AlayaCare's **Privacy & Security Addendum** ("**PSA**") sets out additional information relating to the privacy and security of the data, including Personal Information, that is collected, used, disclosed, retained, or disposed of by Customer using AlayaCare's cloud-based platform. This PSA supplements the provisions of the subscription agreement (AlayaCare's **Master Subscription and Services Agreement** or equivalent ("**MSSA**")) between Customer and AlayaCare. In the event of a conflict, the MSSA will govern.

AlayaCare maintains an information security program and the associated controls required to comply with applicable laws and regulations, including PIPEDA and PHIPA. Independent verification of AlayaCare's information security programs and related controls are set out in AlayaCare SOC Reports and related attestations, current versions of which can be requested by Customer through the AlayaCare Trust Center.

Protection of Customer Data

Responsibilities Relating to Personal Health Information

AlayaCare is a provider of hosted, electronic health record solutions to Customers who are health care providers and who are subject to laws and regulations governing the use and disclosure of **Personal Information, Sensitive Personal Information and Personal Health information** ("**PHI**"). Canada's PIPEDA and Ontario's PHIPA, along with the regulations adopted under those statutes, govern the handling of PHI. In providing its services, AlayaCare plays an important role in the legal and regulatory regimes that apply to Customers; this collaborative effort is often referred to as a "shared responsibility" model.

Role of Customer and Role of AlayaCare

Under PHIPA, Customer is a Health Information Custodian and responsible for the provision of notice, disclosure, and/or obtaining consent from its Users prior to transferring Customer Data to AlayaCare's software platform.

AlayaCare is considered a Health Information Network Provider (HINP) and has specific responsibilities which differ from those of Customer. These responsibilities include providing a plain language description of AlayaCare's services for Customers to share with their end users (and making a general version publicly available), keeping records of access to, transfers of and unauthorized uses of PHI, and entering into thorough written agreements with both Customers and third parties.

A more thorough overview of these responsibilities is set out in in AlayaCare's published HINP Notice available in the AlayaCare Trust Center.

Shared Responsibility of Customer Data

Customer Data is processed only under the direction and control of Customer. AlayaCare retains no ownership of the Personal Data processed as part of the Services. AlayaCare does not maintain a direct relationship with the individuals whose Personal Data is stored in Customer's databases managed by AlayaCare. Accordingly, AlayaCare does not require, request nor collect individual consents or instructions to access, use, restrict, correct, update or delete Personal Data. Customer is responsible for informing its Users to direct any such requests to them. AlayaCare will promptly forward any requests it receives from Users to Customer. However, if Customer is unable to respond to a particular Personal Data related request, AlayaCare will provide support services to reasonably assist Customer to carry out any such responses.

Collection of and Permitted Uses of Personal Information

Privacy & Security Addendum to MSSA (AC24.2-PSA-ONT-PROD).docx

AlayaCare may collect Personal Information from Customer or from Customer's end Users directly via the use of its software platform or via other interfaces with authorized healthcare information providers, including but not limited to:

- Patient demographic information
- Patient medical history
- Remote patient monitoring data
- Reports created by employees of Customer during healthcare interventions with their clients
- Time and attendance data (including geolocation) related to visits with patients
- System information to diagnose and debug software issues.

AlayaCare will use Personal Information as required to optimize the Services it provides to Customer, to provide updates for the Services and to provide support and maintenance services. It may also use aggregated usage information for statistical purposes (e.g. showing the total traffic through its servers). It may also analyze usage information to evaluate and improve the features and functionality of the Services.

AlayaCare may also use anonymized and aggregated information gathered in connection with Customer Data to improve the quality of the AlayaCare Services, to provide additional services and for the marketing of the AlayaCare Services. This anonymized and aggregated information is not associated with any individual account and will not identify Customer, its clients, nor any of its care providers or other Users. AlayaCare will not disclose any Customer Data that is not anonymized. AlayaCare will perform daily backup of Customer Data for disaster recovery purposes and Customer allows AlayaCare to access and copy Customer Data for that purpose.

Sharing and Disclosure.

AlayaCare does not use nor disclose this Customer Data for purposes other than those for which it was collected, except with Customer's consent (including contractual consent) or as required by law. AlayaCare will not under any circumstances sell or rent Customer Data to third parties and will only share Customer Data to the following:

- Service providers that facilitate the Services, provide any or all part of the Services on AlayaCare's behalf or help it improve the Services (for example, data storage, web analytics, mapping providers and maintenance service providers). These services providers have access to Customer Data only for purposes of performing these tasks on AlayaCare's 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 AlayaCare's compliance with applicable laws, rules, regulations, or guidelines; or (iv) or to establish, protect, or exercise its legal rights or defend against legal claims or demands; and
- Individuals to whom the disclosure of Customer Data has been authorized by Customer.

Retention and Deletion

In accordance with PIPEDA and PHIPA, AlayaCare will retain Personal Information

- as required to manage and administer the Services;
- as required to carry out any legal responsibilities (e.g., legal holds and other legal procedures);
- to resolve a dispute (including enforcement of a contract); or,
- as expressly communicated to Customer at the time of collection.

For as long as Customer's AlayaCare databases remain active, AlayaCare will retain all Customer Data until all applicable retention periods have expired and do so in a manner designed to ensure that it cannot be reconstructed or read. Following such periods, if it is not feasible for AlayaCare to delete or destroy such retained Customer Data, it will continue using the same safeguards of protection and security outlined in this PSA and related subordinate policies, for as long as it cannot be destroyed.

Access Controls

AlayaCare maintains validated policies and procedures that define requirements for granting, provisioning, and revoking access to its systems and data it processes. New or modified user access to networks and in-scope applications are authorized by an AlayaCare-designated system administrators and granted based on job role via a defined access provisioning process. Role-based access control (RBAC) is used to support segregation of incompatible functions.

Users are required to authenticate via unique user account ID and password, with multifactor authentication (and, in designated cases, hardware tokens) before being granted access to in-scope networks, systems and applications. User access reviews of network and application accounts are conducted no less than semi-annually to ensure appropriate logical access is maintained. Further details of the access controls and related procedures that AlayaCare enforces are set out in the current SOC 2 Report.

Risks, Threats, and Breach Notification

AlayaCare as an organization, including its software platform and the supporting infrastructure it provides, maintains administrative, technical and physical safeguards in place to protect against threats, vulnerabilities and risks to the security and integrity of the PHI under its control. When the Services are accessed using current browser technology, Secure Socket Layer (SSL) technology protects information using both server authentication and data encryption to help ensure that data is safe, secure, and available only to each specific User. AlayaCare also implements a security methodology based on dynamic data and encoded session identifiers and hosts the Service in a secure server environment which uses firewalls and other advanced technology to prevent external access or interference. Unique usernames and passwords are also required and must be entered each time a User logs in to the AlayaCare platform. AlayaCare trains its staff about the protection of Personal Information, and the importance of compliance with relevant privacy legislation and company policies. All employees and contractors are required to sign confidentiality agreements.

These safeguards help to prevent unauthorized access, maintain data accuracy, and ensure the appropriate use of PHI. If AlayaCare detects a threat to security or vulnerability in connection with Customer Data, it will contact Customer at the first reasonable opportunity to recommend protective measures. Additionally, incidents of suspected or actual unauthorized handling of Personal Information are always directed to AlayaCare's Legal and Compliance team, which is responsible for determining escalation and response procedures based on the severity and nature of the incident. Incidents involving unauthorized handling of PHI will be governed by applicable laws and regulations. If AlayaCare determines that PHI has been misappropriated or otherwise wrongly acquired, it will promptly issue a report to each affected Customer in addition to any other reporting required by Applicable Law.

For Customers who use the AlayaCare platform, its APIs and other integration mechanisms to connect to other Customer and third-party systems, Customer should be aware that the third parties who provide those connected systems may have different procedures in place to protect PHI than the standards AlayaCare has implemented. Customer should ensure that they are aware of the protections and procedures afforded by such third parties.

Security Incidents, Business Continuity and Disaster Recovery

AlayaCare maintains a comprehensive Security and Incident Response Plan (" **SIRP"**) and staff receive annual training. The SIRP and the capabilities of the key members of AlayaCare's incident response team are reviewed annually, with tabletop exercises and training serving as a means of continuous process improvement and risk mitigation. All actual or suspected incidents are treated in accordance with the SIRP, and a critical assessment and analysis is performed as part of the remediation and post-mortem activities designated by the SIRP.

The Business Continuity and Disaster Recovery Plan is also tested annually, at a minimum, using scenarios based on threat likelihood and magnitude, and lack of availability of key personnel and systems. This plan is updated based on

the results of such tests. Recovery strategies, including data replication, onsite and offsite backups, and a high availability architecture are used for all critical data and production systems to assure restoration of service.

Audit Logs and Consent Directives

The AlayaCare platform is developed to be applicable to various jurisdictions while containing the flexibility to be utilised in more specific contexts. Most jurisdictions require some form of audit logs or reporting when PHI is being collected and processed. AlayaCare provides details relating to the key elements of its audit and logging capabilities which can serve as a baseline upon which Customer can map their specific requirements and use cases.

The AlayaCare platform logs and audits a variety of user and administrative activities and those relating to access and security of Customer's AWS tenant. AlayaCare's audit logs record a comprehensive account of system activities, including details such as the user who performed the action, a timestamp of occurrence, and other pertinent information. This data can be used to uncover potential security threats or compliance breaches, diagnose file system or network device issues, and monitor system performance over time.

Additionally, AlayaCare's software platform enables Health Information Custodians to abide by the consent directives of their end users. While the functionality of the platform provides the tools for Health Information Custodians to comply with PHIPA, the shared responsibility model requires the actor closest to the individual whose information is being collected to ensure compliance.

More Information and Customer Inquiries

For any questions, requests or concerns regarding privacy or data security, Customer can reach AlayaCare's support desk through its existing channels or it can contact AlayaCare at privacy@alayacare.com.

Resources relating to Audit Logs are set out in the AlayaCare Trust Center. Certain additional configurations can be implemented for Customer on request by AlayaCare's professional services and data management teams.

Glossary of Terms and Artifacts

Customer Data means the electronic health records of clients and users of AlayaCare Customers and other information which would be considered Personal Information under Applicable Law.

Electronic Health Record means the electronic systems developed and maintained to enable Health Information Custodians to collect, use and disclose personal health information.

Health Information Custodian (HIC) means a person or organization who has custody or control of personal health information as a result of or in connection with performing the person's or organization's powers or duties, as described in section 3(1) of PHIPA.

Health Information Network Provider (HINP) means a person who provides services to two or more health information custodians where the services are provided primarily to custodians to enable the custodians to use electronic means to disclose personal health information to one another, as described in section 6(1) of Ontario Regulation 329/04, under PHIPA.

Infrastructure means the cloud hosting services provided by Amazon Web Services and the complementary subservices as set out in the AlayaCare SOC Reports.

Personal Information and Personal Health Information (**PHI**) means information that is used by a government authority, financial institution or insurance carrier to distinguish a person from other individuals (*e.g.*, social insurance

number, social security number, credit card information, or insurance policy number) and is, by definition, private. Such information can be used to identify an individual (*e.g.*, a person who works for a healthcare provider, or a recipient of home or home health care services). Information about an individual's health, including insurance and billing information, is **PHI** under PHIPA and its regulations, which is listed in the table below and considered to be the '**Applicable Privacy Laws**'.

Privacy Impact Assessment or ***PIA*** means the report setting out AlayaCare's systematic methodology for identifying and assessing privacy risks associated with its organizational practices and in connection with the delivery of its cloud-hosted electronic medical records platform, the current version of which is available to Customer via the AlayaCare Trust Center.

Services means the cloud-based electronic health record software platform and its clinical and financial management software made available to Customer and Customer's Users via the Infrastructure on a subscription basis as set out in a Master Subscription and Services Agreement or equivalent.

SOC 2 Report means the System and Organization Controls 2 (SOC 2) + HITRUST CSF Type 2 issued by AlayaCare's independent auditors dated December 12, 2023.

Third-Party Providers has the meaning set out in Section 4 of the MSSA.

Threat Risk Assessment or ***TRA*** means AlayaCare's assessment of organizational security weaknesses and mitigation measures, as made available in the Trust Center.

Trust Center or ***AlayaCare Trust Center*** means AlayaCare's hosted information center for security, privacy and compliance information and key resources, available to Customer and approved third parties at ***trustcenter.alayacare.com***.

Applicable Information Privacy Laws

Applicable Law	Type of Personal Information Governed by the Law	Jurisdiction
Personal Information Protection and Electronic Documents Act, SC 2000, c. 5 ("**PIPEDA**")	"An Act to support and promote electronic commerce by protecting personal information that is collected, used or disclosed in certain circumstances, by providing for the use of electronic means to communicate or record information or transactions…." Personal Health Information is expressly excluded from Part 1 ("Protection of Personal Information in the Private Sector").	Canada
Canada's Anti-Spam Legislation S.C. 2010, c. 23 ("**CAN-SPAM**")	"An act to promote… the economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities…." Requires express or implied consent to send commercial electronic messages (*e.g.*, emails, texts and instant messages).	Canada
Personal Health Information Protection Act, SO 2004, c. 3, Sch. A	Personal Health Information	Ontario

(including Ontario Regulation 329/04) (" **PHIPA**")		