HealthStream

by tekasco

Privacy and Data Security Policy

Privacy Policy

GENERAL STATEMENT

Tekasco Ltd, (the "Company", "we", "us" or "our"), provides the website located at www.tekasco.co.uk (the "Website") to support healthcare application or website providers by providing their end users with access to certain third party applications, programs, and/or devices that the end users may elect to connect to using the Website (collectively, the "Service").

This privacy policy ("Privacy Policy") applies to the Website and to the Service and describes the information we collect, how we use it, with whom we share it.

The Company controls, owns, and manages the information collected on the Website and by and through the Service and may use the information to build and grow our business in the manner as described in this Privacy Policy.

THE INFORMATION WE COLLECT

In this section, we provide you with details about some of the information we currently collect about users of our Website and of our Service (collectively, "User Data").

- User Key. Your healthcare application or website (each, a "healthcare portal") provides us with a user key (the "User Key") that identifies you as a registered member of the healthcare portal. This allows us to verify that we are authorized to provide you with the Service.
- Personal Information. We may collect information by which you may be personally identified, such as name, address, e-mail address and/or telephone number, and information required for the payment of goods or services that you order from us, including credit card numbers, security codes and other financial information ("Personal Information").
- Program Data. We will collect User Data produced by your use of, or uploaded by you to, certain integrated third party applications, programs and/or devices that you may elect to use in connection with the Website and/or the Service ("Programs"). We provide you with information about Programs that connect with the Service. These Programs typically have features that collect and store data and/or other information about you and/or permit you to upload the same to your user account with the Program. When you choose to integrate these Programs with the Service,

they will be able to provide us with access to some or all of that data and/or other information (the “Program Data”).You should review information from the Programs, including their privacy statements and terms of use, prior to using them or allowing them access to any information about you. These Programs are not sold, designed or manufactured by the Company. All support for these Programs is provided by the Program provider. The Company does not warrant and is not responsible for the quality, use or operation of the Programs and your use of any such Programs is governed by separate terms of use and privacy statements by the Program provider. We then share the Program Data with your healthcare portal provider.

- Company Applications. We will collect health and wellness user data produced by your use of, or uploaded by you to, Company’s applications that you may elect to use in connection with the Website and/or the Service (“Company Apps”). We provide you with information about Company Apps that connect with the Service or that are used in connection with the Website and/or the Service. These Company Apps have features that collect and store data and/or other information about you, including health and wellness user data. When you choose to access or use the Company Apps, they will be able to provide us with access to some or all of such data and/or other information (the “Company App Data”).
- Cookie Information. “Cookies” are small files that a site or its service provider transfers (if you allow) to your computer, mobile phone or other device with a web browser and data storage capability that enables the sites or service provider’s systems to recognize your browser and capture and remember certain information. Most web browsers will accept cookies by default, but they can be set to reject cookies, either from all websites or from specific sites. You can also manually delete cookies from your web browser. These options are generally set through a “Privacy” setting in your browser setup, but you should know that in some cases blocking, rejecting or deleting cookies may impact your ability to use the Website or the Service. We use cookies to help remember you as a user. We may also use cookies in the future in other ways to provide and to improve the Service, to make the Website easier to use, or for other similar purposes.

- Navigational Information. We may collect and use information and data from you when you are using the Service and/or Website through the standard operation of our Internet servers. Information collected from you may include user Internet Protocol (IP) addresses, browser type and version, domain names, referring/exit pages, devices, operating system, date/time stamp, click stream data and anonymous statistical data regarding your use of the Service and/or Website. For example, we can tell which Internet Service Provider our users use, but not the names, addresses or other information that would allow us to identify users. We use this information to analyse trends, to administer and to improve the Service and Website, to track users' movements around the Website and to gather demographic and other aggregate information (as described in more detail below) about our user base as a whole.
- Clear Gifs. We may also employ a software technology called "clear gifs" (also known as "web beacons" or "web bugs") that helps us better manage content on the Website by providing us feedback as to what content is effective. Clear gifs are tiny graphics with a unique identifier, similar in function to cookies, and are used to track the online movements of users. In contrast to cookies, which are stored on your web enabled device's hard drive, clear gifs are embedded invisibly on a website page, web-based document or email message and are about the size of the period at the end of this sentence. Clear gifs may be used in our HTML-based emails to confirm receipt of, and response to our emails, including those that you forward to other recipients.
- Site Information. Due to communications standards on the internet, when you visit the Website, we typically automatically receive the URL of the site from which you came and the site to which you are going when you leave our Website. We also receive the internet protocol address of your computer (or the proxy server you use to access the Internet), your computer operating system and type of web browser you are using, email patterns, your mobile device and mobile operating system, as well as the name of your ISP or your mobile carrier. We may also receive location data passed to us from third-party services or GPS-enabled devices that you have enabled.

- Site Analytics. We may analyse your use of the Website and/or Service with third party software that allows us to monitor and record your navigation and usage activities, in order to better customize and improve our Website, Service and other products.
- Aggregated User Data. In an ongoing effort to better understand and serve the users of the Website and the Services, we may analyse the User Data and conduct research on demographics, interests, behaviour and other topics based on User Data of our end users, including you, that is provided to, collected by or otherwise available to us. We use the User Data from you and other users and reformat, supplement, compile, analyse and/or aggregate these datasets together to create what we term "Aggregated User Data." We use such Aggregated User Data for product development and to improve our products and services and may share certain components of this User Data and/or Aggregated User Data with our affiliates, agents and business partners as described below.

HOW WE USE THE INFORMATION WE COLLECT

- Sharing with Healthcare Portal Providers. We share the Program Data we collect from the Programs with your application provider.
- Outside Contractors. We may employ independent contractors, vendors, suppliers and other third parties to support our services and products (including the Website and the Service), such as hosting, monitoring and maintaining the Website and/or the Service, administering or monitoring emails, analysing our users' preferences, developing or improving applications for the Website and the Service and providing other related services. These parties may sometimes have limited access to User Data, while providing products or services to us. Access to your User Data by these parties is limited to the information that we determine, in our sole discretion, to be reasonably necessary for them to perform their function for us. While we will seek to require outside contractors to protect the privacy of your User Data under privacy policies or confidentiality agreements that are at least as protective of your User Data as this Privacy Policy, and will not authorize them to use your User Data except for the express purpose for which it is provided, we do not bear any responsibility for any actions or policies of these parties.

- Business Transfers. We may also disclose and/or transfer your User Data to third parties in connection with a corporate transaction, such as a merger, acquisition by another company or sale or other transfer of all or a portion of our business or assets.
- Lawful requests by public authorities. We will disclose personal information in response to lawful requests by public authorities, including when there is a need to meet national security or law enforcement requirements.

REVIEWING, UPDATING AND DELETING YOUR INFORMATION

EU individuals have the right to access their personal data. We provide your healthcare portal provider with the capability to review, update and delete your User Data, including your personal health data. We require your permission before any of your User Data (including your personal data) is accessed, retrieved or made available to your healthcare portal provider. You may change your level of permission at any time to enhance or limit the collection, use, and/or disclosure of your User Data (including your personal data). In addition, we provide your healthcare portal provider the ability to allow you to revoke permission to access your User Data (including your personal data) and will permanently delete any records that we have of your User Data (including your personal data).

LINKS AND ADVERTISING

We do not advertise on our Website or through the Service and do not provide any User Data to advertisers or otherwise to third parties for the purpose of advertising or marketing. From time to time, the Website may contain hyperlinks ("Links") to third parties, including third party providers of certain Programs. Such Links are for your reference only, and we neither control the privacy policies of such linked websites nor are we liable or responsible in any way for the use of any personally identifiable information that you may provide such sites. We recommend that you remain aware when you leave the Website and review the terms of use and privacy policies of each linked website.

You should also be aware that if you voluntarily disclose personally identifiable information in an email or other communications with any third party listed on the Website or in other materials, that information, along with any other information disclosed in your communication, can be collected and correlated and used by such third parties and may result in your receiving unsolicited messages from other persons. Such collection, correlation, use and messages are beyond our control.

SECURITY

- Steps we take to keep your information secure. The security of your User Data is important to us. We have put in place commercially reasonable physical, electronic, and managerial procedures to safeguard and secure User Data from unauthorized access, including as set forth in more detail in our Company Security Policy.
- Risks inherent in sharing information. Notwithstanding our commitment to protect your information, you should be aware that there is always some risk involved in transmitting information over the internet. In addition to the risk that the employees, contractors and others subject to our Security Policy may fail to follow required procedures, there is also some risk your or our network and/or security systems could be circumvented or breached, including by third parties who use our Website or Service in order to do so. As a result, while we strive to use commercially reasonable means to protect your User Data, we cannot ensure or warrant the security and privacy of your User Data or any other information you transmit to us, or of your or our network and/or security systems. If you have any questions regarding the security of the Website or the Service, you can contact our privacy team at the email address set forth above.

CHILDREN'S POLICY

The Website and the Service are for general audiences and neither is directed toward those under 18 years of age. We do not knowingly collect Personal Information from children under 13 without parental consent. If you become aware that a child has provided us with Personal Information, please contact our Privacy Officer at the email address in the Contact Information section. If we become aware that a child under 13 has provided us with Personal Information, we will take steps to remove such information and terminate the child's account.

ENFORCEMENT

We regularly review our compliance with this Privacy Policy. Please let us know of any questions or concerns you have regarding this Privacy Policy or our compliance with this Privacy Policy by contacting our Privacy Officer at the email address in the Contact Information section. When we receive formal written complaints, it is our policy to contact that complaining user regarding his/her concerns. We will cooperate with the appropriate regulatory authorities to resolve any complaints regarding the transfer of personal data that cannot be resolved between the Company and an individual or entity.

Please remember that your use of the Website and the Service is also governed by our Terms, which are available separately.

CHANGES TO THIS PRIVACY POLICY

We may revise this Privacy Policy from time to time. When we do so, we will revise the “Updated” date at the top of this Privacy Policy. Any such change will be effective immediately upon posting on the Website. You are responsible for checking the Privacy Policy for such changes.

CONTACT INFORMATION

If you have questions or complaints regarding this Policy or our practices, please contact the Company at:

Tekasco Ltd
Privacy Officer
5 Goggbridge Lane
Warwick, CV34 6JE
United Kingdom
info@tekasco.co.uk

Data Security Policy

DATA SECURITY POLICY IN BRIEF

Tekasco Ltd. (“Tekasco”) focuses on security from the ground up. Our Data Centers, managed by Microsoft Azure, are SAS 70 Type II certified, SSAE16 (“SOC 2”)/HIPAA/HITRUST Compliant, and feature proximity security badge access and digital security video surveillance. Our server environment can only be accessed via Two-factor Authentication over secure channels. We run monthly Vulnerability Assessments on our production environment. Additionally, all access to our web portal is secured over HTTPS using at least TLSv1.2 cryptographic protocols with AES-256 encryption. Only directors of the business have access to client data.

DEFINITION OF TERMS & SYSTEM USERS:

Client — A customer of Tekasco.

User — An individual with access to a HealthStream Application.

Member — A Client User whose account is provisioned through Client’s Web Portal. A Member cannot login or otherwise access any HealthStream Application directly.

Developer — A User that can create vendor applications in HealthStream for the purpose of integrating mobile health applications and/or devices.

DATA CENTER AND HARDWARE

All Tekasco HealthStream application and database servers are physically managed by Microsoft Azure in secure data centres within the United Kingdom and United States. Our security procedures utilise industry best practices from sources including The Centre for Internet Security, Microsoft, Red Hat and more. All data centre facilities are certified SOC 2/HIPAA/HITRUST Compliant and have 24/7 physical security of data centres and Network Operations Centre monitoring.

Physical Security

Microsoft manages the physical access to the data centres. They control both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Tekasco employees do not have access to physical server hardware.

Data Access and Server Management Security

Tekasco uses multi-factor authentication to access our hosting environment. Only directors of Tekasco can access the server network.

Environmental Safeguards

All Azure data centres are equipped with automatic fire detection and suppression (either wet-pipe, double-interlocked pre-action, or gaseous sprinkler systems), climate and temperature controls, fully redundant uninterruptible power supplies, and generators to provide back-up power for each physical site.

DATA STORAGE AND BACKUPS

All Member Data stored in our Tekasco HealthStream system is encrypted at rest using AES-256 encryption. Tekasco maintains numerous full backups of all Client data. These backups are stored in a geographically and logically separated environment.

Client Data Policies

Client data includes data stored by Clients in Tekasco HealthStream applications, information about a Client's usage of the application, data instances in the Customer Relationship Management system to which we have access, or data that the Client has supplied to us for support or implementation. When managing Client Data, we consider the following:

1. Client Data is not to be disclosed outside of Tekasco, except to the Client who owns the data or to a partner who has been contracted by the Client to manage or support their account.
2. Client Data should only be shared using a secure transmission methods and protocols. Approved transmission methods include the emailing of encrypted files or use of a Client-provided secure transfer method.
3. Client Data must never be stored outside of the Tekasco HealthStream Application unless required for a specific need and with executive level approval. If there is a need to archive Client Data (for example, data provided by a Client during implementation or training), the data should be stored on a central file server in a secure manner and deleted from any personal computers immediately. This need includes report exports, contact lists, presentations that contain Client information, and Client agreements.
4. Client Data should only be accessed on a need-to-know basis. Specifically, a Client's account should only be accessed to provide support, troubleshoot a problem with that account, or for supporting the system.
5. Client Data should never be changed without the explicit permission of the Client, except for the need to address and repair data quality issues.

Destruction of Server Data

In order to maintain system integrity, Client Data that has outlived its use is retained for no more than 60 days before it is destroyed. The data may remain in our backup files for up to fourteen (14) months, as it is our policy to maintain weekly backups for a minimum of 52 weeks before those backups are destroyed. De-identified activity data from Members may be stored in perpetuity for future analysis.

Incident Response

Tekasco security administrators will be immediately and automatically notified via email if implemented security protocols detect an incident. All other suspected intrusions, suspicious activity, or system unexplained erratic behaviour discovered by administrators, users, or computer security personnel must be reported to a security administrator within one (1) hour.

Once an incident is reported, security administrators will immediately begin verifying that an incident occurred and the nature of the incident with the following goals:

6. Maintain or restore business continuity
7. Reduce the incident impact
8. Determine how the attack was performed or the incident happened
9. Develop a plan to improve security and prevent future attacks or incidents
10. Keep management informed of the situation and prosecute any illegal activity

Determining the Extent of an Incident

Security administrators will use forensic techniques, including reviewing system logs, looking for gaps in logs, reviewing intrusion detection logs, interviewing witnesses and interviewing the incident victim to determine how the incident was caused. Only authorized personnel will perform interviews or examine evidence, and the authorized personnel may vary by situation.

Notifying Clients of an Incident

Clients will be notified via email within one (1) hour upon detection and confirmation of any incident that compromises access to the service, compromises data, or otherwise affects Users. Clients will receive a status update every four (4) hours and upon incident resolution.

Application Security

All data transfer and access to Tekasco applications will occur only on Port 443 over an HTTPS connection using at least TLSv1.2 cryptographic protocols with AES-256 encryption.

System Updates and Security Patches

As a hosted SaaS solution, we regularly improve our system and update security patches. No Client resources are needed to perform these updates. Non-critical system updates will be installed at predetermined times. Critical application updates are performed ad hoc using rolling deployment to maximize system performance and minimize disruption. All updates and patches will be evaluated in a virtual production environment before implementing.

Vulnerability and Security Testing

Tekasco performs Vulnerability Assessments and creates security reports of our production environment once a quarter. Tekasco also perform external penetration testing by a third party on at least an annual basis. Additional internal security testing is performed on the testing environment before code is checked into a master repository.

Member Login and Session Security

Members are not able to directly login to Tekasco's HealthStream application. All Member logins and sessions are authenticated via a secure access token.

Application Password Management

All Tekasco passwords must have at least twelve (12) characters with at least one number, one lowercase letter, one uppercase letter and one special character.

Disaster Recovery

Tekasco maintains data stores mirrored across multiple geographic availability zones in Azure within the United Kingdom. While most data stores are kept in sync in near real-time, some are updated every six (6) hours. In a disaster situation, the full Tekasco HealthStream platform will be recreated and available in a different region within six (6) hours of disaster declaration.

PHI Handling Policy

All Tekasco staff members are made aware of relevant external regulations as part of their onboarding and training process, and all staff who may encounter PHI are trained on our PHI handling processes.

Tekasco expects professional integrity of our collaborators, Clients and partners providing PHI to us and will assume that they have obtained the Member's consent to use their data in this way.

Where a Business Associate Agreement or similar contract relating to PHI is in place, staff members work under the terms of that agreement. Where no such agreement exists, the Tekasco PHI handling policy and process are followed.