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 Québec's *Loi sur la protection des renseignements personnels dans le secteur privé* ("***Loi sur le privé***"), as amended by Loi 25. 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 are available to Customer in the AlayaCare Trust Center.

Protection of Customer Data

Responsibilities Relating to Personal Information and Health-related 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 (*renseignements personnels sensibles*) and Personal Health information (referred to here as "PHI")**. Canada's PIPEDA and Québec's *Loi sur le privé*, 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 Québec's *Loi sur le privé*, Customer is considered an *enterprise* and, while AlayaCare is also an *enterprise* in its own right, its role is best characterized as that of a *third person*. Within the shared responsibility model, AlayaCare's role is to be understood with reference to Customer.

Accordingly, AlayaCare may, in the event of a confidentiality incident that presents a risk to an affected individual, notify both the affected individual and the Commission d'accès à l'information, pursuant to Quebec law and regulations, while also informing Customer. AlayaCare will assist Customer in assessing the sensitivity of the information concerned, the anticipated consequences of its use and the likelihood that such information will be used for injurious purposes before notifying the affected individual and will keep a register of all confidentiality incidents, which will be available to the Commission at its request.

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

AlayaCare may collect Personal Information from Customers or from Customers' 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 Customers 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 Customers, to provide updates to 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 Customers' 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 Quebec's *Loi sur le privé*, 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); and

- as expressly communicated to Customer at the time of collection.

For as long as Customer's AlayaCare databases remain active, AlayaCare will retain all Personal Information until all applicable retention periods have expired and do so in a manner designed to ensure that it cannot be reconstructed or read. The method retention of retention is proportional to the sensitivity of the information stored. Following such periods, if it is not feasible for us to delete or destroy such retained Customer Data, it will continue using the same safeguards of protection and security outlined in this PSA 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 data and systems. New or modified user access to networks and in-scope applications are authorized by an AlayaCare-designated system administrator and granted based on job role via a defined access provisioning process. Role-based access control (RBAC) is used to support segregation of functions and minimum necessary access.

Users are required to authenticate via unique user account ID and password, with multifactor authentication (and in designated tasks, 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 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, Customers 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. Customers 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

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.

AlayaCare provides details relating to the key elements of its audit and logging capabilities can serve as a baseline from which Customers can map to their specific requirements and use cases. These resources are set out in the AlayaCare Trust Center. Certain additional configurations can be implemented for Customers upon request by AlayaCare's professional services and data management teams.

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.

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.

Enterprise has the same meaning as within article 1525 of the Québec Civil Code.

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

(Sensitive) Personal Information 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 that, due to its nature, (in particular its medical, biometric or otherwise intimate nature) or the context of its use or communication, entails a high level of reasonable expectation of privacy, is Sensitive Personal Information (*renseignements personnels sensibles*) under Québec's *Loi sur le privé*, which is listed in the table below and considered to be the '**Applicable Privacy Laws**'.

Privacy Impact Assessment or ***PIA* (*Évaluation des facteurs relatifs à la vie privée or EFVP*)** 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.

Third Person is to be understood in the context of Québec's *Loi sur le privé,* though it is not defined in that statute.

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 Customers 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
Act respecting the protection of personal information in the private sector *(Loi sur la protection des*	(Sensitive) Personal Information (Renseignements personnels (sensibles))	Québec

renseignements personnels dans le secteur privé), CQLR c P-39. **(*"Loi sur le privé*")**		