# Telemed Privacy Policy

Telemed Innovations Inc ("**Telemed**", "**We**", "**Us**") has created this Privacy Policy ("**Policy**") in order to set out how we collect, use, and disclose personal information through the Telemed.ca Platform and related Services (as those terms are defined in our Terms of Service). Telemedmd.ca is a Patient relationship management software-as-a-service platform which allows registered CPSO doctors ("**Physicians**") to connect, treat and provide health care consulting through OHIP and private services to patients across Ontario ("**Patients**").

The privacy of our users is of great importance to us. By visiting our website located at **www.telemedmd.ca** (the "**Website"**) or using the Services in any manner, you acknowledge that you accept the practices and policies outlined in this Policy and you hereby consent to the collection, use and disclosure of your personal information in accordance with this Policy.

## 1 WHAT DOES THIS POLICY COVER?

This Policy covers our collection, use and disclosure of information about identifiable individuals ("**Personal Information**"). This Policy does not apply to the practices of companies that we do not own or control. We do not knowingly collect or solicit Personal Information from anyone under the age of 18 or knowingly allow such persons to register for the Services. Physicians are responsible for maintaining their own privacy policies governing the collection, use and disclosure of Patient Personal Information.

## 2 COLLECTION AND USE OF PERSONAL INFORMATION AND OTHER DATA

### 2.1 Telemed Account Information

In order to use certain aspects of the Services, users may be required to have a valid Telemed account to log in to the Platform ("**Account**"). When you register for the Services, Telemed collects Your Account username and password in order to authenticate Your Account access and provide You with access to the Services.

### 2.2 Patient Information

Patients will be required to provide a date of birth and residential address. In order to allow Patients to use the Services, Telemed will also collect Patients medical information and insurance information (collectively, "**Patient Data**"). This information is stored in the Platform, as identified through the Platform, to allow the physician to verify the Patient's identification, bill the Patient's insurance company and ship products ordered to the Patient.

Telemed collects the Patient's medical history in order to allow Patient's to keep track of consultations done and easily request medical information.

### 2.3 Demographic Data

All Patient Data collected by the Platform is aggregated and anonymized by Us to create aggregate statistical data ("**Statistical Data**") which we use to provide insights to Physicians and our other clients, including age of users, patients' average distance from pharmacies, how frequently Patients use the Platform. The Statistical Data does not include any Personal Information.

### 2.4 Usage Data

Telemed may also collect certain information users of the Website and Services, such as Internet addresses, time spent logged into the Services and other usage data. This information is logged to help diagnose technical problems, and to administer our Website and Services in order to constantly improve the quality of the Service. Telemed uses the usage data that we collect to provide the Services and to continuously improve the Services.

### 2.5 Surveys

Telemed may collect Personal Information that our Physicians and their Patients provide in a survey prompted by Telemed and/or one of its partners, including, but not limited to, Personal Information, preferences, and medical information, for the purpose of better understanding the needs of Physicians and Patients. Telemed will share only anonymized, aggregated survey results with its partners.

### 2.6 Cookies

Technologies such as cookies, beacons, scripts and tags are used by us and our third party partners. These technologies are used in analyzing trends, administering the website, tracking users' movements around the website, and gathering demographic information about our user base as a whole. We may receive reports based on the use of these technologies by these companies on an individual and aggregated basis. Various browsers may offer their own management tools for removing these types of tracking technologies.

Standing alone, cookies do not identify you personally. They merely recognize your browser. Cookies come in two flavors: session and persistent-based. Session cookies exist only during an online session. They disappear from your computer when you close your browser software or turn off your computer. Persistent cookies remain on your computer after you've closed your browser or turned off your computer. They include such information as a unique identifier for your browser.

Telemed uses session cookies containing encrypted information to allow the system to uniquely identify you while you are logged in. This information allows Telemed to process your online transactions and requests. Session cookies help us make sure you are who you say you are after you've logged in and are required in order to use the Service.

Telemed uses persistent cookies that only Telemed can read and use, to identify the fact that you are a Telemed user. We are especially careful about the security and confidentiality of the information stored in persistent cookies. Users who disable their web browser's ability to accept cookies will be able to browse our Website but may not be able to use all features of our Service.

Our third party partners also employ clear gifs (a.k.a. Web Beacons/Web Bugs), images, and scripts that help them better manage content on our site. We do not tie the information gathered to our Patient Data.

## 3 STORAGE LOCATION AND TRANSFER OF PERSONAL INFORMATION

Telemed stores its data, including Personal Information, on servers located in Canada. By submitting information, you agree to this transfer, storing or processing of your Personal Information in Canada. You acknowledge and agree that your Personal Information may be accessible to law enforcement and governmental agencies in Canada under lawful access regimes or court order.

## 4 DISCLOSURE OF PERSONAL INFORMATION WITH THIRD PARTIES

### 4.1 Disclosure of Statistical Data

Telemed discloses aggregate Statistical Data to its partners and Physicians, and other third parties, who may use the data for business purposes. This information does not include any Personal Information or otherwise identify any individual Patients.

### 4.2 Service Providers and Business Partners

We may from time to time employ other companies and people to perform tasks on our behalf and need to share Patient Data with them to provide the Services to you. Unless we tell you differently, such third parties do not have any right to use the Personal Information we share with them beyond what is necessary to assist us. This includes third party companies and individuals employed by us to facilitate our Services, including the provision of maintenance services, database management, Web analytics and general improvement of the Services, and businesses who engage our Services (to the extent provided for above).

### 4.3 Business Transfers

If we (or substantially all of our assets) are acquired, or if we go out of business, enter bankruptcy, or go through some other change of control, Personal Information may be made available or otherwise transferred to the new controlling entity, where permitted under applicable law.

### 4.4 With Your Consent

If we need to use or disclose any Personal Information in a way not identified in this Privacy Policy, we will notify you and/or obtain your express consent as required under applicable privacy laws.

## 5 RETENTION

We will keep your Personal Information for as long as it remains necessary for the identified purpose or as required by law, which may extend beyond the termination of our relationship with you. Generally, Telemed uses reasonable efforts to delete Personal Information within 30 days of a use deleting their Account. However, we may retain certain data as necessary to prevent fraud or future abuse, or for legitimate business purposes, such as analysis of aggregated, non-personally-identifiable data, account recovery, or if required by law. All retained Personal Information will remain subject to the terms of this Privacy Policy.

## 6 ACCESS, CORRECTION AND ACCURACY

You have the right to access the Personal Information we hold about you in order to verify the Personal Information we have collected in respect to you and to have a general account of our uses of that information. Upon receipt of your written request, we will provide you with a copy of your Personal Information, although in certain limited circumstances, and as permitted under law, we may not be able to make all relevant information available to you, such as where that information also pertains to another user. In such circumstances we will provide reasons for the denial to you upon request. We will endeavor to deal with all requests for access and modifications in a timely manner.

We will make every reasonable effort to keep your Personal Information accurate and up to date, and we will provide you with mechanisms to update, correct, delete or add to your Personal Information as appropriate. As appropriate, this amended Personal Information will be transmitted to those parties to which we are permitted to disclose your information. Having accurate Personal Information about you enables us to give you the best possible service.

## 7 CHANGES TO THIS POLICY

We may amend this Policy from time to time. Use of Personal Information we collect is subject to the Policy in effect at the time such information is collected, used or disclosed. If we make material changes or changes in the way we use Personal Information, we will notify you by posting an announcement on our Website or Services or sending you an email prior to the change becoming effective. You are bound by any changes to the Policy when you use the Website after such changes have been first posted.

## 8 BREACH MANAGEMENT

A security event is an observable occurrence relevant to the confidentiality, availability,integrity, or privacy of company controlled data, systems or networks. A security incident is a security event which results in loss or damage to the confidentiality,availability, integrity, or privacy of company controlled data, systems or networks.

### 9.1 Reporting

If a Telemed Innovations Inc employee, contractor, user, or customer becomes aware of an information security event or incident, possible incident, imminent incident, unauthorized access, policy violation, security weakness, or suspicious activity, then they shall immediately report the information using one of the following communication channels:

- Email privacy@telemedmd.ca information or reports about the event or incident

Reporters should act as a good witness and behave as if they are reporting a crime. Reportsshould include specific details about what has been observed or discovered.

### 9.2 Severity

Telemed Innovations Inc security and IT team shall monitor incident and event tickets and shallassign a ticket severity based on the following categories.

#### S3/S4 - Low and Medium Severity

Issues meeting this severity are simply suspicions or odd behaviors. They are not verified and require further investigation. There is no clear indicator that systems have tangible risk and do

not require emergency response. This includes lost/stolen laptop with disk encryption, suspicious emails, outages, strange activity on a laptop, etc.

### S2 - High Severity

High severity issues relate to problems where an adversary or active exploitation hasn't been proven yet, and may not have happened, but is likely to happen. This may include lost/stolen laptop without encryption, vulnerabilities with direct risk of exploitation, threats with risk or adversarial persistence on our systems (e.g.: backdoors, malware), malicious access of business data (e.g.: passwords, vulnerability data, payments information), or threats that put any individual at risk of physical harm.

### S1 - Critical Severity

Critical issues relate to actively exploited risks and involve a malicious actor. Identification ofactive exploitation is required to meet this severity category.

## 9.4 Escalation and Internal Reporting

*S1 - Critical Severity:* S1 issues require immediate notification to the IT department (it@telemedmd.ca and VP of Operations). After which communication will be sent over to the Engineering team to begin determining next steps to contain the S1 breach and further issuesrelated to the initial incident reported.

*S2 - High Severity*: A high alert ticket must be completed and the appropriate manager (see S1above) must also be notified via email with a reference to the ticket number.

*S3/S4 - Medium and Low Severity*: A low alert ticket must be created and assigned to theappropriate department for response.

## 9.5 Documentation

All reported security events, incidents, and response activities shall be documented in a ticketsystem located through our internal security/ incident share point folder.

A root cause analysis may be performed on all verified [S1] security incidents. A root cause analysis report shall be documented and referenced in the incident ticket. The root cause analysis shall be reviewed by the IT Manager who shall determine if a post-mortem meeting willbe called.

## 9.6. Incident Response Process

For critical issues, the response team will follow an iterative response process designed to investigate, contain exploitation, eradicate the threat, recover system and services, remediatevulnerabilities, and document a post-mortem with the lessons of an incident.

### Summary

- Event reported
- Triage and analysis
- Investigation
- Containment & neutralization (short term work)
- Recovery & vulnerability remediation
- Hardening & Detection improvements (lessons learned, long term work)

# 9 BUSINESS CONTINUITY & DISASTER RECOVERY PLAN

In the event of a major disruption to production services and a disaster affecting the availability and/or security of the Telemed Innovations Inc office, senior managers and executive staff shall determine mitigation actions. A disaster recovery test, including a test of backup restoration processes, shall be performed on an annual basis. Continuity of information security shall be considered along with operational continuity. If the Telemed Innovations Inc office becomes unavailable due to a disaster, all staff shall workremotely from their homes or any safe location.

## 9.1 Communications and Escalation

Executive staff and senior managers should be notified of any disaster affecting Telemed Innovations Inc facilities or operations. Communications shall take place over any available regular channels including [MicrosoftTeams, Microsoft Office 365, AVAROS EMR and phone). Key contacts shall be maintained on the on-call schedule and key contacts:

### Roles and Responsibilities

| Role | Responsibility |
|---|---|
| **IT Manager** | **The IT Manager shall lead BC/DR efforts to mitigate losses and recover the corporate network and information systems.** |
| **Departmental Heads** | **Each department head shall be responsible for communications with their departmental staff and any actions needed to maintain continuity of their business functions. Departmental heads shall communicate regularly with executive staff and the IT Manager.** |
| **Managers** | **Managers shall be responsible for communicating with their direct reports and providing any needed assistance for staff to continue working from alternative locations.** |
| **VP of Operations** | **The VP of Operations, in conjunction with the CEO and CFO shall be responsible for any external and client communications regarding any disaster or business continuity actions that are relevant to customers and third parties.** |
| **VP of Engineering** | **The VP of Engineering, in conjunction with the VP of Operations, shall be responsible for leading efforts to maintain continuity of Telemed Innovations Inc services to customers during a disaster.** |
| **Chief HR Officer** | **The CHRO shall be responsible for internal communications to employees as wellas any action needed to maintain physical health and safety of the workforce.**<br>**The CHRO shall work with the IT Manager to ensure continuity of physical security at the Telemed Innovations Inc office.** |

Strategy for maintaining continuity of services can be seen in the following table:

| KEY BUSINESSPROCESS | CONTINUITY STRATEGY |
|---|---|
| **Customer (Production) Service Delivery** | **Rely on AWS availability commitments and SLAs** |
| **IT Operations** | **Not dependent on HQ. VPN is redundant between HQ and Colo.Critical data is backed up to alternate locations.** |
| **Email** | **Utilize Office 365 Email and its distributed nature, rely on Microsoftstandard service level agreements.** |
| **Finance, Legal and HR** | **All systems are vendor-hosted SaaS applications.** |
| **Sales and Marketing** | **All systems are vendor-hosted SaaS applications.** |

## 10 CONTACT US

If you have any questions, concerns or suggestions about our privacy practices, please contact our Chief Compliance Officer. Please include your name and contact information if you would like us to respond to you.

Maple Corporation
ATTN: Dhrumil Mehta - Chief Compliance Officer
it@telemedmd.ca
(888)-350-2323
Unit 5 - 2200 Dundas St E, Mississauga ON L4X 2V3