Shift Health Paradigms
TickiT Security and Privacy Fact Sheet

Question 1: Will personal identifiers or personal health information be collected?

a) TickiT utilizes a single primary patient identifier. The format and use of this identifier is at the discretion of the institution.
b) The TickiT platform allows for a variety of surveys to be created by the client. The information may or may not constitute personal health information depending on the application.

Shift Health Paradigms has made it a priority to follow the Freedom of Information and Privacy Protection Act of BC (FOIPPA) and The Personal Information Protection and Electronic Documents Act of Canada (PIPEDA and PHIPA).

Question 2: Who will have access to the data at each stage of processing and/or analysis?

Answer Summary

The Licensee will designate which Users (healthcare providers, administrators, researchers) have been explicitly granted access to the clinical data. The Licensee may also grant Users limited access to site-specific anonymized data for research purposes. Shift Health Paradigms has a Privacy Policy that restricts access to the data to a single employee through a password protected website. The only reasons for accessing data may be for maintenance or if specifically requested to do so in writing by a Licensee (see below).

Detailed Response

Institutions that use TickiT are represented in the database as accounts. Each account represents an entire institution or a part thereof. While data is stored collectively on a secure server, each account is entirely separate. No data is shared between accounts, nor is it possible for a User of a given account to view, create or modify data from any other account.

Security safeguards are in place at all relevant points to prevent both accidental and deliberate unauthorized access. Industry-standard security provisions including logging, password strength, expiry and failed login attempt limits are also in place.

As a result, access to data is limited to Users who have been granted access to a given account. This access is further divided into assignable roles. In a large institutional setting all these User roles may be filled by different people, while in a smaller clinic, one person may fulfill them all. By assigning different roles the Licensee is capable of selectively granting access to the data.

As stewards of TickiT® and TickiT®'s infrastructure, Shift Health Paradigms has a Privacy Policy that restricts employee's access to the data to performing duties such as server maintenance and backup. Wherever possible, access is limited to bulk data operations that do not involve viewing individual records. At all times, Shift Health Paradigms' Privacy Policy is upheld.

Finally, with explicit consent of both the institution and patient/person, anonymized data is used by Shift Health Paradigms to conduct research into TickiT® and its use. This use is entirely elective and considered opt-in.

Question 3: Describe how the data will be stored and transmitted (e.g. computerized files, hard copy, video recording, audio recording, PDA, and other).

Answer Summary:
TickiT® stores encrypted data on a secured server located in a secure Canadian datacentre. Authorized Users are capable of exporting single and groups of records from their site in a variety of formats.

Detailed Response
Shift Health Paradigms operates a dedicated, secure server that serves as the primary store for data used by TickiT®. Stored data (data at rest) is encrypted using 256-bit AES encryption within the database. All data transfer between the database, TickiT application and/or the end user (data in motion) is additionally secured through a 256-bit AES encrypted SSL tunnel. The server is not used for other tasks beyond storing encrypted TickiT®.

Data backups are encrypted, transmitted via encrypted channels, and stored on a server with highly limited physical access.

Shift Health Paradigms employees who access the server adhere to the Shift Health Paradigms Privacy Policy, and do so only for the development and maintenance of TickiT®.

Authorized Users may export the data in a variety of formats. This includes exporting the results of single surveys in PDF and printed formats, as well as exporting groups of surveys as tabular CSV data.

Question 4: Describe the safeguards in place to protect the confidentiality and security of the data.

Answer Summary
TickiT® uses a variety of security safeguards based on Canada Health Infoway EHR privacy and security requirements.

Detailed Response
TickiT® includes industry-standard security provisions for secure access and login. This includes, but is not limited to:

- HTTP 256-bit AES SSL encryption for all communications
- Data stored in databases (data at rest) are encrypted
- Database backups are encrypted and stored securely
- Account-level sandboxing of all Users to prevent unauthorized access of other institutions' data
- Configurable password expiry requiring users to update passwords periodically
- Configurable access restriction in the form of an IP address whitelist
- Minimum password strength requirements
- Configurable automatic failed login user suspension
- Comprehensive logging of account and data accesses
- All data hosted on a secure, task-dedicated server in a physically secured datacentre.
- Countermeasures to prevent accidental or intentional submission of false survey data.

Question 5: Describe how long the data will be retained and when and how the data will be destroyed.

TickiT® currently retains data for an unlimited time period, up to the lifespan of the parent account. While a long-term archival system is planned, Shift Health Paradigms plans to support optional infinite data retention for its customers.

However, when an account is removed from TickiT® the account's data, as well as all encrypted backups of such data, is also destroyed. For research projects with the need for limited data retention, this can be performed at a predetermined date or upon request.

On the devices used for administering the survey, data is only retained as long as is needed to complete the questionnaire. Upon closing of the application or beginning a new questionnaire, all data is destroyed.

It is important to remember that TickiT® retains no control over data that is exported from the system. It is important to ensure that your institution's Privacy Policies and Practices are appropriate for the data that is being collected.