HIPAA Compliance

HIPAA §164.312 Technical Safeguards and §164.308(a)(7)(ii) Administrative Safeguards

Tuyu is compliant with all of the below.

First, our data center locations (Amazon Web Services) are fully HIPAA compliant, in the context of the general categories and areas:

- Firewall
- Web Application Firewall (WAF)
- Two-Factor Authenticated VPN
- Antivirus / Anti-malware
- Intrusion Detection
- Vulnerability Assessment & Notification
- Event Management
- Continuous Audit
- Change Control
- Patch Management
- Project Management
- Server Configuration and Management
- Transparent Database Encryption (TDE)

§164.312 Technical Safeguards

Standard: Person or entity authentication. Verify person / entity seeking access to electronic protected health information is the one claimed.

- Unique user IDs
- Access is restricted by e-mail address
- Email address validation is required through the use of a confirmation link
- All passwords are encrypted during client-server communications and when accessing the website using a web browser or mobile device
- Ability to enforce strong password / master password creation
- Users are able to change their password
- Passwords can be reset but not recovered

Access Control

§164.312 Technical Safeguards

(a)(1)Standard: Access control. Allow access only to those persons or software programs that have been granted access rights.

(a)(2)(i)Unique user identification (Required). Assign a unique name and/or number for identifying and tracking user identity.

(a)(2)(iii)Automatic logoff (Addressable). Terminate an electronic session after a predetermined time of inactivity.

(a)(2)(iv) Encryption and decryption (Addressable). Encrypt/decrypt electronic protected health information.

- Administrative SoD (Separation of Duties) with multiple levels of access control and administrator privileges
- Administrators cannot access accounts of other administrators
- Administrators can set disk space, maximum file storage, and maximum bandwidth or users, user groups, or sites
- Option to require strong / master password for all file transfers
- All files are automatically deleted after a configurable time period
- Option to restrict the number of times a file can be downloaded
- Restrict ability to send files by user, group, email address domain, or site

Privacy

§164.312 Technical Safeguards

(e)(1) Standard: Transmission Security

(e)(2)(ii) Encryption (Addressable). Encrypt electronic protected health information (that is being transmitted)

- User IDs and passwords are always encrypted
- All uploads and downloads are transmitted on an encrypted SSL connection; no exceptions
- All data is encrypted at rest or is suitably protected by some equivalent technology (fragmented BLOBs, etc.)
- Passwords are never transmitted unless over a secure, encrypted connection (FG is not susceptible to sidejacking nor is there a firesheep vulnerability)

Integrity

(c)(1)Standard: Integrity. Protect electronic health information from improper alteration or destruction.

(c)(2) Implementation specification: Mechanism to authenticate electronic protected health information (Addressable). Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.

(e)(2)(i) Integrity controls (in transmission) (Addressable). Ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.

All access to the system is captured in detailed logs and is monitored

Physical access to hardware is restricted and physical access is guarded 24 hours per day, 7 days per week including holidays

(Tuyu does not work by user/client-only provided key. The nature of the business for which Tuyu customers subscribe to prohibits such provisions, much like defined IP ranges).

Availability

§164.308(a)(7)(ii) Administrative Safeguards

(a) Data backup plan (Required). Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.

(b) Disaster recovery plan (Required). Establish (and implement as needed) procedures to restore any loss of data.

- Database backups are performed on all servers at least once daily
- Database backups are stored on a separate hardware appliance, on site, with physical access security safeguards in place and fire retardant protection
- Uploaded files are not included in backups. In the event of a hardware failure, uploaded files may not be recoverable. Files sent using the service are intended to be copies in transit, that are always scheduled for automatic deletion; SendToPerson.com is not a file storage service and your files may be deleted at any time for security and privacy purposes
- Hardware is monitored 24 hours per day, 7 days per-week to ensure service availability
- Redundant hardware and telecommunications systems are in place to ensure that under all circumstances service can be restored within four hours or less
- Disaster recovery plans are in place to notify system administrators, replace failed or damaged equipment, and restore backups at any time of day or night

Audit

§164.312 Technical Safeguards

(b) Standard: Audit controls. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

§164.308 Administrative Safeguards

(a)(5)(ii)(c) Log-in monitoring (Addressable). Procedures for monitoring log-in attempts and reporting discrepancies.

- Client-Server Logging: Capture Client-Server connections and activities related to the storage and transfer of files
- Web browser access logging: Collect detailed records of all user's activities and access to the system, including the upload and download of files
- Logs are included in and protected by backup and redundancy systems
- Detailed reporting is available of all system activity, and can be filtered by user, site, or email domain name
- All attempts to access the system (success or failure) are recorded along with details such as IP address and web browser details

Additional HIPAA Compliance Details

If the answer is yes to one or more of the following questions, the entity must secure compliance by regulatory statute. Otherwise the entity is compliant by exclusion:

Are you a "covered entity" (CE) or a "business associate" of a CE under the Health Insurance Portability and Accountability Act (Health Insurance Reform: Security Standards,

45 CFR, Parts 160, 162, and 164)?

Are you a covered "financial institution" or "service provider" as outlined in the Gramm-Leach-Bliley Act (Sections 501 and 505(b), codified at 15 U.S.C. 6801 and 6805(b))?

Are you a publicly traded company? If so, Section 404 of the Sarbanes-Oxley Act of 2002 requires you to publish and enforce rules for implementing internal controls of your corporate financial data.

Do you rely on outsourced partners and/or application service providers (ASPs) to accomplish your business needs?

Does your business deliver outsourced services?

Is your business critical to the US infrastructure or economic base?.

Business Associates

[45 CFR 164.502(e), 164.504(e), 164.532(d) and (e)]

By law, the HIPAA Privacy Rule applies only to covered entities – health plans, health care clearinghouses, and certain health care providers. However, most health care providers and health plans do not carry out all of their health care activities and functions by themselves. Instead, they often use the services of a variety of other persons or businesses. The Privacy Rule allows covered providers and health plans to disclose protected health information to these "business associates" if the the information only for the purposes for which it was engaged by the covered entity, will safeguard the information from misuse, and will help the covered entity comply with some of the covered entity's duties under the Privacy Rule. Covered entities may disclose protected health information to an entity in its role as a business associate only to help the covered entity carry out its health care functions – not for the business associate's independent use or purposes, except as needed for the proper management and administration of the business associate.

. . .

Other Situations in Which a Business Associate Contract Is NOT Required:

[45 CFR 164.502(e), 164.504(e), 164.532(d) and (e)]

With a person or organization that acts merely as a conduit for protected health information, for example, the US Postal Service, certain private couriers, and their electronic equivalents.

(End of Excerpt)