Avaya Privacy Laws Compliance Guide: *Personal Health Information Protection Act* (Ontario)

At Avaya, security and privacy are of primary importance. Avaya is committed to building on its experience through leading edge technology solutions that enhance privacy, as well as cloud solutions that aim to deliver both security and privacy.

This includes complying with local and regional privacy and security regulations and giving Avaya's customers the tools they need to be compliant with Canadian data protection regulations, including Ontario's *Personal Health Information Protection Act* (PHIPA).

Avaya's commitment to privacy and security extends to implementing organization-wide policies and practices as well as physical and technical security measures aimed at promoting security and privacy of customer data, including personal health information (PHI). As part of Avaya's Trust Center, Avaya publishes additional information about our security practices, including information about Avaya's certifications and accreditations. While Avaya prohibits the use of its services to breach privacy laws, Avaya cannot prevent all abuses of its services. Customers are responsible for their compliance with privacy laws and for ensuring their staff comply with privacy laws.

This document describes Avaya's privacy and security practices as they relate to PHI and how Avaya can help Ontario customers who act as health information custodians comply with Ontario health information privacy laws.

1. What is PHIPA?

PHIPA is Ontario's health-specific privacy legislation. Through its comprehensive privacy framework, it regulates all collection, use and disclosure of individuals' PHI by health information custodians, and individuals and organizations that receive PHI from custodians. Under PHIPA, PHI includes any identifying information relating to an individual's physical or mental health, or the provision of healthcare to the individual (including their health number).

2. How Avaya Helps Customers Acting as Health Information Custodians Meet Their Obligations

Avaya has implemented privacy practices and technical and physical security measures to protect customer data, including PHI.

(a) Avaya's Privacy Practices to Help Health Information Custodians Meet Their Obligations

Avaya's privacy practices include:

- ensuring that Avaya complies with PHIPA and its regulations when it collects, uses and discloses PHI.

- only using and disclosing the PHI to which it has access in the course of providing services to the customer in accordance with PHIPA and the instructions of the customer, and informing customers of when it cannot comply with this practice.

- ensuring its employees or any person acting on its behalf are unable to access PHI unless they agree to comply with the same restrictions Avaya is subject to under PHIPA.

- assisting customers in complying with requirements to inform and explain to individuals how their PHI is collected, used or disclosed.

- enabling customers to respond to requests from individuals for access to or correction of PHI.

- following instructions of customers to return, dispose of or store PHI in a secure manner when the services are terminated.

- following instructions of customers to provide assistance in keeping PHI accurate and up-to-date.

- complying with data security breach notification requirements and notifying customers of any security breach of PHI (including unauthorized access) at the first reasonable opportunity and as required under its contracts with customers.

- assisting customers in complying with data security breach notification obligations, including in the event that personal health information is stolen, lost or accessed by an unauthorized person.

- committing to help customers meet their compliance requirements, including in relation to information practices and electronic audit logs under PHIPA.

- storing PHI in jurisdictions outside of Ontario only as permitted by PHIPA. Upon request, Avaya can provide product-specific information regarding storage location.

(b) Avaya's Physical and Technical Measures to Help Health Information Custodians Meet Their Obligations

Avaya will protect PHI by employing procedures to meet the privacy and security requirements of PHIPA and its regulations. Avaya's administrative, physical and technical measures to promote data privacy and security include:

- restricting physical access to customer data processing equipment, including by:
    - an electronic access control system,
    - 24/7 video recording of physical facilities,
    - intrusion detection or engaging on-premises security officers, and
    - restricting access to various zones at its premises based on roles and periodically revalidating access.

- restricting logical access to customer data and processing equipment, including through:
    - unique user IDs for access with formal authorization processes and unique complex passwords,

- role-based access, least-privileged access and need-to-know only access,
- access logs,
- multi-factor authentication of Avaya's VPN for remote access,
- encrypted endpoints,
- centrally monitored and updated anti-virus programs and regular anti-virus scans,
- secure deletion and/or disposal of data, and
- secure storage of backup media and testing backups.

- using secure communication channels and logging, including:
  - using VPN with a multi-factor authentication for remote access,
  - using firewalls with stateful inspection, default denial access rules, role-based and least-privileged access on a "need to know" basis, logging and alerting of access, an annual review, and
  - using encrypted email if this has been enabled by the customer, using TLS.

(c) Avaya's Data Breach Incident Response Team and Privacy Law Advisors

Avaya also has a Data Breach Incident Response Team (DBIRT) that provides leadership in the event of a data breach. This is a cross-functional team established with the specific purpose of responding to actual and suspected data breaches. The DBIRT operates according to Avaya's Data Breach Incident Response Plan, which provides a well-defined, organized, repeatable and documentable approach to efficiently and effectively respond to data breaches to minimize their impact on Avaya or third parties, including Avaya's customers.

Avaya also receives advice from a leading Canadian law firm on privacy law compliance.

3. Who to Contact about Avaya's Security and Privacy Practices

For any questions about Avaya's security and privacy practices, including in relation to health information-related practices, please contact:

Avaya Global Privacy Office

Email: dataprivacy@avaya.com