L'**Annexe sur la confidentialité et la sécurité** (« **ACS** ») fournit des renseignements supplémentaires concernant la confidentialité et la sécurité des données, y compris les renseignements personnels, qui sont recueillis, utilisés, divulgués, conservés ou éliminés par le Client à l'aide de la plateforme infonuagique d'AlayaCare. Le présent ASP complète les dispositions de l'accord de souscription **(Accord-cadre de souscription et de services** d'AlayaCare [« **ACSS** »]) conclu entre le client et AlayaCare. En cas de conflit, l'ACSS prévaut.

AlayaCare maintient un programme de sécurité de l'information et les contrôles associés nécessaires pour se conformer aux lois et règlements applicables, y compris la LPRPDE et la LPRPS. Le contrôle indépendant des programmes de sécurité de l'information d'AlayaCare et des contrôles connexes est exposé dans les rapports SOC d'AlayaCare et leurs attestations, dont les versions actuelles peuvent être demandées par le client dans le Trust Center d'AlayaCare.

Protection des données du Client

Responsabilités relatives aux renseignements personnels sur la santé

AlayaCare fournit des solutions de dossiers médicaux électroniques hébergés aux Clients, lesquels sont des prestataires de soins de santé, assujettis aux lois et réglementations régissant l'utilisation et la divulgation de **Renseignements personnels et de Renseignements personnels sur la santé** (« **RPS** »). La LPRPDE du Canada et la LPRPS de l'Ontario, ainsi que les règlements adoptés en vertu de ces lois, régissent le traitement des RPS. En fournissant ses services, AlayaCare joue un rôle prépondérant dans les systèmes juridiques et réglementaires qui s'appliquent aux clients; cet effort collaboratif est souvent désigné comme un modèle de « responsabilité partagée ».

Rôles du Client et d'AlayaCare

En vertu de la LPRPS, le Client est un dépositaire de renseignements sur la santé et est tenu de fournir un avis, de divulguer et/ou d'obtenir le consentement de ses utilisateurs avant de transférer toute donnée du Client à la plateforme logicielle d'AlayaCare.

AlayaCare est reconnue comme Fournisseur d'un réseau d'information sur la santé (FRIS) et assume des responsabilités spécifiques qui diffèrent de celles du Client. Ces dernières prévoient notamment de fournir aux clients une description vulgarisée des services d'AlayaCare à partager avec leurs utilisateurs finaux (et de rendre publique une version générale); de tenir un registre des accès, des transferts et des utilisations non autorisées de RPS; et de conclure des accords écrits détaillés avec les clients et les tiers.

Une synthèse plus détaillée de ces responsabilités est présentée dans l'avis FRIS publié par AlayaCare et disponible dans le Trust Center d'AlayaCare.

Responsabilité partagée des données du client

Les **données du client** ne sont traitées que sous la direction et le contrôle du client. AlayaCare ne détient pas la propriété des données personnelles traitées dans le cadre des services. AlayaCare n'entretient aucune relation directe avec les personnes dont les données personnelles sont stockées dans les bases de données du client gérées par AlayaCare. Conséquemment, AlayaCare n'exige pas, ne demande pas et ne recueille pas de consentements individuels ou de directives concernant l'accès, l'utilisation, la restriction, la correction, la mise à jour ou l'effacement des données à caractère personnel. Il incombe au client d'informer ses utilisateurs de lui adresser toute demande de ce type. AlayaCare transmettra sans délai au client toute demande émanant d'utilisateurs. Toutefois, si le client n'est pas en mesure de répondre à une demande particulière liée aux données personnelles, AlayaCare assurera un soutien raisonnable au client pour l'aider à répondre à cette demande.

Recueil et utilisation autorisée des renseignements personnels

AlayaCare peut recueillir des renseignements personnels auprès du Client ou des Utilisateurs finaux du Client soit directement par l'utilisation de sa plateforme logicielle, soit par d'autres interfaces auprès de fournisseurs de renseignements médicaux autorisés, y compris, mais sans s'y limiter :

- Renseignements démographiques concernant le patient
- Historique médical du patient
- Données de surveillance à distance du patient
- Rapports créés par les employés du Client lors de la prestation de soins de santé à leurs clients
- Données relatives aux horaires et aux présences (y compris la géolocalisation) liées aux visites avec les patients
- Informations sur le système pour diagnostiquer et déboguer les problèmes logiciels.

AlayaCare utilisera les renseignements personnels au besoin pour optimiser les services fournis au Client, pour fournir des mises à jour des services et pour fournir des services d'assistance et de maintenance. Elle pourrait également utiliser des données d'utilisation agrégées à des fins statistiques, par exemple pour indiquer le trafic total sur l'un de ses serveurs. Elle pourrait également utiliser les données d'utilisation pour évaluer et améliorer les caractéristiques et les fonctionnalités de ses services.

AlayaCare peut également utiliser des informations anonymes et agrégées recueillies en relation avec les Données Client pour améliorer la qualité des Services AlayaCare, pour fournir des services supplémentaires et pour le marketing des Services AlayaCare. Ces informations anonymes et agrégées ne sont pas associées à un compte individuel et n'identifieront pas le Client, ses clients, ni aucun prestataire de soins ou tout autre utilisateur. AlayaCare ne divulguera pas les Données Client qui ne sont pas anonymisées. AlayaCare effectuera une sauvegarde quotidienne des Données Client à des fins de reprise après sinistre et le Client permet à AlayaCare d'accéder et de copier les Données Client à cette fin.

Partage et divulgation.

AlayaCare n'utilise pas et ne divulgue pas les Données client à des fins autres que celles pour lesquelles elles ont été recueillies, sauf avec le consentement du Client (y compris le consentement contractuel) ou si la loi l'exige. AlayaCare ne vendra ou ne louera en aucun cas les données des clients à des tiers et ne partagera lesdites données qu'avec les personnes suivantes :

- Les fournisseurs de services qui contribuent aux services, fournissent la totalité ou une partie des services au nom d'AlayaCare ou l'aident à améliorer les services (par exemple, le stockage de données, l'analyse Web, les fournisseurs de cartographie et les fournisseurs de services de maintenance). Ces fournisseurs de services n'ont accès aux Données des clients qu'aux fins de l'exécution de ces tâches au nom d'AlayaCare;
- Les représentants des forces de l'ordre, les agences gouvernementales ou d'autres autorités judiciaires (i) en réponse à leur demande; (ii) lorsque la loi le permet ou l'exige; (iii) pour établir la conformité d'AlayaCare avec les lois, règles, réglementations ou lignes directrices applicables; ou (iv) pour établir, protéger ou exercer ses droits légaux ou pour se défendre contre des réclamations ou des demandes légales; et
- Les personnes à qui le client a autorisé la divulgation des données le concernant.

Rétention et suppression

Conformément à la LPRPDE et la LPRPS, AlayaCare conservera les renseignements personnels

- dans la mesure où cela est nécessaire pour gérer et administrer les services;

- dans la mesure où cela est nécessaire à l'exercice de toute responsabilité légale (p. ex., saisie légale et autres procédures légales);
- pour résoudre un litige (y compris l'exécution d'un contrat); ou,
- tels que communiqués expressément au Client au moment de la collecte.

Tant que les bases de données AlayaCare du client restent actives, AlayaCare stocke toute Donnée du Client jusqu'à l'expiration de toutes les périodes de conservation applicables, de manière à ce qu'elle ne puisse pas être reconstituée ou lue. À l'issue de ces périodes, s'il n'est pas possible à AlayaCare de supprimer ou de détruire les Données du Client conservées, nous continuerons à utiliser les mêmes garanties de protection et de sécurité que celles décrites dans le présent ASP et les politiques subordonnées connexes, tant qu'elles ne pourront pas être détruites.

Contrôles des accès

AlayaCare applique des politiques et des procédures éprouvées qui déterminent les modalités d'octroi, d'approvisionnement et de révocation de l'accès à ses systèmes et aux données qu'elle traite. Les nouveaux accès ou les accès modifiés aux réseaux et aux applications sont autorisés par des administrateurs de système désignés par AlayaCare et accordés en fonction du rôle de l'utilisateur par le biais d'un processus d'approvisionnement en accès spécifique. Le contrôle d'accès fondé sur les rôles (CAFR) est utilisé pour favoriser le cloisonnement des fonctions incompatibles.

Les utilisateurs sont tenus de s'authentifier au moyen d'un identifiant et d'un mot de passe uniques, d'une authentification multifactorielle (et, dans certains cas précis, de jetons matériels) avant de pouvoir accéder aux réseaux, systèmes et applications relevant du champ du projet. Des vérifications de l'accès des utilisateurs au réseau et aux comptes d'application sont effectuées au moins deux fois par an afin de s'assurer que l'accès logistique approprié est assuré. Des précisions sur les contrôles d'accès et les procédures connexes appliquées par AlayaCare figurent dans le rapport SOC 2 en vigueur.

Risques, menaces et avis de violation

AlayaCare, en sa qualité d'organisation, et notamment de plateforme logicielle et d'infrastructure de soutien connexe, maintient des mesures de protection administratives, techniques et physiques afin de se prémunir contre les menaces, les vulnérabilités et les risques pour la sécurité et l'intégrité des RPS dont elle a la charge. Lorsque les services sont accessibles au moyen de la technologie actuelle des navigateurs, la technologie Secure Socket Layer (SSL) protège les données en utilisant à la fois l'authentification du serveur et le chiffrement des données afin de garantir que les données sont sûres, sécurisées et accessibles uniquement à chaque utilisateur spécifique. AlayaCare applique également une méthodologie de sécurité basée sur des données dynamiques et des identifiants de session codés et héberge le service dans un environnement de serveur sécurisé, lequel utilise des pare-feu et d'autres technologies avancées pour empêcher les interférences ou l'accès d'intrus extérieurs. Des noms d'utilisateur et des mots de passe uniques sont également exigés et doivent être saisis chaque fois qu'un client se connecte à la plateforme AlayaCare. AlayaCare forme son personnel à la protection des renseignements personnels et à l'importance du respect de la législation sur la protection de la vie privée et des politiques de l'entreprise. Tous les employés et les sous-traitants sont tenus de signer des accords de confidentialité.

Ces mesures de protection contribuent à empêcher l'accès non autorisé, à préserver l'exactitude des données et à garantir l'utilisation appropriée des PHI. Dans le cas où AlayaCare constate un risque de sécurité ou de vulnérabilité en rapport avec les données du client, elle communiquera avec ce dernier dans les plus brefs délais afin de lui recommander des mesures de protection. Par ailleurs, les incidents liés à la manipulation non autorisée, réelle ou présumée, de renseignements personnels sont toujours adressés à l'équipe responsable des questions juridiques et de conformité d'AlayaCare, laquelle est chargée de déterminer les procédures d'escalade et de réponse, en fonction de la gravité et de la nature de l'incident. Les incidents impliquant une manipulation non autorisée de RPS seront régis par les législations et réglementations applicables. Si AlayaCare détermine que des RPS ont été détournés ou autrement

obtenus de manière illégitime, elle émettra sans délai un rapport à chaque client concerné, parallèlement à tout autre rapport exigé par le droit applicable.

Les clients qui ont recours à la plateforme AlayaCare, à ses API et à d'autres mécanismes d'intégration pour se connecter à d'autres systèmes de clients et de tiers doivent savoir que les tiers fournissant ces systèmes peuvent avoir mis en place des procédures de protection des RPS différentes des normes mises en œuvre par AlayaCare. Le Client doit s'assurer de connaître les mesures de protection et les procédures offertes par ces tiers.

Incidents de sécurité, continuité des activités et reprise après sinistre

AlayaCare a mis en place un plan complet de sécurité et de réponse aux incidents (« **PSRI** ») et son personnel est formé chaque année. Le PSRI et les aptitudes des principaux acteurs de l'équipe de réponse aux incidents d'AlayaCare sont revus chaque année, avec des simulations et des formations destinées à améliorer en permanence les processus et à minimiser les risques. Tout incident réel ou présumé est traité conformément au PSRI, et une évaluation et une analyse critiques sont effectuées conformément aux activités de remédiation et post-mortem prévues par le SIRP.

Le Plan de continuité des activités et reprise après sinistre est également examiné au minimum chaque année, à l'aide de scénarios fondés sur la probabilité et l'ampleur de la menace, ainsi que sur le manque de disponibilité du personnel et des systèmes clés. Ce plan est mis à jour en fonction des résultats de ces tests. Des stratégies de récupération, notamment la reproduction des données, les sauvegardes sur site et hors site, et l'architecture à haute disponibilité sont utilisées pour les données critiques et les systèmes de production afin d'assurer le rétablissement du service.

Journaux d'audit et directives relatives au consentement

La plateforme AlayaCare a été développée pour être applicable à différentes juridictions tout en ayant la flexibilité nécessaire pour être utilisée dans des contextes plus spécifiques. La plupart des juridictions exigent, de quelque manière que ce soit, des journaux d'audit ou des rapports lorsque des renseignements personnels sont recueillis et traités. AlayaCare détaille les principaux aspects de son audit et de ses capacités de journalisation, pour servir de référentiel à partir duquel le Client peut adapter ses besoins spécifiques et ses cas d'utilisation.

La plateforme AlayaCare consigne et contrôle diverses activités administratives des utilisateurs et liées à l'accès et à la sécurité du locataire AWS de chaque client. Les journaux d'audit d'AlayaCare contiennent un compte rendu complet des activités du système, y compris les détails relatifs aux utilisateurs qui ont effectué les actions, l'horodatage des événements, ainsi que d'autres informations pertinentes. Ces données peuvent être utilisées pour identifier des menaces potentielles pour la sécurité ou des atteintes à la conformité, pour diagnostiquer des problèmes liés au système de fichiers ou aux périphériques de réseaux, et pour observer les performances du système dans le temps.

En outre, la plateforme logicielle d'AlayaCare permet aux dépositaire de renseignements sur la santé de satisfaire aux exigences en matière de consentement de leurs utilisateurs finaux. Bien que la plateforme fournisse les outils permettant aux dépositaires de renseignements sur la santé de satisfaire la LPRPS, le modèle de responsabilité partagée exige que ce soit la partie prenante qui soit la plus rapprochée de la personne dont les renseignements sont recueillis qui garantisse la conformité.

Autres informations et requêtes des clients

Pour toute question, demande ou préoccupation concernant la confidentialité ou la sécurité des données, le client peut contacter le service de soutien d'AlayaCare par les voies existantes ou il peut contacter AlayaCare à l'adresse privacy@alayacare.com.

Les ressources relatives aux journaux d'audit se trouvent dans le Trust Center d'AlayaCare. Certaines configurations supplémentaires peuvent être mises en œuvre pour le Client sur demande par les services professionnels et les équipes de gestion des données d'AlayaCare.

Lexique des termes et des objets

Les ***données du Client*** désignent les dossiers médicaux électroniques des clients et des utilisateurs des clients d'AlayaCare et toute autre information qui serait considérée comme des renseignements personnels en vertu de la loi applicable.

Dossier médical électronique : les systèmes électroniques développés et maintenus pour permettre aux dépositaires de renseignements sur la santé de recueillir, exploiter et divulguer des renseignements personnels sur la santé.

Dépositaire de renseignements sur la santé (DRS) : personne ou organisation qui détient ou contrôle des renseignements personnels sur la santé dans le cadre de l'exercice de ses fonctions, tel que décrit à l'article 3(1) de la LPRPS.

Fournisseur d'un réseau d'information sur la santé (FRIS) : personne qui fournit des services à deux dépositaires de renseignements sur la santé ou plus, principalement pour leur permettre de recourir à des moyens de communication électroniques pour échanger des renseignements personnels sur la santé, conformément à l'article 6 (1) de la réglementation de l'Ontario 329/04, en vertu de la LPRPS.

Infrastructure définit les services d'hébergement infonuagiques fournis par Amazon Web Services et les sous-services connexes, conformément aux rapports SOC d'AlayaCare.

Renseignements personnels et Renseignements personnels sur la santé (**RPS**) : les données utilisées par une autorité gouvernementale, une institution financière ou une compagnie d'assurance pour distinguer un individu des autres (*p. ex.,* le numéro d'assurance sociale, le numéro de sécurité sociale, les informations relatives à la carte de crédit ou le numéro de la police d'assurance) sont privées. Ces derniers peuvent être utilisés pour identifier une personne (*p. ex.,* une personne travaillant pour un prestataire de soins ou un bénéficiaire de services de soins à domicile). Les renseignements sur la santé (y compris les données relatives aux assurances et à la facturation) sont des renseignements sur la santé protégés (« **RSP** ») en vertu de la LPRPS et des législations provinciales, énumérées dans le tableau ci-dessous et considérées comme « **loi applicable en matière de protection de la vie privée** ».

L'***Évaluation des facteurs relatifs à la vie privée*** ou ***EFVP*** renvoie au rapport exposant la méthodologie systématique d'AlayaCare visant à identifier et à évaluer les risques relatifs à la vie privée associés à ses pratiques organisationnelles et à la prestation de sa plateforme de dossiers médicaux électroniques hébergés en nuage, dont la version actuelle est mise à la disposition du client via le Trust Center d'AlayaCare.

Services désignent la plateforme logicielle de dossier médical électronique infonuagique et son logiciel de gestion clinique et financière mis à la disposition du client et des utilisateurs du client via l'infrastructure sur la base d'un abonnement tel que défini dans un accord-cadre de souscription et de services ou un accord équivalent.

Le rapport SOC 2 désigne les contrôles des systèmes et des organisations (SOC 2) + HITRUST CSF Type 2 émis par les auditeurs indépendants d'AlayaCare en date du 12 décembre 2023.

Fournisseurs tiers a été défini à l'article 4 de l'ACSS.

Évaluation des risques et des menaces (***ERM***) : analyse par AlayaCare des lacunes de sécurité de l'organisation et des mesures d'atténuation, publiée dans le Trust Center.

Trust Center ou ***AlayaCare Trust Center*** désigne le centre d'information hébergé d'AlayaCare contenant des renseignements sur la sécurité, la confidentialité et la conformité ainsi que des ressources clés, accessibles aux clients et aux tiers approuvés à l'adresse ***trustcenter.alayacare.com*** (en anglais).

Lois sur la protection des renseignements personnels applicables

Loi applicable	Type d'informations personnelles régies par la loi	Juridiction
Loi sur la protection des renseignements personnels et les documents électroniques, SC 2000, c. 5 (« **LPRPDE** »)	« Loi visant à soutenir et à promouvoir le commerce électronique en protégeant les renseignements personnels recueillis, utilisés ou divulgués dans certaines circonstances, en prévoyant le recours à la voie électronique pour communiquer ou enregistrer des renseignements ou des transactions… » Les Renseignements personnels sur la santé sont expressément exclus de la Partie 1 (« Protection des renseignements personnels dans le secteur privé »).	Canada
La Loi canadienne anti-pourriel S.C. 2010, c. 23 (« **CAN-SPAM** »)	« Loi visant à promouvoir… l'économie canadienne par la réglementation de certaines pratiques qui découragent l'exercice des activités commerciales par voie électronique… » Requiert un consentement explicite ou implicite pour pouvoir envoyer des messages électroniques commerciaux (*p. ex.*, des courriels, des textos et des messages instantanés).	Canada
Loi sur la protection des renseignements personnels sur la santé, SO 2004, c. 3, Sch. A (y compris la réglementation de l'Ontario 329/04) (« **LPRPS** »)	Renseignements personnels sur la santé	Ontario