ConnectingGTA Combined Back-End and Front-End Solution

Privacy Impact Assessment

(Executive Summary & Conclusion)

Privacy Office

Document Identifier: n/a

Version: 1.4

Owner: University Health Network

Executive Summary

The ConnectingGTA Program is a health information sharing initiative that will benefit patients and health care providers in the central Ontario region. There are approximately 750 health service providers in this region, serving a population of 6.75M (51 per cent of Ontario's population). However, these providers face significant barriers in their ability to exchange patient health information to support timely and efficient treatment of their patients due to the prevalence of diverse legacy clinical information systems and limited capabilities for integration. Providers are therefore often limited to health information within their organization or practice, which can constrain the quality of care that clinicians provide their patients.

The ConnectingGTA Program is working in partnership with six central Ontario LHINs (Central, Central East, Central West, Mississauga Halton, Toronto Central and North Simcoe Muskoka) to plan and implement the ConnectingGTA Solution, which will build the foundational infrastructure needed to provide clinicians with access to their patients' data from multiple sources in a secure and trusted manner. University Health Network (UHN) will be a delivery partner for the ConnectingGTA Program, working with eHealth Ontario to move the eHealth Strategy forward in central Ontario.

The ConnectingGTA Solution will electronically link and integrate patient information from across the care continuum and make it available at the point-of-care to support the provision of health care and improve both patient and clinician experiences. This health information will include data from regional and provincial data services including the Ontario Laboratory Information System (OLIS) and eventually other sources such as the ODB and GTA West DI-r. The Solution is comprised of two primary components: a Back-End Solution that allows Participants to transmit and store PHI in a Clinical Data Repository; and the Front-End Solution, which allows Participants to view PHI in this Repository at their points of care.

UHN intends to launch a Limited Production Release (LPR) of the ConnectingGTA Solution in Q4 of fiscal year 21013/14. In this LPR, approximately 50 Clinicians from 16 ConnectingGTA Participants will be able to access the ConnectingGTA Solution and view clinical data for their patients.

The LPR will be conducted over two stages:

- In Stage 1, clinician end users will be engaged in clinical testing and validation of the ConnectingGTA Solution to ensure that clinical data is delivered as needed to support the provision of care;
- In Stage 2, clinician end users will engage in general clinical use of the ConnectingGTA Solution.

In addition to providing an opportunity for clinical end users to test the ConnectingGTA Solution, the LPR will provide UHN with an opportunity to implement and make adjustments to the operational framework that will support the ConnectingGTA program, including the ConnectingGTA privacy and security program.

For the LPR, the ConnectingGTA Back-End Solution will support the population of the CDR by 16 Originating Participants who will contribute PHI associated with prioritized data types via HL7 messages. These data types will be limited, in the LPR to the following:

- Documents and Notes
- Visits and Encounters
- DI Results
- Other Results
- Community Care

Laboratory and Pathology Results will also be available to end users in the LPR through a data feed from the OLIS via the ConnectingGTA Front-End Solution and will be used for the provision of health care to their patients. Each time a Participant clinical user views PHI through the Solution, they are considered to have collected this PHI as health information custodians (HICs) under PHIPA from the Participants who contributed the PHI to the CDR (and thereby disclosed this PHI as HICs).

This privacy impact assessment (PIA) has been conducted by MD+A Health Solutions on behalf of UHN and considers:

- the full scope of the ConnectingGTA privacy program and safeguards as they pertain to the LPR;
- the business processes within the ConnectingGTA Program that involve PHI; and
- the authority of UHN, ConnectingGTA Participants, and Service Providers to participate in these processes.

MD+A also uses the ten principles of the *CSA Model Code for the Protection of Personal Information* as a framework for evaluating the privacy safeguards and associated program that UHN has put in place to protect the PHI that will be managed within the ConnectingGTA Program and Solution.

The assessment has revealed no significant privacy risks. UHN has defined and is in the process of implementing a robust ConnectingGTA privacy program, including:

- a privacy and security governance structure;
- a full suite of privacy and security policies and procedures; and
- a privacy and security team to develop and implement the privacy program.

The privacy issues and risks that have been identified for UHN are summarized in section 1.1 immediately below. MD+A has noted three key themes pertaining to the identified risks:

- Ten of the seventeen risks identified pertain to components of the ConnectingGTA privacy program that are, at time of writing, incomplete, but that are expected to be completed before the launch of the LPR. In many cases, MD+A has seen substantial evidence that program components are close to completion – for instance, draft documents, or presentations to governance bodies for approval of a policy approach.
- UHN has developed a comprehensive suite of privacy and security policies that are intended to guide its interaction with the ConnectingGTA Participants in conducting such privacy operations as access requests or incident management. The policies and procedures have been clearly written and are explicit about the steps that should be taken to address very specific privacy scenarios.

  However, it is possible that some ConnectingGTA Participants, as well as some patients, may find the policies and procedures too dense or complex to implement in the way that UHN intends.

MD+A has recommended both a review of the policy compliance, as well as patient communications materials to provide clarity to patients about their options regarding how they can exercise their privacy rights in relations to ConnectingGTA.

- Several issues raised in the PIA pertain to UHN's relationship to the ConnectingGTA Service Providers, specifically TELUS (provider of the Front End and Back End Solutions) and eHealth Ontario (hosting services provider). UHN has not yet established a framework for operations or for auditing that will guide its interactions with these Service Providers during the LPR.

  ConnectingGTA Participants will require clarity regarding the activities and PHI-handling practices of the Service Providers if their confidence in the ConnectingGTA privacy and security safeguards is to be maintained. UHN should ensure that it has established a framework for working with and ensuring the privacy and security compliance of the ConnectingGTA Service Providers.

MD+A recommends that UHN develop a risk response plan to address the issues and recommendations that have been identified in this PIA, and follow this plan to mitigate or eliminate the identified risks. UHN has defined a robust privacy and security program, for ConnectingGTA, and the authors of this PIA are confident that the identified issues will be addressed by UHN to support the successful launch of the LPR

UHN should consider a supplementary privacy assessment in the period between the launch of the LPR and prior to full clinical operations.

1.1 Summary of Privacy Findings

Privacy Risk
1. Participation Agreement 4 (for the Viewing Period) is not complete
2. No process defined for PSC to review non-compliance with ConnectingGTA privacy policies
3. No retention and disposal procedures for PHI collected by UHN to support execution of ConnectingGTA privacy procedures
4. Privacy policies may present implementation challenges due to the complexity of the procedures, the scope and the volume of the responsibilities assigned to UHN
5. LPR Privacy and Security Manual and UHN internal procedures have not been completed.
6. No privacy and security operational framework developed for ConnectingGTA Service Providers
7. LPR Privacy and Security Training Plan is not complete
8. Auditing and monitoring criteria for Participants have not been defined in ConnectingGTA Auditing policy

9. No auditing framework has been developed for ConnectingGTA Service Providers and service providers

10. OLIS data that is unmasked in the ConnectingGTA Solution can be viewed by all employees of the Participant that overrode the consent directive on the data.

11. Patient Overview view in the ConnectingGTA Provider Portal may lead to greater than required collection of PHI by end users.

12. UHN has not documented the roles and individuals supporting ConnectingGTA that will have access to PHI

13. UHN has not completed the Data Retention policy for ConnectingGTA

14. Privacy administrators connecting to the privacy/consent portals do not have full two-factor authentication

15. UHN will not know if participating organizations are properly auditing access to PHI made available through ConnectingGTA

16. UHN has not finalized an ongoing audit and assurance program that can provide assurance to Participants that other Participants are meeting Security and Privacy compliance requirements

17. UHN has not developed communications materials to guide interactions with patients during privacy operations

Conclusion

UHN has made significant progress in the development of the ConnectingGTA privacy program, and in the development of the safeguards that support it. Most notable among these safeguards are a robust privacy governance function that provides the ConnectingGTA privacy team and ConnectingGTA stakeholders with appropriate guidance and input, a comprehensive agreements framework, and detailed privacy policies and procedures that will support all ConnectingGTA stakeholders in meeting their specific privacy obligations, and that demonstrate respect for patient privacy rights.

MD+A sees no significant issues with the technical and information security safeguards that have been deployed for the ConnectingGTA Solution. The ConnectingGTA privacy team is well-integrated with the other ConnectingGTA business functions within UHN, such as Training and Adoption and Site Implementation, and also with the ConnectingGTA operational planning function; the privacy team is therefore appropriately supported in developing and implementing the ConnectingGTA privacy program.

MD+A therefore believes that UHN is well-positioned to address the privacy issues that have been identified in this PIA, and, in particular, the gaps in the privacy and security program that UHN intends to address for the LPR. Key areas where UHN should focus its efforts in the period leading up to the launch of the LPR include the completion of a privacy and security training plan for the LPR, an operational framework that will guide UHN and the ConnectingGTA Service Providers in working together to address privacy and security operations, the Privacy and Security Manual for the LPR, and auditing and monitoring criteria to support the Audit policy and procedures.

Recommendations to address the identified issues have been provided; in many cases, the recommendation is simply that UHN completes the identified privacy program component. UHN should nonetheless develop a risk response plan based on the risk register in this PIA, to determine the manner in which it will address the privacy risks.