PRIVACY POLICY

Effective November 27, 2019

InputHealth[1] builds privacy-centric collaborative health care solutions to help clinical professionals run their practices and improve patient outcomes. In short, we run a next generation electronic health record platform that lets patients and their care teams remain connected. Your personal information, including sensitive health information, may be stored and accessed within our platform. We take this responsibility very seriously. The purpose of this Privacy Policy is to let you know that regardless of who you are or where you are located, your privacy is our priority.

Before outlining our privacy efforts, it is important for you to understand how we make money. Our Services[2] help medical professionals collect, manage, and secure patient health records. We are paid on a subscription basis by individual clinics and larger health care institutions. We do not and will never sell personal information to third parties. We are in the business of health care, not advertising. Health professionals work hard to earn your trust. We are committed to maintaining this trust by providing a secure platform built on a transparent business model.

This Privacy Policy informs you of our practices with respect to how we collect and use your personal information in connection with our Services. Together with our Terms of Service, this policy is intended to help patients, patient family members, and clinical service providers understand how we manage personal information. Many of our privacy commitments are driven by specific legal requirements. Others are best practices that we

[1] In this Privacy Policy, the words "we", "us", "our", or InputHealth refers to Input Health Systems Inc. and its affiliate companies.

[2] "Services" includes our full range of electronic health products, including without limitation, the inputhealth.com website, the Collaborative Health Record ("CHR") product, the Patient Reported Outcomes ("PRO) product, and the InputHealth Virtual product.

feel are important to improving security or the delivery of health care. Where there are trade-offs between your privacy and making information available at the point of care, we will continue to work hard to ensure that you remain equipped to provide informed consent regarding your preferences.

We will keep this policy updated as technology, privacy laws, and patient expectations evolve. This Privacy Policy is divided into the following sections, summarized as follows:

1. **Regulatory Compliance**	Privacy and regulatory compliance is determined by individual clinic requirements in the places they operate.
2. **Your Personal Information**	Our Services collect and store contact information, payment details, and highly sensitive health information. This information is used solely for health care related purposes. Please contact your health care provider to access, correct, or obtain copies of your personal information.
3. **Sharing Your Personal Information**	We share your information to operate the Services, to comply with your requests, and to support the administrative needs of health care clinics. Your information is never sold or used for advertising purposes.
4. **Medical Research**	De-identified information may be used for medical research with your express consent or for health care research performed within InputHealth using fully anonymized data sets.
5. **Security**	We apply industry-standard administrative, physical, and technical controls to secure your personal information.
6. **Data Retention**	Individual clinics select their own data retention requirements. To delete your personal information, please contact your health service provider.
7. **Links**	We include links to external sites. Once you leave the Services, your personal information is governed by the privacy policies of third-parties.
8. **How can we help?**	If you have any questions about this Privacy Policy, please don't hesitate to contact us.

REGULATORY COMPLIANCE

Our Services are an electronic platform used by regulated health professionals and their support staff. We work with individual clinics to meet their respective compliance obligations. While we do not have direct relationships with individual patients, we are committed to maintaining a secure chain of custody for personal information.

Each clinic is required to comply with health record and privacy laws in the places where they operate. This Privacy Policy does not:

1. reflect the policies or procedures of individual clinics;
2. determine what privacy compliance obligations are applicable to each clinic; or
3. establish any obligation for InputHealth to audit each clinic's compliance with applicable laws.

For clarity, our Services are an electronic medical record platform and we do not ultimately control the content or the user behaviour within the Services. Each clinic owns all electronic health records within its account and is responsible for controlling access to these records through the allocation of user credentials.

If health care professionals are dissolving a practice relationship, ownership of patient records as well as patient notification requirements will be specified by each professional's regulatory body. In the event of disputed patient records on dissolution of a health care practice, we will require a court order clarifying access and ownership.

As a platform, we still play an important role in protecting patient privacy. Where specific technical requirements exist, we work with each clinic to help them meet their compliance obligations.

YOUR PERSONAL INFORMATION

HOW PERSONAL INFORMATION IS COLLECTED

We do not require or compel patients to disclose personal information nor do we specify the information that is requested or shared. Access to our Services is provided by individual clinics pursuant to each provider's clinical, regulatory, and business requirements. Your personal information may be collected within our Services when you:

- enroll as a patient at a clinic that is using our Services;
- are a family member of a patient registered at a clinic that is using our Services;
- disclose information to health care professionals or staff at a clinic using our Services;
- are communicating with a clinic that is using our Services;
- have test results forwarded to a clinic using our Services;
- take a questionnaire, or complete a survey delivered through our Services;
- are using our website; or
- are a clinical service provider using our Services.

Our Services may collect certain types of information using tracking code, website analytics, or "cookies" that are added to your device. For example, allowing you to move within our Services without multiple-login requests. If you use your browser or device to disable the acceptance of cookies, you may experience limited access the Services.

WHAT PERSONAL INFORMATION IS COLLECTED

Your personal information stored within the Services may include:

- Contact Information: including last name, first name, address, date of birth, phone number, email address
- Demographic Information: Sex, gender identity, ethnic details, sexual preferences

- Personal Information of your family members, including contact information and relationship details (e.g. spouse, dependent child)
- Treatment Associations: health care providers and medical and health care related organizations
- Health Records: Information regarding your treatment created either by you or by one of your health care providers
- Communications: Correspondence between you and your health care providers which may include private or health-related information provided by either party
- Appointments: Scheduled calendar events, which or may not include a health care provider or medical records
- Usage information: Device usage, geographic location, IP address, access times and days.

Our Services are designed to solicit and store the minimum amount of personal information anticipated for your treatment. The Services can be customized by individual clinics and may be used to collect and store additional types of personal information for clinical use. For example, some clinical users may determine that more family history or the location of your previous residences may be useful for informing decisions at the point of care. Our Terms of Service prohibit individual clinics from collecting, storing, and sharing personal information for non-health care purposes.

WHY PERSONAL INFORMATION IS COLLECTED

Clinics use your personal information in support of your treatment and in collaboration with your other health care service providers. Your personal information is used for the following purposes:

- Your Treatment
    - Completing health questionnaires prior to your visit with a health care provider.
    - Creating a picture of your health and helping inform treatment decisions.
    - Communicating with you or your designated family members.

    - Scheduling your treatment.
    - Communicating information to other health care providers as deemed necessary for your care
- Your Management of Health Records
    - Storing your personal health record
    - Managing your upcoming appointments
    - Tracking your prescription records
- Collaborative health care
    - Helping multiple treatment providers work together to consolidate information and deliver better treatment outcomes.
    - Receiving test results and sharing test results with your other service providers.
- Improving the Services
    - Verifying and authorizing your access to the Services.
    - Providing technical support for users within subscribing clinics.
    - Analyzing the use of the Services to improve how they work.
- Medical Research
    - With express consent, collecting anonymized information for medical and health care research as described below.
- Legal Obligations
    - Our Services may be used to comply with court orders.
    - Complying with certain professional regulatory requirements, insurance documentation, or tax obligations.

ACCESSING AND MODIFYING YOUR PERSONAL INFORMATION

We believe in the right of individuals to access their personal information. If you are a patient or patient family member and would like to access your health records, please contact your health service provider that is using our Services. Health records are owned by individual clinics and your right to access your personal information is through these

clinics. Access to health records is governed by individual clinic policies as well as by privacy and health record laws where each clinic operates.

We also believe in the right of individuals to modify, correct and update their personal information. In certain contexts, patients may use our Services to update their personal information, but we cannot control how that data is managed by individual clinics. If you feel that there is incorrect data in your account, please contact your health services provider that is using our Services.

ELECTRONIC COMMUNICATIONS

If you have registered as a patient, a patient family member, or as a designated proxy at a health services provider using our Services, you have "opted-in" to receiving our electronic communications. Our Services support multiple notification methods. You may "opt-out" at any time by using the unsubscribe link in the footer of our emails or by contacting your treating clinic to change your communication preferences.

SHARING YOUR PERSONAL INFORMATION

InputHealth does not and will not sell your personal information. Your information will also never be used for advertising purposes. By default, your personal information is accessible within individual clinics who are using our Services. There are limited circumstances in which your personal information may also be shared with third parties:

COLLABORATIVE HEALTH CARE

Sharing information with your external health care providers, including specialists, testing/diagnostic facilities, hospitals, and associated clinics. For example, if you are referred to an ophthalmologist for an eye issue as well as a diagnostic clinic for a blog test, the Services would provide these third-party professionals with access to your information. Their contributed records would subsequently be added to your health records.

EXPRESS PERMISSION

Circumstances in which you explicitly opt-in to share your personal information. For example, if you have diabetes, you may be asked whether you would agree to share certain medical information in order to participate in a diabetes registry.

NETWORK

Our Services live in the cloud. This means that they are running on a web of network exchanges and data centers. We work with carefully selected network infrastructure providers to deliver the Services. While encryption shields the Services from access, your personal information is held within their networks in an encrypted form.

BILLING

Your health care provider may need to share your personal information for payment purposes, whether to a provincial health ministry, your health maintenance organization,

or another insurer. Similarly, certain information may be disclosed in the context of payment processing by bank or credit card.

APIs

Our Services integrate with third party applications in order to fulfill certain functions. For example, our Services may integrate with separate billing applications so that clinics don't need to use two different programs. These integrations occur through application programming interfaces (APIs) in our Services. We take great care to ensure that any third-party integrating with our Services is bound by privacy and security commitments consistent with this Privacy Policy. However, the use of third party applications will be governed by the privacy policies and terms of service of such third party providers and we cannot guarantee how personal information in their control will ultimately be managed.

BUSINESS TRANSACTIONS

In the event InputHealth or your clinic undergoes a business transition, such as a merger, acquisition by another company, or sale of all or a portion of its assets, your personal user information may be included within the assets transferred. Where such business transactions are anticipated or completed, we will comply with the applicable privacy obligations in the jurisdiction in which your clinic operates.

LEGAL REQUIREMENTS AND EMERGENCY SITUATIONS

Your personal information may be disclosed as required by law, whether to comply with a judicial proceeding, court order, or legal process served on our Services.

We may also share your personal information in the context of an emergency, as requested by a public authority, if in our judgment it appears that there is an imminent danger to an individual or group and that a court order will not be practical in the circumstances.

MEDICAL RESEARCH

Our Services are purpose-built for improving health care outcomes at the point of care. This clinical work is ultimately informed by research. The aggregate data generated by our Services is exceptionally valuable for supporting these research efforts. While many platforms choose to sell de-identified data for research purposes, we do not feel that this is consistent with your privacy being our priority. De-identified data is not good enough if that data is being shared with third-party researchers where there is always a potential risk for re-identifying the data by combining it with other information. We have taken a different approach. We will only use de-identified data where:

1. You have provided express consent after being informed of the full scope of the research; or
2. Anonymized data is used for research performed within InputHealth.

This second option is important to us because it ensures that a) privacy obligations are never outsourced to a third party and b) we can continue to expand our efforts for improving patient care beyond the Services themselves.

For example, we may de-identify a large number of patient records to help answer a question like “How can a clinic staff adequately for flu season?” by looking at seasonal patient volumes. Such research would only be completed in situations where our researchers are confident that the data being used is truly anonymous and where individuals cannot be re-identified.

SECURITY

There is no privacy without security. Our Services are hosted with leading enterprise cloud infrastructure providers. We also perform industry-standard security audits to

monitor our performance, including being SOC2 Type II certified and ISO 13485:2016 compliant.

We do not disclose the technical details of our security efforts in order to better protect the Services from targeted attack. In general terms, we apply industry-standard administrative, physical, and technical security controls. Where we work with third parties, security is enforced through both technical and contractual means.

DATA RETENTION

Each health care provider is subject to the electronic health record regulations in the places in which they operate. By default, our Services retain records indefinitely so long as the subscribing clinic remains a paying user. If your treating clinic has closed their account or failed to make timely payments, your personal information may be deleted after a specified number of days pursuant to our Data Retention Policy.

Should it be necessary for legal purposes to dispose of your personal health information, the health care provider can contact us (as below) to request secure and complete disposal of your health information. We are unable to delete your personal information without consent from your health care provider.

LINKS

For your convenience, we may provide links to certain third-party websites or referrals to certain third parties' products or services. If you choose to visit a third party's website or use its products or services, please be aware that the third party's privacy policy, and not the InputHealth privacy policy, will govern your activities and any information you disclose while interacting with the third party.

HOW CAN WE HELP?

PATIENT PRIVACY CONCERNS

If you are a patient or designated proxy of a patient and have concerns about how your treating clinic is handling your personal health information, you must contact the appropriate individual within your treating clinic, such as their privacy officer or clinic manager.

QUESTIONS

For all other questions or concerns about this Privacy Policy or our privacy practices, please feel free to contact us at privacy@inputhealth.com.