

Privacy at INSIG

Updated: August 12, 2024

INSIG HEALTH (“**Insig**”, “**us**” or “**we**”) are proud to offer you the Tia and Virtualclinic+ webpages (the “**Webpages**”) and the associated online clinics and apps (the “**Platforms**”). INSIG is committed to protecting your personal information and complying with applicable data protection and privacy laws. This “Privacy Policy” tells you how we do so.

This Privacy Policy applies to the collection, use and disclosure of personal information by health care professionals, including physicians, physician assistants, and therapists (“**HCPs**”) who use the platforms to provide individuals with telehealth or telemedicine services (“**Health Services**”) or assisting with the provision of services (“**Support Services**”) on INSIG.

Some HCPs may be subject to additional privacy laws and professional requirements that govern how HCPs collect, use and disclose personal information. In certain cases, the HCP and not INSIG is responsible for the protection of your personal information. In such cases, INSIG will be considered the HCPs agent and shall continue to protect all personal information in accordance with this privacy policy, but shall collaborate with the HCP as required. If you have any questions about this, we encourage you to reach out to privacy@well.com.

We will update this Privacy Policy as necessary. Please check it regularly.

1. What information do we collect?

Webpages - Cookies

Unless you opt-out, our Webpage uses “Cookies” and other automatic data collection technologies with your consent to collect personal information whenever you visit or interact with the Webpages, including unique identifiers and preference information such as IP address, technical usage, browser type, time zone settings, language preferences, operating system, unique device identifiers, search history, page response times and length of visit, pages viewed, marketing preferences or navigation and clickstream behavior for online interactions.

These Cookies helps us understand how you use the Webpages and the content of the Webpages in order to make improvements. We also may use these Cookies to promote our services through marketing and advertising. These Cookies may be accessed or disclosed to third-parties for the purpose of serving you relevant advertisements.

You can opt-out of Cookies or prevent third-party websites from accessing our Cookies through the privacy settings on your browser. However, opting-out of our Cookies may disable some of the Webpages’ features, and may prevent us from providing you with the information and services you have requested.

Webpages - Contact-Us (online form, chat box, or e-mail)

When you submit a form on the Webpages, use our customer service chat messenger, or e-mail us with a question, we will collect personal information about you like your name, e-mail, phone number, and company name. This information will be used by INSIG to communicate with you, provide you with the information you requested, and conduct appropriate follow-up.

Webpages - Direct Marketing

If you sign up to receive direct marketing or promotional communications from INSIG, we will collect your name and e-mail to inform you about INSIG and the associated products and services. If you sign-up to receive newsletters or request additional information about INSIG’s parent company WELL Health Technologies Corp.

(“WELL”), we will share your name and e-mail address with WELL so they can provide you with the information you requested.

Platform – Provider Account Creation

When a HCP registers to become a HCP on the Platform, we will collect personal information about the HCP like name, e-mail, phone number, billing details, information about their medical practice, and information about their registration with their respective provincial colleges. This information will be used by INSIG to create an account for the HCP with INSIG and the respective Platform (“**HCP Accounts**”), verify they have a valid license to act as a HCP with their respective provincial college, confirm their identity in the future, and to contact the HCP with respect to their use of the Platform.

Platform – Patient Account Creation

When an individual registers as a patient on the Platform to access Health Services with a HCP, we will collect their name, e-mail address, phone number, gender, date of birth, province/territory/state of residence, healthcare card, and credit card information or other billing information. This information will be used to create a user account for the individual (“**User Account**”). While we collect your credit card information, we use Stripe to process all payments, and as such, do not store such information.

The Health Services and Support Services are also available for use by children at the discretion of the HCP. For all patients under the age of 18, the holder of the User Account must be the patient’s parent or legal guardian. The parent or legal guardian may be asked to provide personal information about the minor in order to register them to use the User Account (“**Registered Child**”).

Platform – Patient Visits

Through the use of the Platforms, HCPs may collect and use personal health information about the patient. HCPs may collect personal health information verbally or by text, including: the reason for the patient’s consultation request, relevant health history, present condition or symptoms and current treatments. This information is used by the HCP to provide the Health Services and /or Support Services. The HCPs may log this personal information about the visit to the relevant User Account on the Platform, which may be referenced by them and other HCPs in the future. Patients are also able to log personal health information into their User Account to allow easy reference by HCPs.

During your visit with a HCP, the HCP may utilize artificial intelligence transcription technology embedded in the Platform, which will record your voice to help create a summary of your visit on the Platform for record keeping purposes. Once the summary note is made, your voice recording is deleted shortly after. Please refer to section 11 of this privacy policy for more information on how we use and protect this technology, or reach out to privacy@well.com with your questions or feedback.

In some cases, some HCPs who use the Platforms and interact with patients are governed by their own privacy policies with respect to the collection, use and disclosure of personal information to comply with the laws of the HCP’s local jurisdiction. HCPs are required to keep logs of each patient visit within their own practice medical records off the Platform.

2. Why do we use personal information?

We use your personal information to:

- manage our relationship with you and provide you with the information or services you request,

- create a HCP Account for HCPs interested in providing Health Services or Support Services through the Platforms,
- create a User Account for patients interested in receiving Health Services or Support Services through the Platforms,
- facilitate the delivery of Health Services or Support Services to patients by HCPs using the Platforms, including maintaining records as required by different provincial laws and HCP governing bodies;
- conduct research and evaluate development on the Webpages, including analyzing testing data to improve our services,
- communicate with you regarding inquiries for information or customer service request or employment opportunities,
- detect, prevent or investigate security breaches,
- process insurance, credit card or other payment information as agreed to on the Webpages or through the use of the Platforms,
- protect our business, and
- maintain appropriate records for internal administrative purposes.

INSIG reserves the right to aggregate and anonymize personal information (including personal health information) stored on its system and use such aggregated information as it sees fit.

3. Who do we share the personal information with?

We may share some of your personal information, including personal health information, with third-party service providers in order to operate the Webpages, the Platforms, or to provide you with the information you request. We only use service providers that ensure a comparable level of protection for your information, as provided in this Privacy Policy. Our contracts with our service providers ensure they comply with that obligation and use your personal information only for the services requested.

Exceptionally, we may collect, use or disclose personal information without your consent in the following limited circumstances:

- when the collection, use or disclosure of personal information is permitted or required by law or by regulatory proceedings,
- in an emergency that threatens an individual's life, health, or personal security,
- when we require legal advice from a lawyer,
- to protect ourselves from fraud,
- to a collection agency in order to collect our unpaid accounts, or
- to investigate an anticipated breach of an agreement or a contravention of law.

If we merge with another business, we will inform you of any impact on your personal information.

Webpage

We only share your personal information with service providers, including our affiliates, in order to operate the Webpages. This includes potentially sharing your personal information for:

- providing requested services or information,
- operating and optimizing the Webpages, or
- customer service.

Platform

We may share your personal information, including personal health information, with service providers, HCPs registered on the Platforms, and other third-parties you request (such as pharmacies or HCPs not using the Platforms). This includes sharing your personal information for:

- fraud prevention,
- payment processing via Stripe,
- providing requested services or information,
- operating the Webpages or Platforms,
- customer service, and
- facilitating the delivery of Health Services or Support Services.

4. How long do we keep personal information?

We retain personal information for as long as required to provide the services for which it was collected, otherwise, in accordance with applicable legal and regulatory requirements.

HCPs engaged by INSIG are subject to their own regulatory and professional rules which require them to retain personal health information, including personal health information they collected on the Platforms, for a *minimum* length of time. Depending on the province of where the HCP is located, the minimum retention periods which INSIG adheres to are as follows:

Province/Territory	Minimum Retention Period	Age of Majority
British Columbia	16 years from the date of last entry or 16 years from when the patient reaches the age of majority, whichever is later	19
Alberta	10 years from date of last entry or 2 years from when the patient reaches the age of majority, whichever is longer	18
Saskatchewan	6 years from the date of last entry or 2 years from when the patient reaches the age of majority, whichever is later	18
Manitoba	10 years from date of last entry or 10 years past the age of majority for minor patients	18
Ontario	10 years from the date of last entry or 10 years from when the patient reaches the age of majority or until the physician ceases to practice if	18

	some conditions are met. CPSO recommends retaining records for a minimum of 15 years.	
Quebec	10 years from date of last entry	18
New Brunswick	10 years after the patient was last seen or until age 21, whichever is longest	19
Nova Scotia	10 years after date of last entry or 10 years after the patient reaches the age of majority	19
Prince Edward Island	10 years after date of last entry or 10 years after the patient reaches the age of majority	18
Newfoundland & Labrador	10 years after last provision of service or until age 21 for patients last seen when a minor, whichever is longer	19
Yukon	6 years from date of last service or 2 years after the patient reaches the age of majority, whichever is longer	19
Northwest Territories	10 years from date of last entry or 2 years after the patient reaches the age of majority, whichever is longer	19
Nunavut	10 years from date of last entry or 2 years after the patient reaches the age of majority, whichever is longer	19

5. How do we keep personal information accurate?

We take reasonable steps to ensure that any personal information in our custody is accurate and up-to-date but we mostly rely on you to notify us of any changes to personal information you provided us.

6. How do we protect your personal information?

We use reasonable and appropriate physical, administrative and technical measures (including encryption) designed to help you secure your personal information against accidental or unlawful loss, access or disclosure. Only staff and service providers who have a legitimate business purpose for accessing the personal information collected by us are authorized to do so. Unauthorized use of personal information by anyone affiliated with INSIG is prohibited and constitutes grounds for disciplinary action.

Certain HCPs who utilize the Platforms will have additional security policies and procedures to manage individual's personal information (including personal health information).

Even though we take all necessary steps to protect your personal information, security breaches cannot be eliminated and we cannot guarantee no breach will ever occur.

7. Where do we store personal information?

All personal information INSIG collects is stored on secure servers in Canada.

However, personal information processed by our third-party service providers may be done outside of the jurisdiction where the data is stored. While being processed in another jurisdiction, such personal information is subject to that jurisdiction's laws, which may permit governmental authorities the right to access your personal information.

HCPs on the Platforms are required by their respective provincial colleges to maintain appropriate records of each patient visit. This involves them using electronic medical records or other digital services which store your personal information, including your personal health information, which may be on servers (or have back-ups) located outside of Canada.

For more information on our service providers or where we store personal information, contact us at info@insighealth.com.

8. Links to third-party sites

Our Webpages or use of the Platforms may lead you to third-party websites, including websites advertising products or services. These websites are separate and distinct from INSIG and WELL and have their own separate privacy policies. We are not responsible in any way for how these website collects, uses or discloses your personal information, so it is important to familiarize yourself with the privacy policies before providing your personal information to them.

9. Direct marketing

You may sign up to receive marketing or promotional communications from WELL. Where you have expressly consented, we may use your personal information to inform you about us and our products and our services, including promotional offers and events.

If you no longer wish to receive marketing or promotional communications from us, you can opt-out at any time by:

- using the unsubscribe feature found in our emails and other electronic communications, or
- contacting us via email at info@insighealth.com or marketing@well.company.

We remove your contact information from our distribution list as soon as you unsubscribe.

10. Consent

By registering for an account with INSIG to use the Platforms, INSIG customer HCPs obtained your consent (or the guardian's consent for a Registered Child) to collect, use or disclose your personal for the purposes of (i) delivering Health Services and Support Services to you, and (ii) registering you as a HCP on the Platforms. If you no longer wish for your personal information to be processed for these purposes, please contact privacy@well.company and stop using the Platform.

11. Artificial Intelligence

INSIG integrates with “WELL AI Voice” an ambient scribe technology as part of the HCP’s operation of the Platform. WELL AI Voice helps create a text summary of the appointment which is then reviewed and saved by the HCP as part of their ongoing records of your visit to satisfy their record keeping obligations. This technology allows the HCP to spend the appointment focused on you and your needs rather than note-taking.

INSIG has entered into a contract with the provider of WELL AI Voice to ensure that all personal information collected by such technology is protected in accordance with the terms of this Privacy Policy. INSIG may utilize additional artificial intelligence technologies in the future to help facilitate the delivery of Health Services and Support Services. Speak with your physician if you wish to opt-out of their use of these technologies.

For more information on INSIG’s use of these technologies, please contact privacy@well.company.

12. Your rights

You also have the right to:

- make a written request to access your personal information,
- request us to restrict our use or disclosure of your personal information,
- object to our use or disclosure of your personal information,
- request that we edit, but not remove, certain information (like an e-mail address),
- request that we transfer to another organization the personal information you have provided us,
- request us to delete the personal information we hold about you, and
- request we delete your account.

Contact us at privacy@well.company to exercise any of these rights. In order to confirm your identity, we may require you to answer some security questions or provide proof of identity. We will respond within 30 days. If we cannot grant your request, for example if you make an access request and providing you access would disclose personal information about another person, we will give reasons. Please note, any requests with respect to your personal health information will be redirected to the relevant HCP.

We will address all requests with equal attention.

13. Contacting us

Accountability with respect to your personal information is important to INSIG. In the event that you have any questions (including how personal information is managed by INSIG), complaints or concerns about this Privacy Policy, or if you have reason to believe that we may have failed to adhere to it, please contact us by sending an email. Questions regarding your rights and responsibilities under this Privacy Policy can be directed to our privacy officer at privacy@well.company.

If after contacting us you are still not satisfied, you have the right to file a complaint with your local privacy authority.