emocha Health®

HIPAA-Compliance & Security

+ The emocha platform is a suite of remote engagement and monitoring applications, with both mobile (iOS/ Android) and web components.

+ emocha's technology was initially conceived by clinicians and public health scientists at Johns Hopkins University in 2008: making emocha one of the first mobile health platforms ever. All emocha applications comply with HIPAA regulations on how to handle protected health information (PHI), including -- but not limited to -- secure encryption of data, access controls, and industry-standard best practices.

+ A robust & comprehensive role-based permission system limits system access to only authorized, authenticated users to ensure the need-to-know basis of PHI.

+ All PHI is encrypted both in-flight and at-rest, and all access to, or modification of, patient data and system configuration is logged: complying with HIPAA requirements.

+ The server infrastructure is secured from both physical and remote access. emocha also requires that all providers of external information system services comply with security requirements related to PHI and HIPAA regulations.

+ Data is stored for 7 years, per HIPAA requirements.

Information Storage

+ emocha's servers are hosted "in the cloud" via Amazon Web Servers at secure data centers. Physical access is extremely limited, if not impossible.

+ Log-in credentials are managed by a combination of strong password and private keys.

Password-Protection

+ emocha enforces specific identification and authentication procedures through password complexity, forcing users to change the default password at first login, and continuously working to ensure that all user accounts are unique.

+ Additional criteria to ensure password protection includes a password-protected screen lock mechanism, and a session lock after 15 minutes of inactivity.

Encryption

emocha Health®

+ The emocha platform uses two main kinds of encryption: in-flight and at-rest. In-flight encryption refers to the encryption of all data while being transmitted. Data being sent from a client, whether web-based or a mobile application, is sent via a secure HTTPS connection.

+ emocha audits its SSL configuration regularly, ensuring that system configuration is as up-to-date as possible.

+ At-rest encryption means that all protected health information (PHI) in the database and disk is always stored encrypted. This includes any record of a user, anything in the error log or audit log tables, any patient data, and all information submitted: including video files or GPS coordinates.

+ Data sent from mobile devices is encrypted on the device as soon as it has been collected. Data is then transmitted to the server over a secure HTTPS channel and deleted from the device as soon as receipt of the transmission is confirmed.

+ Recorded photos or videos are not visible in the device's general media gallery applications (e.g., there is no way to view the videos that are submitted -- they do not live on the phone's hardware). When retrieving any data from the database, the encrypted data is fetched by the application, then decrypted before being sent to the client.