

OnCall Health Privacy Policy

OnCall Health allows health care providers to enhance their service with secure video consultations, and patients to consult health care providers from the privacy and convenience of the location they choose. This means personal information and personal health information is collected by OnCall Health. This information is highly sensitive and protected by the is protected by The Personal Information Protection and Electronic Documents Act (Canada) (PIPEDA) and all applicable provincial and territorial personal health information protection legislation throughout Canada. OnCall Health is committed to safeguard it at the corresponding level. This Privacy Policy describes the physical, technological and administrative measures we implement to safeguard personal and personal health information. We comply with privacy law and we honour the trust of our users by taking every necessary measure to protect personal and personal health information.

By law, personal information is information that relates to an identifiable individual, to the exclusion of business contact information (name, title, work address, work phone number or work email address). Personal health information includes information that relates to an identifiable individual's health, physical or mental, health history including family health history, or medical treatment.

If we update this Privacy Policy, we will notify you.

Read on to learn more, and if you have questions, feel free to reach our Designated Privacy Contact, Chief Privacy and Security Officer, Nicholas Chepesiuk: nicholas@oncallhealth.ca, 1-647-964-4134.

Our commitment

OnCall Health will never collect, use or disclose personal or personal health information without the consent of the individual it relates to.

OnCall Health safeguards personal and personal health information on the basis of risk assessments and industry standards regarding physical security, technological security and administrative policies and processes, as explained further below.

OnCall Health complies with all applicable personal health information legislation where it operates.

Information we collect

From health care providers:

We collect name, business contact information as well as specialization.

From patients:

When consulting their own health care provider registered with OnCall Health, we collect:

- Name and email of the patient

- Date and time of the appointment
- Any written instructions by the provider added to the "notes for patient" after the appointment
- Files attached by the provider or patient during or after the appointment inside the platform, usually as PDF or Word documents

How we protect the information we collect

OnCall Health protects personal and personal health information through integrated physical, technological and administrative safeguards:

Physical safeguards:

OnCall Health premises are divided into secure areas where electronic equipment and personal and personal health information cannot be accessed without authorization.

Access is controlled by a code and monitored in a manner that keeps all personal and personal health information secure from unauthorized access.

OnCall Health electronic equipment does not include portables that leave the premises.

All necessary backups are safely locked away.

OnCall Health does not keep personal or personal health information on paper.

Technological safeguards:

OnCall Health stores all personal and personal health information in Montreal, Canada, with Amazon Web Services Secure Cloud (AWS). AWS is certified as compliant with ISO/IEC Standard 27018:2014 Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors. In addition to the independent certification process under ISO/IEC 27018:2014, this Standard also includes the right to audit AWS for compliance.

The secure video and/or text consultation is encrypted with the AES cipher using 256-bit keys. Here are the details of our encryption:

- The basic voice, video, and text traffic are converted into cipher, a form which cannot be understood by anyone except authorized parties.
- The conversion is done with random keys that change from the beginning to the end of the conversation to make it even more secure.
- The keys last a short period of time and are neither stored nor persistent anywhere.

OnCall Health destroys or anonymizes all personal and personal health information when it is no longer necessary to deliver service.

OnCall Health employees can only gain technological access to personal information or personal health information collected by OnCall Health:

- With a robust password, based on required elements.
- Upon authorization, granted strictly on a need-to-know basis, defined according to job requirements.

Access is monitored through technological audit trails.

Audit trails are regularly reviewed to ensure compliance.

Administrative measures:

OnCall Health has appointed a Designated Privacy Contact, mentioned above, who acts as Chief Privacy and Security Officer (CPSO) responsible for information systems monitoring and information security policy and procedure management.

The CPSO is responsible for compliance with OnCall Health's privacy programme including:

- Undertaking threat and risk assessments on a regular basis and as systems are approved
- Adopting policies and procedures on the basis of threat and risk assessments to mitigate all identified risks, and updating these policies and procedures as necessary.

OnCall Health users may access their personal information by accessing their account and, should they require assistance, by contacting our CPSO.

Upon the express request of a user, OnCall Health will immediately close the user's account and destroy or anonymize all personal information related to that account.

OnCall Health completes background checks on all its employees before they start employment. As soon as employment starts, OnCall Health trains, supports and supervises all its employees on its Privacy Policy and procedures.

Contractors are held to the same high level of protection of personal and personal health information as OnCall Health through contractual agreements, including audits, based on OnCall Health's Privacy Policy and procedures.

OnCall Health senior management receives regular reports on privacy compliance and, in turn, reports to the Board for oversight.

OnCall Health is regularly audited by a third party to ensure we are meeting our privacy obligations. This is part of a process for OnCall Health to reassess all policies and procedures on an ongoing basis to ensure that legal requirements are met and personal and personal health information is highly secure.

How we use the information we collect

OnCall Health will never use personal or personal health information for purposes other than those for which it is provided – with express consent – and those necessary to deliver the service requested by the user.

OnCall Health will never sell the personal information or personal health information it collects, nor otherwise make any such information available to a third party in exchange for remuneration.

OnCall Health will never disclose personal or personal health information, except as required by law and upon demonstrated lawful authority.

Should OnCall Health conduct market or product research, it will never use personal nor personal health information, which is traceable to any individual; rather, it will fully anonymize information, meaning the risk of this information being traced back to a given individual is reduced to the greatest extent possible.

Should OnCall Health offer users the opportunity to receive relevant information on products or services, or promotions, OnCall Health will seek the users' explicit consent to exercise that option.

Breach response

Experience tells us that there is no total guarantee against data breaches. However, as described above, OnCall Health has taken all reasonable measures to prevent breaches.

Furthermore, in the event of a breach, OnCall Health would immediately mitigate its impact by:

- Notifying users at the first reasonable opportunity, namely as soon as we identify the breach
- Applying remedial measures immediately.

Ensuring patients' meaningful consent

To ensure OnCall Health patients' meaningful consent, OnCall Health provides relevant information in this Privacy Policy, as well as through the availability of our Designated Privacy Contact, nicholas@oncallhealth.ca, 647-964-4134, and subjects the use of OnCall Health secure video consultations to the following patient consent form.

To proceed with registration for OnCall Health secure video consultations, a patient must expressly agree to the terms of the following consent form.

OnCall Health Secure Consultation Patient Consent Form

I agree to OnCall Health secure video or text consultations with a health care provider on the basis of the following information:

OnCall Health will collect my name, the name and contact information of the health care provider (including their specialization), as well as the time of our appointments.

OnCall Health consultation will occur on a secure video feed, safeguarded as described in the OnCall Health Privacy Policy.

OnCall Health will not use my personal or personal health information without my consent except as necessary to provide its services.

OnCall Health will never sell my personal or personal health information, nor otherwise make any of my personal information available to a third party in exchange for remuneration.

OnCall Health will never disclose my personal information except as required by law and upon demonstration of lawful authority.

Upon my express request, OnCall Health will immediately close my account and destroy or anonymize all personal information related to my account.

OnCall Health

Politique de protection de la vie privée¹

L'entreprise OnCall Health permet aux prestataires de soins de santé d'enrichir leurs services au moyen de consultations vidéo sécurisées, et aux patients de consulter des professionnels de la santé à partir d'un endroit privé et commode de leur choix. Cela signifie qu'OnCall Health recueille des renseignements personnels, ainsi que des renseignements personnels sur la santé. Ces renseignements sont hautement confidentiels et sont protégés par la *Loi sur la protection des renseignements personnels et les documents électroniques (Canada)* (LPRPDE), ainsi que par toutes les lois provinciales et territoriales en matière de protection des renseignements personnels sur la santé, qui s'appliquent à travers le Canada. OnCall Health est soucieuse d'assurer à ces renseignements une protection à la hauteur de leur degré de confidentialité. La présente politique de protection de la vie privée (la « Politique ») décrit les mesures matérielles, technologiques et administratives qu'applique OnCall Health afin de veiller à la sauvegarde de renseignements personnels et de renseignements personnels sur la santé. OnCall Health respecte les lois sur la protection de la vie privée et la confiance que lui font les utilisateurs de ses services, en ayant recours à tous les moyens nécessaires pour protéger de tels renseignements.

Comme le prévoit la loi, les renseignements personnels sont ceux qui concernent un individu identifiable, à l'exclusion de ses coordonnées d'affaires (nom, désignation du poste, adresse de son lieu de travail, numéro de téléphone ou adresse électronique au travail). Les renseignements personnels sur la santé comprennent ceux qui concernent la santé physique ou mentale d'un individu identifiable, ses antécédents médicaux, y compris ceux de sa famille, ou les traitements médicaux reçus par l'individu en question.

Si OnCall Health procède à une mise à jour de la présente Politique, vous en serez avisé.

Pour en savoir plus, poursuivez votre lecture. Si vous avez des questions, n'hésitez pas à communiquer avec la personne ressource désignée en matière de protection de la vie privée et le chef de la protection des renseignements personnels et de la sécurité chez OnCall Health, Nicholas Chepesiuk : nicholas@oncallhealth.ca, 1-647-964-4134.

L'engagement d'OnCall Health

Sans le consentement de la personne concernée, OnCall ne recueillera jamais de renseignements personnels ou de renseignements personnels sur la santé, et n'utilisera et ne divulguera jamais ces renseignements.

Tel qu'expliqué de manière plus détaillée ci-dessous, OnCall Health offre une protection de renseignements personnels et de renseignements personnels sur la santé qui est conçue en fonction des critères d'évaluation des risques et des normes de l'industrie applicables en matière de sécurité matérielle et technologique et de politiques et procédures administratives.

Partout où OnCall Health exerce ses activités, celle-ci respecte toutes les lois applicables en matière de protection de renseignements personnels sur la santé.

¹ Afin de faciliter votre lecture du présent texte, nous avons employé le masculin comme genre neutre pour désigner aussi bien les femmes que les hommes.

Renseignements recueillis par OnCall Health

De la part de professionnels de la santé :

OnCall Health recueille leurs noms, leurs coordonnées professionnelles et les renseignements pertinents au sujet de leur spécialisation.

De la part de patients :

Lorsqu'un patient consulte son propre professionnel de la santé et que celui-ci est inscrit chez OnCall Health, cette dernière recueille les renseignements suivants :

- le nom et l'adresse électronique du patient;
- la date et l'heure du rendez-vous;
- toutes instructions écrites que le professionnel de la santé ajoute au dossier du patient à la suite du rendez-vous;
- les fichiers (généralement en format PDF ou Word) que le professionnel de la santé ou le patient auront joints au dossier de ce dernier par l'intermédiaire de la plateforme d'OnCall Health, pendant ou après le rendez-vous.

Protection offerte par OnCall Health

OnCall Health protège les renseignements personnels et les renseignements personnels sur la santé par l'intermédiaire d'un ensemble intégré de moyens de sauvegarde matériels, technologiques et administratifs.

Moyens de protection matériels :

Les locaux d'OnCall Health sont divisés en zones sécurisées au sein desquelles il est impossible d'accéder au matériel électronique et à des renseignements personnels ou à des renseignements personnels sur la santé sans en avoir obtenu l'autorisation.

L'accès aux différentes zones sécurisées est contrôlé au moyen d'un code et est supervisé de manière à ce que tous les renseignements personnels et renseignements personnels sur la santé soient protégés contre un accès non-autorisé.

Le matériel électronique d'OnCall Health ne comprend pas de dispositifs portables qui pourraient être emportés à l'extérieur des locaux.

Toutes les copies de sauvegarde nécessaires sont conservées sous clé en lieu sûr.

OnCall Health ne garde pas de copies papier de renseignements personnels ou de renseignements personnels sur la santé.

Moyens de protection technologiques :

OnCall Health stocke tous les renseignements personnels et renseignements personnels sur la santé qu'elle recueille à Montréal (Québec, Canada), avec *Amazon Web Services Secure Cloud* (AWS), qui offre une plateforme de services d'informatique en nuage sécurisés. AWS est certifiée ISO/IEC 27018 :2014 (la « Norme ») – Code de bonnes pratiques pour la protection des informations personnelles identifiables (*personally identifiable information* – PII) dans l'informatique en nuage public agissant comme processeur de PII. En plus de l'assurance écrite – sous forme de certificat donné par une tierce partie indépendante – que les services d'AWS sont conformes aux exigences de la Norme, il est également prévu qu'AWS se soumette à une vérification de sa conformité avec les critères de cette Norme.

Les consultations sécurisées en mode vidéo ou texte sont cryptées selon la norme de chiffrement de données avancée (*Advanced Encryption Standard* – AES), avec des clés de 256 bits. Voici les modalités du processus de cryptage suivi par OnCall Health :

- L'essentiel des informations en mode voix, vidéo ou texte est converti en code, c'est-à-dire en une forme que personne ne peut comprendre, à l'exception des intervenants qui ont l'autorisation voulue.
- Cette conversion est d'autant plus sécurisée qu'elle est effectuée à l'aide de clés aléatoires qui sont modifiées tout au long de l'échange.
- Ces clés ne subsistent que pendant un court espace de temps, et ne persistent et ne sont archivés nulle part.

OnCall Health détruit ou anonymise tous les renseignements personnels et tous les renseignements personnels sur la santé dès que ces renseignements ne sont plus nécessaires pour la prestation de services.

Les employés d'OnCall Health n'ont un accès informatique aux renseignements personnels et aux renseignements personnels sur la santé recueillis par OnCall Health que sous les conditions suivantes :

- avec un mot de passe fort, établi selon des critères obligatoires;
- après avoir obtenu l'autorisation voulue, qui n'est accordée strictement qu'à ceux qui ont un véritable besoin de connaître les renseignements concernés, besoin qui est défini selon les exigences du poste de l'employé en question.

L'accès aux renseignements personnels et aux renseignements personnels sur la santé est supervisé au moyen des pistes de vérification des audits technologiques.

Afin de garantir le respect des conditions d'accès, les pistes de vérification sont examinées sur une base régulière.

Mesures administratives :

Comme mentionné ci-dessus, OnCall Health a nommé une personne ressource désignée en matière de protection de la vie privée, qui joue le rôle de chef de la protection des renseigne-

ments personnels et de la sécurité (CPRPS), et qui est chargée de la supervision des systèmes d'information et de la gestion des politiques et procédures de sécurité de l'information.

Le CPRPS a pour mission de faire respecter le programme d'OnCall Health en matière de protection de la vie privée, ce qui comprend :

- procéder, sur une base régulière et au fur et à mesure que différents systèmes sont approuvés, à l'évaluation des menaces et des risques;
- adopter les politiques et les procédures nécessaires en fonction des résultats des évaluations des menaces et des risques de manière à limiter les risques identifiés, et mettre ces politiques et procédures à jour lorsque nécessaire.

Les utilisateurs des services d'OnCall Health peuvent accéder à leurs renseignements personnels en se connectant à leur compte. S'ils ont besoin d'aide pour ce faire, ils peuvent communiquer avec le CPRPS d'OnCall Health.

À la demande expresse d'un utilisateur, OnCall Health fermera immédiatement son compte et détruira ou anonymisera tous les renseignements personnels s'y rapportant.

OnCall Health procède à la vérification des antécédents de tous ses employés avant qu'ils n'entrent en poste. Dès que ses employés commencent le travail, OnCall Health veille à ce qu'ils suivent une formation sur la présente Politique et les procédures qui s'y rapportent, et à ce qu'ils reçoivent le soutien et l'encadrement nécessaires pour les mettre en application.

Sous l'effet d'ententes contractuelles, les fournisseurs d'OnCall Health se voient imposer les mêmes critères rigoureux que les employés d'OnCall Health pour ce qui est de la protection des renseignements personnels et des renseignements personnels sur la santé. Ces fournisseurs font également l'objet d'audits qui portent sur les exigences de la présente Politique et des procédures qui s'y rapportent.

Des rapports sur le respect des obligations de l'entreprise en matière de protection de la vie privée sont régulièrement présentés aux cadres supérieurs d'OnCall Health. À des fins de contrôle, ces cadres soumettent à leur tour ces rapports au conseil d'administration d'OnCall Health.

OnCall Health fait l'objet d'audits réguliers menés par des tiers, de façon à veiller à ce que l'entreprise s'acquitte de ses obligations en matière de protection de la vie privée. Ces audits font partie d'un processus en vertu duquel OnCall Health réévalue de manière continue ses politiques et ses procédures afin de faire en sorte que toutes les obligations juridiques applicables soient respectées et que les renseignements personnels et les renseignements personnels sur la santé restent hautement sécurisés.

Utilisation des renseignements recueillis par OnCall Health

OnCall Health n'utilisera jamais les renseignements personnels ou les renseignements personnels sur la santé qui leur sont fournis par un utilisateur – avec le consentement exprès de ce dernier – à des fins autres que celles pour lesquelles ces renseignements ont été fournis ou celles qui sont nécessaires afin d'assurer la prestation du service demandé par l'utilisateur.

OnCall Health ne vendra jamais les renseignements personnels ou les renseignements personnels sur la santé qu'elle recueille, et ne les mettra jamais à la disposition d'autrui contre rémunération.

OnCall Health ne divulguera jamais de renseignements personnels ou de renseignements personnels sur la santé, sauf lorsqu'une loi applicable le requiert et qu'il a été démontré que la divulgation est exigée par une source d'autorité légitime.

Dans l'éventualité où OnCall Health mènerait une étude de marché ou de produits, elle n'utilisera jamais de renseignements personnels ou de renseignements sur la santé qui pourraient être reliés à un individu déterminé. OnCall Health anonymisera plutôt les renseignements dans leur intégralité, ce qui signifie que le risque qu'ils puissent être associés à une personne donnée est réduit dans toute la mesure du possible.

Dans l'éventualité où OnCall Health offrirait à ses utilisateurs la possibilité de recevoir des informations ou de la publicité promotionnelle concernant divers produits et services, elle obtiendrait le consentement exprès de ses utilisateurs avant de leur envoyer ces informations ou cette publicité.

Intervention en cas de faille dans les dispositifs de confidentialité et de sécurité

L'expérience démontre qu'il n'existe pas de garantie totale contre des failles dans les dispositifs de protection des données. Cependant, comme expliqué ci-dessus, OnCall Health prend toutes les mesures raisonnables afin d'empêcher que de telles failles se présentent.

Par ailleurs, en cas de faille dans ses dispositifs de protection des données, OnCall Health agira immédiatement pour en atténuer les conséquences :

- en avisant les utilisateurs dès que raisonnablement possible, c'est-à-dire aussitôt qu'OnCall Health aura identifié la faille;
- en mettant en œuvre sans délai des mesures correctives.

Garantir le consentement éclairé des patients

Afin de veiller à ce que les patients puissent donner un consentement éclairé, OnCall Health leur fournit les informations pertinentes dans la présente Politique, et leur offre la possibilité de poser leurs questions à sa personne ressource désignée en matière de protection de la vie privée, Nicholas Chepesiuk (nicholas@oncallhealth.ca, 1-647-964-4134).

Pour s'inscrire et pouvoir assister à des consultations vidéo sécurisées offertes par OnCall Health, chaque patient doit avoir expressément confirmé son accord avec les dispositions du formulaire de consentement qui suit.

Consultations sécurisées offertes par OnCall Health Formulaire de consentement du patient

OnCall Health offre un service de consultations sécurisées, en mode vidéo ou texte, avec des prestataires de soins de santé. En me fondant sur les informations suivantes, je consens à participer à de telles consultations sécurisées :

OnCall Health recueillera mon nom, le nom et les coordonnées professionnelles du prestataire de soins de santé (y compris les renseignements pertinents au sujet de sa spécialisation), ainsi que les dates et heures de nos rendez-vous.

La consultation offerte par OnCall Health aura lieu au moyen d'un signal vidéo qui est sécurisé de la manière décrite dans la présente Politique.

OnCall Health n'utilisera jamais mes renseignements personnels ou mes renseignements personnels sur la santé sans mon consentement exprès, sauf dans la mesure nécessaire pour assurer la prestation de ses services.

OnCall Health ne vendra jamais mes renseignements personnels ou mes renseignements personnels sur la santé, et ne les mettra jamais à la disposition d'autrui contre rémunération.

OnCall Health ne divulguera jamais mes renseignements personnels, sauf lorsqu'une loi applicable le requiert et qu'il a été démontré que la divulgation est exigée par une source d'autorité légitime.

À ma demande expresse, OnCall Health fermera immédiatement mon compte et détruira ou anonymisera tous les renseignements personnels s'y rapportant.