Acronis

WHITE PAPER

Personal Health Information Protection Act (Ontario)

Introduction

This document and any other related documentation on compliance produced by Acronis does not offer legal advice. Customers are solely responsible for evaluating and fulfilling their own legal and compliance obligations under PHIPA, as well as for using Acronis Cyber Cloud services in an appropriate manner under PHIPA requirements. All specific service functions can be found via Support documentation.

Respecting privacy and protecting personal data is one of the main goals in offering cloud technologies, especially if we speak about sensitive data. Today's cloud technologies offer a wide range of solutions that medical organizations can use to easily and securely process personal health information. Knowing that these tools meet the strict regulatory requirements of the health care industry is not as easy, though.

PHIPA and OIPC requirements

Based on PHIPA requirements and Office of the Information and Privacy Commissioner of Ontario (OIPC) guidance, organizations should implement a wide range of security measures to ensure personal data remains protected. These include, among others:

- Implementing privacy governance practices, such as designating a publicly reachable privacy contact and publicizing the organization's privacy policy related to the collection, use and disclosure of personal health information.
- Implementing administrative, physical and technical safeguards for the privacy of personal health information.
- Creating information security training for staff to ensure the use of compliance practices when working with personal data.

Personal Health Information Protection Act (PHIPA)

PHIPA's main goal is to provide standards related to protection of personal health information across the health sector and to ensure individuals greater control in terms of how their personal health information is collected, used and disclosed.

PHIPA came into force 1 November 2004 and was amended significantly on 1 October 2020, when the Electronic Health Record part was adopted.

While our customer is a health information custodian (HIC), Acronis is an electronic service provider (ESP), a company **which supplies services** that enable a custodian to collect, use, modify, disclose, retain or dispose of personal health information **electronically**.

Acronis can act as an agent, which means that Acronis can be **authorized by a custodian** to perform services or activities in respect to personal health information **on the custodian's behalf and for the purposes of that custodian.**

Acronis does not control how the customer uses cloud services for personal health information processing, or the customer's security management process. Customers should conduct their own risk analysis, implement a risk management plan and a sanctions policy, and conduct an information system activity review. As part of the security management process, customers should consider how Acronis Cyber Cloud services or specific Acronis products fit within their policies and procedures to prevent, detect, contain and correct security violations.

We use the shared responsibilities model presented below to ensure fulfillment of PHIPA obligations. If you are a subject to PHIPA, please notify us at data-protection-office@acronis.com with the subject "PHIPA instructions" before you start using Acronis services.

NOTE: For more information on what security measures Acronis applies, please check:
https://www.acronis.com/en-us/security/cloud/data-processing-terms/

How Acronis protects your data and what you can do to ensure data privacy:

Privacy and security governance practices:

Acronis	Customer
Acronis has implemented a set of policies and procedures to define purposes of collection of personal data, and ways of processing and sharing personal data. The Acronis Privacy Statement describes what information Acronis collects; why Acronis needs it; how Acronis shares information, and customers' data subject rights, retention period, etc. To respect its customers privacy rights, Acronis has assigned a data protection officer. You can send a request to Acronis data protection team at data-protection-office@acronis.com if you have any questions or concerns.	A health information custodian remains responsible for the personal health information that is collected, used, disclosed and retained or disposed of by an agent. If you are subject to PHIPA and have any specific obligations related to processing personal health information, please notify us at data-protection-office@acronis.com with a subject "PHIPA instructions."

Administrative safeguards:

Acronis	Customer
Acronis maintains an information security management system based on the ISO 27001 standard. Acronis has obtained two certifications which extend general ISO 27001 requirements to: Information security controls for cloud services (ISO 27017:2015), and protection of personally identifiable information (PII) in the cloud (ISO 27018:2019). Acronis has pursued obtaining the System and Organization Controls 2 (SOC 2®) report for service organizations. The standard applies trust services criteria and requirements for organizations, which manage customers' data. Acronis obtained SOC 2 Type 2 compliance for the services we provide through the Acronis Cyber Cloud platform.Acronis is implementing controls for preserving the security, availability, confidentiality and processing integrity of the information.	It is a customer's responsibility to conduct an internal risk assessment before starting to use Acronis services. You can download ISO 27001:2013, ISO 27017:2015 and ISO 27018:2019 certifications from the Acronis Trust Center. If you want to obtain our current SOC 2 report, please check the Acronis Trust Center or contact your account manager or support team. You can rely on Acronis compliance certificates and reports. In addition to what's mentioned above, you can download our STAR Level 1 self-assessment.
All Acronis personnel are obligated to comply with Acronis' confidentiality, business ethics and code of conduct policies. Acronis conducts appropriate background checks on candidates, every Acronis employee is required to sign a nondisclosure agreement (NDA), and user access control is strictly maintained. Acronis **does not** control how the customer uses cloud services for personal health information processing. All customer data is classified as the highest critical asset, in accordance with Acronis' internal data classification policy.	You should inform Acronis in advance about processing personal health information and configure and use the product in accordance with official documentation and applicable contractual terms.

Technical safeguards:

Acronis	Customer
In accordance with Acronis' internal policies and procedures, the following evaluation activities are provided: ▪ Regular penetration tests, performed by an independent third party. ▪ Vulnerability assessment. Acronis performs regular vulnerability scans of internal and data center infrastructure.	Acronis highly recommends their customers to conduct regular vulnerability scans to ensure the proper functioning and security of data. You can check instructions for how to enable vulnerability scanning at Technical documentation and / or Acronis Cyber Protect Cloud.
Internal access control procedures detect and prevent unauthorized access to Acronis systems and information resources. When providing access, Acronis uses centralized access control systems with secure mechanisms and authentication protocols (e.g., LDAP, Kerberos, and SSH certificates), unique user IDs, strong passwords, two-factor authentication mechanisms, automatic logoff and limited control access lists, minimizing the likelihood of unauthorized access. Acronis Cyber Cloud services enforce in-transit and at-rest data encryption by default, with reliable cryptographic algorithms and protocols (e.g., TLS, AES).	Acronis products also provide access control mechanisms such as unique user IDs, password complexity, automatic logoff, session termination, encryption and 2FA. As a part of using Acronis products in a PHIPA-compliant way data must be encrypted on the customer's side. You can find more information about access control mechanisms and encryption at Acronis product documentation.
Acronis uses procedural, software and hardware mechanisms to audit activities at the backend of Acronis Cyber Cloud services. Acronis Cyber Cloud services can provide a chronological record of the following events: ▪ Operations performed by users in the management portal or service. ▪ System messages (e.g., warnings, errors, etc.). The log shows events in the tenant in which customers are currently operating, as well as its child tenants. The default retention period of the logs is not less than 180 days.	You may export Audit log data to SIEM platform and keep it as long as required. We highly recommend that you review logs in accordance with your internal procedures to promptly detect and identify suspicious incidents..
High availability and redundant infrastructures are designed to minimize associated risks and eliminate single points of failure. Acronis follows the approach of need plus two (N+2) for greater redundancy across all hardware layers of its infrastructure. This ensures that if there is a failure in a hardware-layer component, it does not affect either the Acronis critical infrastructure or Acronis customers. This redundant infrastructure enables Acronis to fulfill most types of preventive and maintenance activities without service interruption.	Acronis highly recommends enabling additional services to ensure data integrity such as disaster recovery.

Physical safeguards:

Acronis	Customer
Acronis hosts customers' data within trusted data centers, which employ physical security controls (access control, intruder alarms, CCTV, etc.) to restrict unauthorized physical access and maintain data safety. Only authorized personnel have access to data centers and hardware.	PHIPA does not prohibit storing data outside of Ontario and Canada. Acronis operates two data centers in Canada, one in Toronto and another in Vancouver. You have a right to choose the data center to store your data depending on your own needs and obligations.
Acronis uses a software-defined infrastructure and storage solution, which utilizes a proprietary erasure-coding algorithm which enables the reliable removal of data when required. In the case of hardware decommissioning, Acronis physically destroys broken drives and equipment, according to NIST SP 800-88.	Using encryption as a machine property, you can employ cryptoerasure in line with NIST SP 800-88 by securely removing the decryption keys.

Security training program:

Acronis	Customer
Acronis conducts security training for its personnel, as well as information security training and data protection training, which includes specifics of processing health data. These are obligatory for every employee as a part of their onboarding, and thereafter on an annual basis.	Customers should maintain their own security awareness and training program, including information about how to use and configure Acronis Cyber Cloud services to comply with their internal policies and PHIPA requirements (e.g., how to monitor login attempts and other logs generated by their systems).

Collection, use and disclosure of data:

Acronis	Customer
Acronis is not aware of the content of data our customers store and process this data on behalf of its customers in accordance with provided instructions and contracts.	It is our customers' responsibility to ensure authorized collection, use and disclosure of the PHI they store using our solutions.
Customer's content data resides within their chosen data center (or region). Acronis may provide support to its customers which can include remote access for troubleshooting. **Acronis does not collect, use or disclose PHI viewed during such support sessions for its own purposes.** Acronis ensures its vendors comply with all Acronis requirements related to the treatment personal information and personal health information by signing confidential obligations and / or by including security provisions in agreements.	You can choose a preferred Data Center to store your data. Please note that with PHIPA, transmitting your data to Acronis should be treated as "use" of data, while all applicable restrictions related to collection and disclosure of PHI are our customers' responsibility. If you require confirmation that your data is stored in a dedicated data center, please request this from your account manager or support team. It is your responsibility to ensure no personal health information is visible during remote support sessions.

Retention periods and breach notification:

Acronis	Customer
Acronis stores your data no longer than is necessary to fulfill its obligations. To protect data from accidental deletion and due to specify platform functionality Acronis may retain data up to 30 days.	You can export your data and backups from within the platform to have the most updated version and delete your account if you do not want to store personal health information with Acronis anymore.
Acronis notification rules are described in our Customer Data Processing Agreement (not later than 48 hours after Acronis has a reasonable degree of certainty that a personal data breach has occurred).	You can request a DPA from your account manager or Support Team. If you have any restrictions or specific requirements related to breach notifications, please notify us at data-protection-office@acronis.com with the subject “PHIPA instructions."

Data subjects rights:

Acronis	Customer
Unless prohibited by applicable law, Acronis will notify a customer when Acronis receives a valid request, complaint, demand, legal process or order related to customer personal information from a data subject, government authority or other third party (“Request”). Acronis represents that it has and will maintain appropriate measures to assist customers in responding to Requests, including processes to authenticate, record, investigate and resolve Requests. Acronis will not respond to a Request unless authorized to do so in writing by customers or if Acronis believes its response is required by applicable law.	We highly recommend additional mechanisms to be configured by using specific Acronis Cyber Cloud services. Please check Acronis product documentation. These mechanisms can protect electronic PHI from improper alteration or destruction. You can contact Acronis at data-protection-office@acronis.com with the subject “PHIPA Data access / correction request” and provide terms for response in a case you need Acronis assistance with Requests.

Right to complain:

A person who has reasonable grounds to believe that another person has contravened or is about to contravene a provision of PHIPA or its regulations may make a complaint to the commissioner.
Information and Privacy Commissioner of Ontario is a supervisory organization. For related procedures, please check https://www.ipc.on.ca/health-organizations/phipa-complaint-process/.