RingCentral

PHIPA Compliance Guide

May 2024

RingCentral and the Ontario Personal Health Information Act (PHIPA)

RingCentral takes all customers' data privacy and security seriously. This includes formal compliance with applicable local and regional laws and regulations. As a leading global communications and collaboration cloud service provider, RingCentral's platform services are designed to help our customers meet their compliance obligations under the Ontario Personal Health Information Act (PHIPA).

In this whitepaper, we provide information to help customers understand Ontario's PHIPA and how it fits with RingCentral services. Customers that are subject to PHIPA are responsible for complying with its requirements. Since there is no officially recognized certification for PHIPA such as SOC, PCI, or ISO, here we offer our customers information regarding the policies, processes, and controls established and operated by RingCentral.

Background	Healthcare data is protected by a number of privacy laws and regulations in Canada. In Canada the collection, use and disclosure of personal information within the commercial sector is regulated by federal privacy legislation—the Personal Information Protection and Electronic Documents Act (PIPEDA). PHIPA is Ontario's health-specific privacy legislation, which came into force on November 1, 2004. PHIPA governs the manner in which personal health information may be collected, used and disclosed within the health sector.
How RingCentral Helps Customers Meet Their Needs Under PHIPA	We implement numerous measures to protect our customers' data, but our services are not designed to recognize or classify Personal Health Information ("PHI"). RingCentral does not access customer content to determine whether it contains PHI. Whether content (such as voicemails or call recordings) includes PHI or not, RingCentral applies the same processes and safeguards set forth in this whitepaper. Customers are responsible for using our services in compliance with the legal requirements that apply to them and they should consult their own legal advisors to understand the applicable privacy laws. The following information in this whitepaper explains how we support our customers in protecting PHI.
Privacy Governance	To comply with PHIPA, the Office of the Information Commissioner of Canada recommends that organizations adopt various measures to safeguard PHI, one such measure includes implementing privacy governance and designating a reachable privacy contact. RingCentral has established a Privacy Office, led by the Chief Privacy Officer, which is responsible for privacy governance, establishes the company policies and oversees the

	key privacy processes at RingCentral. The Privacy Office can be reached at privacy@ringcentral.com.
Openness	RingCentral is fully transparent about the ways it handles customer data. Information regarding RingCentral's policies and processes relating to the management of personal information is listed in our Privacy Notice. The Privacy Notice also includes information on how to contact RingCentral's Privacy Office.
Security	PHIPA requires organizations to apply technical controls to ensure the security of PHI in their custody or control. RingCentral's commitment to data security is demonstrated through the adoption of numerous security measures. These measures have been independently verified by outside parties. RingCentral regularly undergoes SOC 2, ISO 27001, ISO 27017, ISO 27018, and HITRUST audits. Current customers can access these audit reports directly through our Trust Portal. Our security measures include: • **Information Security Management**, including a written security program, security policy management, and risk management. • **Independent Security Assessments**, including SOC 2 Type II and IES/ISO 27001. • **Human Resource Security**, including background checks, training, data loss prevention, and subcontractors' due diligence. • **Physical Security**, including restricted access to secure areas, documented access authorization process, and security of its data centers. • **Logical Security**, including user identification and authentication, user authorization and access control. • **Telecommunication and Network Security**, including network management, network segmentation, and network vulnerability scanning. • **Operations Security**, including asset management, configuration management, malicious code protection, vulnerability and security patching, logging and monitoring. • **Data Classification and Handling**, including encryption and destruction of data.

Access & Correction Rights	PHIPA provides individuals with the right to access, correct, and in some circumstances, ask for the removal or modification of their data. RingCentral provides tools that allow customers to handle any individual access requests—customers' account administrators can easily manage these in the Service Web, which is the Admin Portal for RingCentral's Services. For any further help with such requests, customers can also contact the RingCentral support team through the RingCentral Data Subject Request Portal. Individuals may submit a request directly to RingCentral, which in such event shall promptly direct the individual to contact the customer.
Data Breach Management	RingCentral's incident response capability is designed to comply with statutory and regulatory obligations governing incident response. As such, RingCentral maintains an incident response capability to respond to events potentially impacting the confidentiality, integrity and/or availability of Services and/or data. Also, RingCentral has a documented incident response plan based on industry best practices and a process for evidence handling that safeguards the integrity of evidence collected, including allowing detection of unauthorized access. Furthermore, RingCentral will take appropriate steps and measures to comply with statutory and regulatory obligations governing incident response. When RingCentral learns of or discovers a security event which impacts PHI, RingCentral will notify customers without undue delay and will take commercially reasonable steps to isolate, mitigate, and/or remediate such an event.

RingCentral, Inc. 20 Davis Drive, Belmont, CA 94002. ringcentral.com

693725169 05/2024