AlayaCare's SaaS System Solution and Safeguards

AlayaCare, Inc. ("AlayaCare") is a Software-as-a-Service (SaaS) company with its corporate headquarters in Toronto, Ontario, and product and engineering capabilities in Montreal, Quebec. AlayaCare develops and provides home care and home health agencies with an end-to-end software solution that connects care workers, management, external stakeholders, and home health agencies to enable better care. Through the web-based SaaS solution, home health agencies can record and share personal health information (PHI) about their patients. PHI is any information that can identify an individual and relates to the health care services they receive. This includes, but is not limited to, the individual's name, address, telephone number, health card number, health care provider's name, and examination results. AlayaCare is committed to protecting this PHI consistent with the requirements of applicable law, including the Personal Health Information Protection Act of 2004 and its implementing regulation at OR 329/04 (collectively, "PHIPA").

Plain-Language Description of the Software

AlayaCare provides a modern home health software platform to providers in Ontario, in which AlayaCare acts as a health information network provider (HINP) under PHIPA. This software supports the bi-directional sharing of certain health information, including PHI, between home care agencies and third-party actors in Ontario regarding their shared patients. The purpose of this information sharing is to facilitate optimal treatment of the patient through improved care collaboration.

AlayaCare will only share PHI with the following:

- Service providers that facilitate our Services or help us improve the Services (for example, data storage, web analytics, mapping providers and maintenance service providers) have access to Personal Information only for purposes of performing these tasks on our behalf.
- Law enforcement officials, governmental agencies, or other legal authorities (i) in response to their request; (ii) when permitted or required by law; (iii) to establish our compliance with applicable laws, rules, regulations, or guidelines; or (iv) or to establish, protect, or exercise our legal rights or defend against legal claims or demands.
- Any other person whom you authorize the disclosure to pursuant your usage of the Applications.
- We may also share with third parties certain aggregated non-personal information about our users.

Privacy Overview

AlayaCare follows industry best practices and applicable legal requirements (e.g., PHIPA) in connection with information privacy. AlayaCare's Chief Legal Officer and Privacy Officer play active roles in building and managing privacy compliance within AlayaCare's solutions.

AlayaCare maintains a comprehensive information privacy program that addresses AlayaCare's various privacy obligations in accordance with applicable laws. AlayaCare's privacy program includes a PHIPA Privacy Policy that addresses AlayaCare's privacy obligations imposed by PHIPA specific to the protection of PHI of patients in Ontario as both a HINP and as an electronic service provider. For additional information about AlayaCare's PHIPA Privacy Policy, you may contact AlayaCare's Privacy Officer at the address listed at the end of this document.

AlayaCare's customers in Ontario are 'health information custodians' (as defined in PHIPA). AlayaCare is not itself a health information custodian. In its delivery of the Software, AlayaCare is acting as a HINP and is, therefore, subject to the obligations imposed by PHIPA upon HINPs. AlayaCare is not an 'agent' (as defined in PHIPA) of a health information custodian in connection with its delivery of the Software. However, to the extent that AlayaCare performs any separate services as an agent to a health information custodian, AlayaCare and that custodian will identify the specific scope of those agent services in the contract(s) between them and, within that context only, AlayaCare will take on the privacy obligations imposed by PHIPA upon agents.

AlayaCare has no direct relationship or interactions with individual subjects of PHI. Instead, AlayaCare relies upon its health information custodian customers' representations to AlayaCare regarding the consent status of a given individual. Accordingly, to the extent that a custodian utilizes the Software to access, use, disclose, or otherwise interact with the PHI of a given individual, it is the sole responsibility of that custodian to ensure that it has obtained any consents necessary to do so.

Description of Safeguards

AlayaCare monitors, reviews, and updates its applicable policies and practices to ensure the security of the PHI processed and transmitted over its software platform and solutions. AlayaCare uses a variety of administrative, physical, and technical safeguards to protect the PHI that it is entrusted with from unauthorized access, use, copying, modification, and disclosure. The following is a summarized, non- exhaustive list of the safeguards that AlayaCare employs in the protection of PHI.

Administrative Safeguard

Administrative actions, policies, and procedures are implemented to protect the sanctity of PHI and ensure compliance with PHIPA. These requirements cover training and procedures for employees, contingency plans, security incident reporting, and risk management.

AlayaCare's Security and Privacy Committee is committed to identifying and evaluating potential risks that may threaten the achievement of its system requirements and service commitments related to security and availability. Documented policies and procedures are in place to guide personnel in identifying objective risks. Changes in technology, applicable laws and regulations, security threats, and risks are reviewed by AlayaCare on a periodic basis, and existing control activities and Information Security policies are updated as a result.

AlayaCare trains its workforce upon hire and at least annually thereafter regarding AlayaCare's privacy and security obligations and policies with respect to PHI and requires them to demonstrate, to the extent applicable, their understanding of all such obligations and policies. All employees and contractors are required to sign confidentiality agreements.

AlayaCare enters into a contract with each of its health information custodian customers. In those contracts, AlayaCare provides each customer with appropriate assurances regarding AlayaCare's safeguarding of the PHI sourced from those custodians, as required by PHIPA.

Physical Safeguards

Physical safeguards (i.e., the physical measures, policies, and procedures that protect electronic information systems and related buildings and equipment from natural and environmental hazards, and unauthorized intrusion) are an important line of defense in the protection of PHI. In order to define and implement these physical measures, policies, and procedures, AlayaCare first identifies all potential points of physical access to PHI (e.g., data centers, office facilities, etc.), evaluates the reasonable risks associated with each access point, then specifies the means by which those risks will be appropriately managed.

The PHI of AlayaCare's Ontario customers is hosted in Canada on redundant cloud infrastructure in facilities with 24/7/365 physical security monitoring and protection. These physical monitoring and protection measures include physical barriers, multi-factor authentication with biometrics, man-traps, cameras, and 24/7/365 staffing. The data centers are certified in, or have been audited against, applicable industry security standards.

Data transfer between the AlayaCare server and the mobile device is encrypted in transit using HTTPS. PHI is not stored on the mobile device memory; however, some data can be cached locally while using its encrypted database. Upon logout, the database is destroyed.

Technical Safeguards

AlayaCare takes a risk-based approach in determining which technologies, policies, and procedures to employ in the protection of PHI. This strategy involves a combination of various technical controls designed to ensure a multi-layered defense against cybersecurity threats.

In addition to compliance with its regulatory obligations, AlayaCare draws from industry-leading information security standards to employ technical safeguards that cover the entire spectrum of applicable cybersecurity domains, including role-based access controls, user authorization and authentication, configuration management, network security, workstation security, vulnerability management, application security, logging, monitoring, and data encryption, both at rest and in transit. AlayaCare provides its customers with additional details about its technical safeguards under each of these categories as appropriate.

Contact

Please use the following addresses to contact AlayaCare's Privacy Officer if you have any questions about the information in this notice or to identify a privacy or security concern:

Data Privacy & Security Officer
AlayaCare, Inc.
151 Yonge St. Suite 1000,
Toronto, ON M5C 2W7
Email: privacy@alayacare.com