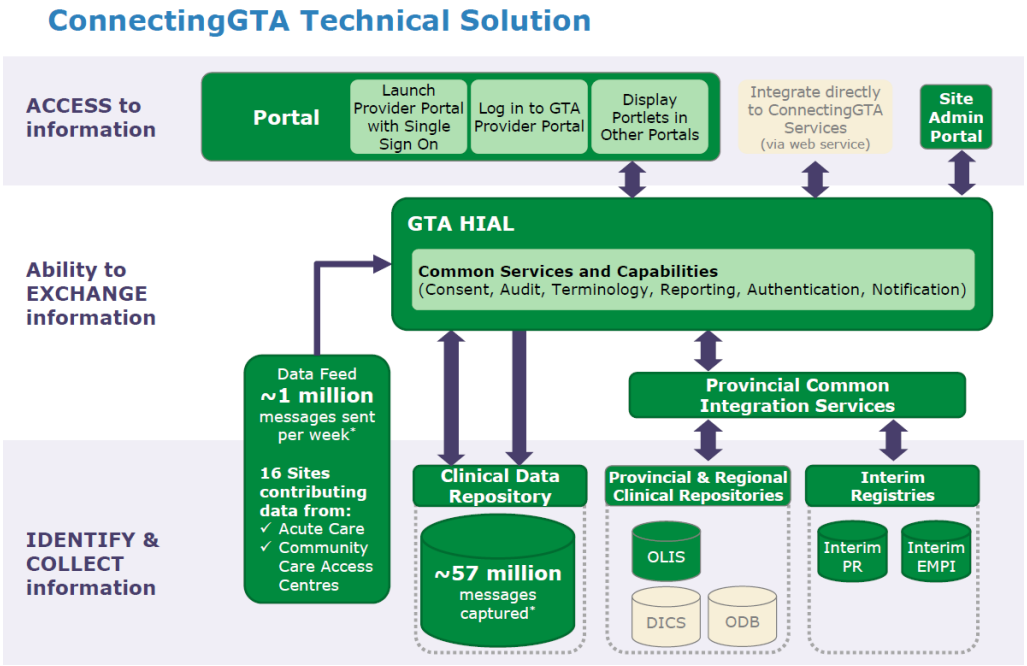
Health Care Providers encompass a wide breadth of individuals and organizations, including (i) a person or entity permitted to provide health care services in Ontario, including a Health Service Provider or HSP as defined under the Local Health System Integration Act, 2006 or a health information custodian as defined under PHIPA; (ii) a prescribed person who compiles or maintains a registry of Personal Health Information under Section 39(1) of PHIPA; (iii) a prescribed entity under Section 45(1) of PHIPA; (iv) a health data institute under Section 47(2) of PHIPA; and (v) a researcher or other person granted access by another Health Care Provider in accordance with PHIPA.

	Consent Management – both local and external domains Privacy Policy Management Access Control – limited display of PHI subject to a directive Override/Break the Glass Auditing
Description	The ConnectingGTA Project is a major clinical integration initiative which encompasses a population of 6.3 million across a large, diverse, and complex set of health care services and Health Care Providers. 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, individual Health Care Providers currently may be repeating laboratory/diagnostic tests or performing 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 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. To achieve this, the ConnectingGTA Project identified the following key objectives: • Providing 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 • Developing and implementing 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 • Developing the infrastructure and services to support other regional and provincial e-health initiatives • Fostering collaboration amongst Health Care Providers in working towards Electronic Health Records (EHRs) and personal health records **Guiding Principles to Deliver Clinical Value.** Use a patient-centered approach to build a comprehensive patient view, by

	capturing and sharing the largest volume of data needed most frequently by patients and providers (e.g. transitions from acute to community). ConnectingGTA seeks to: • Support continuity of care and seamless transition between providers • Deliver clinical value to clinicians as quickly and efficiently as possible • Utilize existing expertise and work effort • Build a compelling value proposition for clinicians and patients **Data Governance:** The Individual may make, modify or withdraw the following Consent Directives in respect of the Individual's PHI in the ConnectingGTA Solution: • Global Consent Directives (Opt-out) • Domain Consent Directives (ie: radiology, labs, etc.) • Record-level Consent Directives • Organizational Consent Directives • Clinician-specific Consent Directives Consent validation Auditing
Standards Implemented	IHE-ATNA audit messages HISPC III Intrastate and Interstate Consent Policy Option: *Opt-out with Exceptions*
Policies Adopted	A [provider-clinician] shall only override a Consent Directive and shall only collect PHI in the ConnectingGTA Solution that is the subject of a Consent Directive where the [provider-clinician] seeking to collect the PHI: • Obtains the express consent of the Individual to whom the PHI relates • Believes on reasonable grounds that the collection is necessary for the purpose of eliminating or reducing a significant risk of serious bodily harm to the Individual to whom the PHI relates and it is not

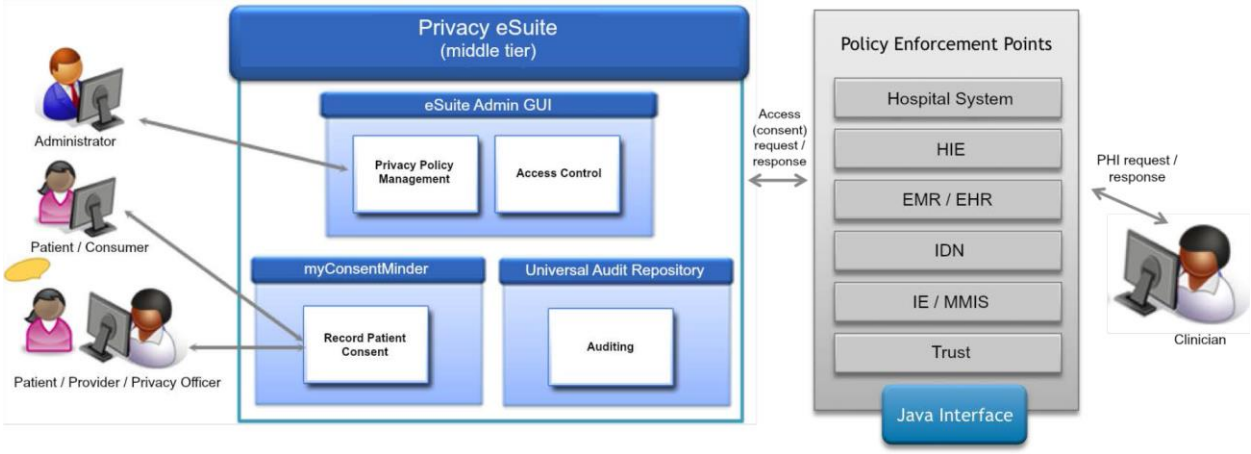
	reasonably possible to obtain the consent of the Individual in a timely manner A [provider-clinician] that overrides a Consent Directive and that collects PHI in the ConnectingGTA Solution that is the subject of the Consent Directive, shall only use or disclose that PHI for the purpose for which the PHI was collected. • *All instances where all or part of the PHI in the ConnectingGTA Solution is collected as a result of an override of a Consent Directive shall be monitored and notice to the [provider-organization]* that collected the PHI in the ConnectingGTA Solution that is the subject of the Consent Directive as well as notice to the Individual to whom the PHI relates shall be provided. US • Nationwide Privacy & Security Framework for Electronic Exchange of IIHI UK • 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	[HIE Participant] EHR Contributor Agreement [HIE Platform Vendor] Master Sales Agreement [HIPAAT] Software License and Maintenance Agreement and associated Statements 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	The overall ConnectingGTA Solution involves a comprehensive integrated technology solution comprised of hardware, software, and services. There are approximately 700 Health Service Providers (HSPs) in the greater Toronto Area (GTA) that have the potential to participate in the ConnectingGTA Solution. From the outset, of these 700 HSPs, there are 5 Community Care Access Centres (CCAC), 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. The overall ConnectingGTA Solution is composed of several information system components, and viewed as a single system by any Point of Service System accessing it. The ConnectingGTA Solution brings together: • A GTA 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 GTA Clinical Data Repository (CDR) with a COTS database designed to store specific Electronic Patient Data • A GTA Provider Portal and Portlets to provide access to ConnectingGTA 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)



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 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



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:

- 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

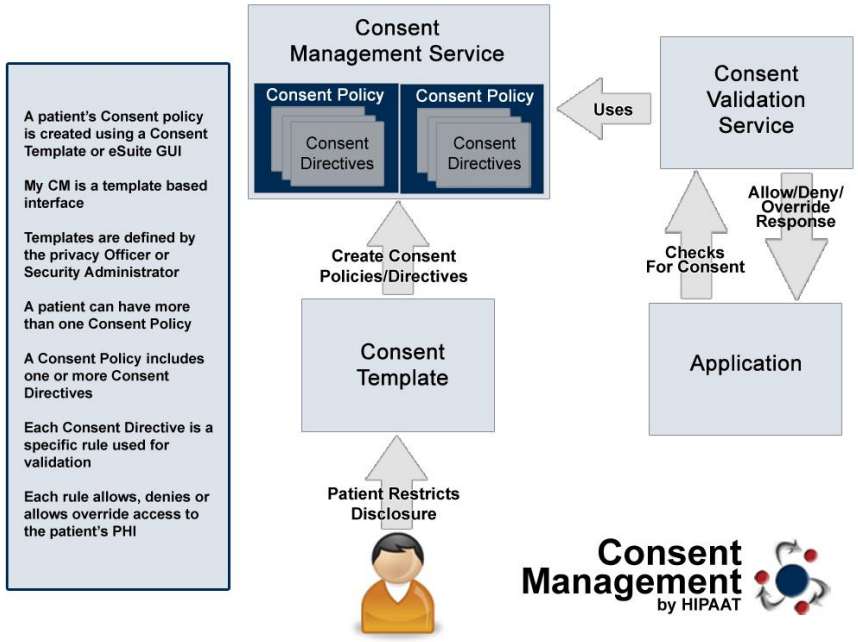
Within the Privacy eSuite environment, there are different components that allow for the proper management of information privacy.

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.

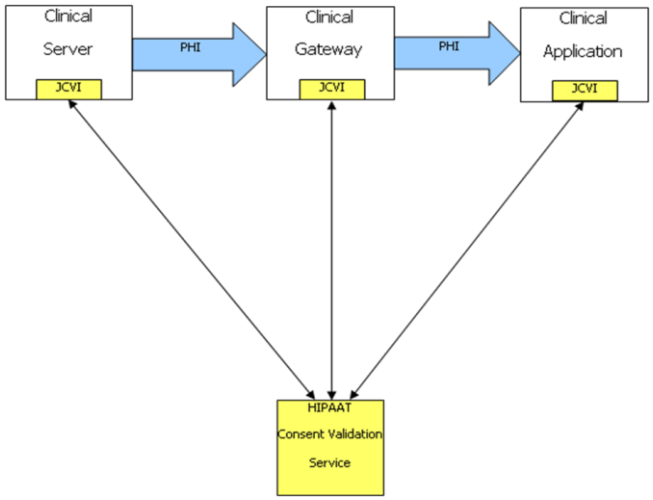
Consent Management Service (CMS). This enables consumer, organizational and jurisdictional privacy policies to be administered and processed into computable access rules.

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.



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 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:
	
	• 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
	  ○ Allows for external Notification Alerts to be utilized
	• Accepts all (IHE ATNA) audit log messages
	
	Interoperability between the cGTA technology platform and the 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): • 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
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. Ensures that the organization manages personal health information in a manner that is consistent with its public commitments and legislative responsibilities. • improve the patient experience • mitigate privacy risks • support best practices
Challenges	Lessons Learned: (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 embed into the clinical and patient processes • Align participant's privacy programs • Test and Learn
References	cGTA Privacy & Security Lead on 2014 HP-IAPP Privacy Innovation Award (large organization category) https://www.youtube.com/watch?v=W5POpi5URxw
Contacts	Kel Callahan HIPAAT International Inc. kcallahan@hipaat.com