LEAFSPROUT PRIVACY POLICY

January 16, 2018

1 INTRODUCTION

One of the central functions of Leafsprout's software is secure and responsible stewardship over personal information, including personal health information (PHI). Leafsprout is committed to protecting the privacy and security of the personal information entrusted to us and with which we come into contact, both in the course of our software's performance, and during setup and maintenance activities.

In terms of compliance, Leafsprout handles PHI in accordance with applicable jurisdictional requirements for privacy and security.

This means that in Canada, at the federal level, Leafsprout complies with Canada's Personal Information Protection and Electronic Documents Act ("PIPEDA") and Canada Health Infoway's (CHI's) Privacy & Security Requirements and Considerations for Digital Health Solutions v. 2.0.

Differing legislation exists in individual provinces across Canada. In Ontario, for example, the applicable legislation is Ontario's Freedom of Information and Protection of Privacy Act ("FIPPA"), and Personal Health Information Protection Act ("PHIPA"). In BC, the applicable legislation Leafsprout complies with is the Freedom of Information and Protection of Privacy Act ("FOIPPA").

In the United States Leafsprout complies with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").

This policy outlines Leafsprout's general approach to information privacy. It is structured according to the ten principles outlined within CHI's Privacy & Security Requirements and Considerations for Digital Health Solutions v. 2.0.

As per HIPAA and CHI requirements, Leafsprout makes use of a number of technical, physical and administrative safeguards in order to ensure the security and availability of PHI it stores within its software. These are described in detail within Leafsprout's Security Policy.

NOTE: Leafsprout reserves the right to modify or supplement this Privacy Policy. The revision history may be found in section 1.4 Document Control of this document.

1.1 TERMS AND DEFINITIONS

PI – Personal Information. This information about an identifiable individual includes such details as:

- Personal address, telephone number or email address
- Any identifying number assigned to an individual (i.e., OHIP number, B.C. PHN, SIN)
- Payment history
- Information relating to age, sex, disability, race, citizenship status, marital status, religion, etc.
- Information relating to education, employment, etc.

PHI – Personal Health Information. This includes such information as:

- Physical or mental health of the individual
- Eligibility for health care
- Reason for receiving health care
- Alternate decision maker
- Clinical information about the individual being referred for service.

Security and Compliance Officer – SCO – see section 2.1 Accountable Person

Health Information Custodian, Custodian – This is an organization or person that delivers healthcare services and has custody or control of Personal Health Information (PHI) as a result of the work it does. Hospitals, radiological practices and physicians are examples of Custodians. The Custodian has the right to deal with the PHI and create records, as well as the responsibility to maintain the confidentiality and security of the PHI. Leafsprout is not a Custodian, but rather provides records management services to Custodians.

Cortex, Cortex Archive – Leafsprout's records-management and sharing service

HIPAA – Health Insurance Portability and Accountability Act of 1996. HIPAA is a piece of US legislation that sets out standards for electronic exchange, privacy and security of health information. HIPAA requirements apply to Covered Entities and their Business Associates who operate in the USA.

HIPAA **Covered Entities** are:

- Health plans
- Healthcare clearinghouses
- Healthcare providers who transmit health information in electronic format in connection with any of the standard transactions governed by HIPAA (e.g., claims, benefit eligibility inquiries, referral authorization requests). HICs, as defined above, fit into this category of Covered Entity.

A HIPAA **Business Associate** is an entity (other than an employee of a Covered Entity) that provides services to Covered Entities that involves the use or disclosure of individually-identifiable health information. Business Associates have obligations under HIPAA related to privacy and security of PHI.

As a provider of cloud archival of medical records, Leafsprout stores PHI, thereby acting as a Business Associate to Covered Entities. As a Business Associate, Leafsprout is obliged to abide by US HIPAA regulations.

1.2 SCOPE

This policy applies to Cortex Archive, and to all Leafsprout personnel and third party service providers Leafsprout has retained to support the delivery of Cortex Archive services. This privacy policy should be read in conjunction with the related policies, standards and procedures that are part of our comprehensive privacy and security program.

1.3 RELATED AND REFERENCED DOCUMENTS

- Canada's Personal Information Protection and Electronic Documents Act ("PIPEDA").
- Canada Health Infoway's Privacy & Security Requirements and Considerations for Digital Health Solutions v. 2.0.
- Ontario's Freedom of Information and Protection of Privacy Act, 1990 ("FIPPA")
- Ontario's Personal Health Information Protection Act, 2004 ("PHIPA")
- British Columbia's Freedom of Information and Protection of Privacy Act, 1996 ("FOIPPA")
- USA's Health Insurance Portability and Accountability Act of 1996
- Leafsprout Security Policy

1.4 DOCUMENT CONTROL

Document Location	This document can be found in Leafsprout's document control system at: Leafsprout/Methodology/LS Privacy Policy.docx
Document Sensitivity	Publicly-available

Revision and Approval History

Author	Approver(s), Title(s)	Version	Date Approved	Summary of Changes
Elizabeth Stark	Cezary Klimczak, CEO	1.1	Jan 15, 2018	Initial revision

2 PRINCIPLE I: ACCOUNTABILITY

2.1 ACCOUNTABLE PERSON

Leafsprout's Security and Compliance Officer (SCO) is accountable for facilitating Leafsprout's compliance with privacy principles, and in particular this policy. Additionally, other Leafsprout personnel may be responsible for acting on behalf of the SCO from time to time. The SCO oversees the Privacy Program and reports directly to Leafsprout's Chief Executive Officer.

Complaints, questions and feedback about Leafsprout's privacy practices may be directed to the SCO.

Leafsprout's Security and Compliance Officer is Elizabeth Stark. Contact information: Leafsprout Technologies Inc. 5915 Airport Road, Suite 915, L4V 1T1 Tel: 647-723-2028, elizabeth.stark@leafsprout.com.

2.2 THIRD-PARTY AGREEMENTS

From time to time Leafsprout deals with other entities (companies and contractors) that provide services to Leafsprout that could potentially involve handling or having access to individually-identifiable health information. Leafsprout ensures that there are agreements in place with any such third-party entities obliging these entities to protect the PI and PHI held within Leafsprout's systems. These agreements include the following information:

- Purpose for which the third party is being given access to the PHI
- A listing or description of the PHI to which the third party will have access
- The purposes for which the PHI may be used or disclosed by the third party
- Obligations of the third party upon termination of the agreement

2.3 PRIVACY POLICY

Leafsprout is committed to respecting personal privacy, safeguarding confidential information, and ensuring the security of information in our care. Leafsprout meets this commitment through our comprehensive Privacy Program. Key components of Leafsprout's Privacy Program include:

- Procedures for the protection of PI and PHI
- Procedures for handling complaints & inquiries
- Training on procedures, policies and practices
- Threat and Risk Assessments

Leafsprout offers public accountability and transparency by making this policy freely available to the general public.

3 PRINCIPLE II: IDENTIFYING PURPOSES

3.1 PURPOSES FOR COLLECTION, USE & DISCLOSURE

Leafsprout stores Personal Information (PI) and Personal Health Information (PHI) on the behalf of Health Information Custodians (Custodians), e.g., radiology practices, in the course of providing a medical record archival and sharing service. Such collected information about users and/or patients may be used for one or more of the following purposes:

- Providing archival and/or sharing services to users
- Performing patient matching as required
- Occasionally, PHI may be accessed incidentally in the course of providing support, maintenance, or investigation of any incident or breach
- Monitoring Cortex
- Providing a view of the medical records and information stored
- Performing analytics on stored data
- De-identifying stored data such that it no longer contains PHI
- Reporting on aggregated data
- Reporting on aggregated usage statistics to users, sponsors, investors, or others, in order to further the intent of Cortex, for process improvement, and to help evaluate the effectiveness of Cortex
- Contacting users or patients regarding requests for access to, or correction of, Personal Information (PI)
- Contacting users for feedback and surveying needs regarding Cortex
- Promoting new or revised services to users
- Promoting use of Cortex
- As legally required by law enforcement or national security agencies

Leafsprout manages and stores PHI collected and entered by a Health Information Custodian (Custodian). The Custodian is responsible for providing notice to their patients regarding consent and purpose for collecting PHI, which may be beyond Leafsprout's purposes.

3.2 LIMITATION OF COLLECTION, USE & DISCLOSURE

Leafsprout will only use PHI collected and stored by Leafsprout for the purposes described in this document. Leafsprout will only disclose this PHI in accordance with the directions of the Custodian on whose behalf the PHI is collected and stored, or as required by law.

4 PRINCIPLE III: CONSENT

The principle of consent means that the knowledge and consent of the individual are required for the collection, use or disclosure of PI or PHI, except when inappropriate.

4.1 DETERMINING / GATHERING CONSENT

Leafsprout does not collect PI or PHI directly from patients, but rather provides storage and sharing services for the healthcare records collected by a Health Information Custodian (Custodian). Determining or gathering knowledgeable consent is the obligation of the Custodian collecting the PHI. Informing the patient/person of the implications of consent decisions is similarly the obligation of the Custodian.

4.2 MECHANISMS FOR STORING AND ACTING ON CONSENT DIRECTIVES

Leafsprout provides mechanisms to the Custodian for storing consent, associating consent with PHI, and appropriately acting on consent directives (including revocation of consent). The use of those mechanisms (or other mechanisms) to record, associate, and act on consent is the obligation of the Custodian. The Custodian is similarly responsible for recording the identity of any substitute decision-makers.

4.3 LOGGING CONSENT-RELATED ACTIONS

Leafsprout logs any consent-related actions undertaken within Cortex.

5 PRINCIPLE IV: LIMITING COLLECTION

The principle of limiting collection means that the collection of PI and PHI shall be limited to that which is necessary for the purposes identified, and that the information shall be collected by fair and lawful means. When interacting directly with the patient, Leafsprout will collect only the PI and PHI that we require to achieve the purposes identified in this document, unless we receive consent from the individual to collect it for another purpose. When acting as a service provider to a Health Information Custodian, Leafsprout does not collect information directly from patients; Leafsprout rather provides storage and sharing services for the information collected by the Custodian.

6 PRINCIPLE V: LIMITING USE, DISCLOSURE AND RETENTION

Leafsprout shall not use or disclose PHI for purposes other than those identified within this document, except with the consent of the individual or as required by law.

6.1 LOG ACCESS, MODIFICATION AND DISCLOSURE

All actions undertaken within Cortex involving stored PHI, including all accesses, modifications, and electronic disclosures, are logged in an audit repository, which is a piece of software incorporated into Cortex Archive that stores detailed information pertaining to events that occur within Cortex.

6.2 NOTIFY PATIENTS/PERSONS OF INAPPROPRIATE ACCESS, USE OR DISCLOSURE

Leafsprout monitors Cortex as outlined within the Leafsprout Security Policy.

In the event that an inappropriate access, use or disclosure is detected, Leafsprout will notify the affected Leafsprout customer(s) without unreasonable delay, and in no case later than 60 days after discovery.

6.3 RETAIN RECORDS

Leafsprout retains records containing PHI in Cortex on behalf of our customers for time periods that are in line with local and/or user-requested requirements, subject to Leafsprout's commercial agreements with the users in question (i.e., Leafsprout does not retain PHI stored in Cortex beyond the expiry of its contractual relationship with an entity).

7 PRINCIPLE VI: ACCURACY

The principle of accuracy means that PHI must be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used. Furthermore, the patient or person must be accurately identified when accessing or modifying their PHI.

Leafsprout does not collect PHI directly from patients, but rather provides storage and sharing services for the healthcare records collected by a Health Information Custodian (Custodian). The responsibility for ensuring accuracy of clinical information collected rests with the Custodian, and any corrections or changes to that information must be made only by the Custodian who has custody of the information.

In order to assist with the task of maintaining accurate records and linking them with the appropriate patients/people when accessing or modifying PHI, Leafsprout makes use of a Master Patient Index (MPI) incorporated into Cortex Archive. An MPI stores demographic information and may be used to coordinate the multiple patient identifiers that may refer to the same person by the various medical information systems involved in that person's care.

8 PRINCIPLE VII: SAFEGUARDS

PHI kept within Cortex is safeguarded by administrative, technical, and physical means appropriate to the sensitivity of that information. These safeguards are designed to protect information in all formats against loss or theft, as well as against unauthorized access, disclosure, copying, and use or modification by inappropriate parties. These safeguards include measures such as:

- Multi-level encryption mechanisms
- Access controls
- Monitoring
- Threat and risk assessments
- Audit logging

A detailed description of security measures in place can be found in the Leafsprout Security Policy. In addition to the safeguards outlined within the Leafsprout Security Policy, Leafsprout has put in place the following:

A Threat and Risk Assessment is completed by Leafsprout to ensure all privacy risk issues are identified. Leafsprout creates plans to address the findings of Threat and Risk Assessments. A summary of this assessment is available. A detailed security safeguard description is found in the Leafsprout Security Policy, which discusses practices such as use of complex passwords, firewalls, encryption of data, Privacy Incident & Breach Management, and access based on least privilege.

8.1 DENOTE PATIENTS/PERSONS AT ELEVATED RISK (E.G., VIPS)

Leafsprout provides the capability within Cortex for Custodians to mark specific patients as being at elevated security risk (e.g., VIP patients) and then apply specified rulesets to these patients.

8.2 TRAINING USERS AND RAISING PRIVACY AWARENESS

All Leafsprout personnel and third-party personnel who have access to PI and PHI managed by Leafsprout undergo privacy and security training on our privacy- and security-related procedures (see Leafsprout Security Policy).

9 PRINCIPLE VIII: OPENNESS

The principle of openness means that an organization shall inform individuals about that organization's approach to managing their PHI. Leafsprout posts our privacy program overview on the Cortex website. Additional information is available upon request.

10 PRINCIPLE IX: INDIVIDUAL ACCESS

Leafsprout does not collect PI and PHI directly from individuals, but rather provides storage and sharing services to a Health Information Custodian (Custodian) for the information collected by that Custodian. Since the commercial arrangements that govern the transfer of PI and PHI are in place with the Custodian, all requests for access to PI and PHI in Leafsprout's care, requests for amendment of PI and PHI, challenges to accuracy and completeness of PI and PHI, should be routed through that Custodian. Notifications and records regarding challenges to accuracy and completeness are the responsibility of the Health Information Custodian.

Upon request, Leafsprout will provide the Custodian with an electronic copy of that Custodian's records for a person/patient whose PI/PHI is managed by Leafsprout. Leafsprout commits to do this in a timely manner, and no later than 30 days after receiving the request.

11 PRINCIPLE X: CHALLENGING COMPLIANCE

Anyone wishing to challenge Leafsprout's compliance with our Privacy Policy may do so in writing to the attention of our SCO (see section 2.1 Accountable Person).

The Security and Compliance Officer is responsible for investigating all privacy complaints, informing complainants and inquirers of our complaint procedures, and treating all complaints as confidential.

If a complaint is found to be justified, Leafsprout will take the appropriate measures, which may include changing company policies and practices.

If the sender provides contact information, Leafsprout will:

- acknowledge the complaint, question or feedback within five (5) business days of receipt and provide information about any relevant internal and external complaint mechanisms;
- respond to the sender's question, feedback or complaint within thirty (30) business days of receipt; and
- notify the sender of the expected timeframe for response if a delay is anticipated.