QUENTRY SECURITY STATEMENT

Quentry employs advanced encryption and access control technologies to ensure that all sensitive medical information is protected. Data uploaded and stored on Quentry can only be accessed and viewed through the individual login accounts that are authorized to view the data. Quentry users are in full control of their login credentials and granting of access rights to their contacts.

Quentry is designed to protect its patient medical data from security breaches and malicious attacks. The sophisticated security measures and architecture implemented for Quentry meet both HIPAA and HITECH requirements for PHI (Protected Health Information), and are designed in accordance with European Union Data Protection Directives.

Quentry is powered by Brainlab, a world leader in software-driven medical technology.

KEY SECURITY MEASURES

Session and Data Transfer Security

Quentry provides physicians, including associated team members with access, control, and sharing of patient information from anywhere within a secure clinical network. Users access data stored in Quentry through the quentry.com web portal or Quentry-connected applications using a combination of encoded session keys and SSL encryption protocols.

- Quentry user passwords must be a minimum of 8 alphanumeric characters, contain a mix of upper-case and lower-case letters, at least one numeral, and are case sensitive.
- Periodic password changes are necessary and users are required to change his/her password regularly. When the user password expires, the user will be prompted to enter a new password on the next login.
- Upon logging in, a user session is created. User sessions remain active until the user logs out, but are also subject to a timeout period. User inactivity timeout period is configurable and can be changed from the User Settings page. Once the inactivity timeout period is reached the user will be automatically logged out.
- In order to access data within the Quentry system, the user must have authenticated and created a valid user session. To access file data stored within Quentry, the user must have a valid session token and have been explicitly granted permissions to access the data.
- All Quentry web pages and web services, and all components communicating with the Quentry secured cloud platform must connect over a HTTPS(2048 bit certificate with 256bit SHA-2 signature) encrypted connection and must have a valid session token.
- Quentry employs the SSL/TLS encrypted data transmission protocol.

BRAINLAB

Quentry | Security Statement

Data Storage and Security

Quentry file data is stored within Amazon AWS (S3), a robust storage service designed for 99.999999999% durability. Quentry encrypts all data during upload and download, as well as throughout the entire storage period.

- S3 stores data redundantly on multiple devices across multiple facilities to ensure availability, and uses Content-MD5 checksums and cyclic redundancy checks (CRC) to ensure data integrity.
- Amazon AWS is ISO 27001, SOC 1/SSAE 16/ISAE 3402 (formerly SAS70), PCI DSS Level 1, and FISMA certified and accredited.
- All files stored within the Quentry system are encrypted using the AES symmetric-key encryption standard with a 256-bit key.
- Quentry user credentials, account data, and patient data are stored separately for increased security. User credentials are stored on Salesforce.com, while account and patient data storage is built on Amazon Web Services.
- All patient data processing and database storage systems utilize encrypted file systems.
- Advanced key management and access control systems ensure that Quentry patient data is accessible only to users who own the data or have been explicitly granted access rights by the data owner.
- Quentry stores all user-generated data on servers located in secured facilities with 24/7/365 surveillance.

De-Identified Patient Data

Quentry offers the option to upload de-identified patient information by choosing to 'De-identify patient details' option when uploading data.

- When this option is selected, personally-identifiable metadata is removed from DICOM files during the upload process.
- Users must confirm that all visible patient information has been removed from the selected data.
- Users may choose to enter alternative identifiers prior to upload to assist with location and communication.

User Access Rights

Quentry users are able to assign data sharing rights to their contacts. Account administrators may also assign rights to CareTeam group members and contacts. The following rights may be assigned:

- By adding a Quentry user as a personal or CareTeam contact, that contact is granted the right to share their existing datasets (Patient Folders) with the user or CareTeam.
- Users may explicitly choose to provide contacts with "Allow Upload" rights. This enables the contact to upload a new dataset (Patient Folder) directly to the user or CareTeam.

BRAINLAB

- When adding users as members of a CareTeam group, the account administrator may assign “Manage” rights to the member. This enables the member to manage CareTeam members and contacts including assignment of rights and permissions.

Sharing Permissions

Images, attached documents, and comments are only viewable by the individual user and those contacts which have been granted access to the specific patient folder. Quentry users are able to define specific data handling permissions for each contact with whom they share patient data. Users define permissions for tasks including viewing, downloading, and uploading additional medical data.

When sharing an individual Patient Folder (contains one or more datasets) with a contact (individual users or CareTeams), the user may grant the contact permission to “View” only, “View and “Download”, or “View, Download, and Add”.

- The “View” permission enables the contact to view all images within the shared patient folder using the Quentry web-based or mobile viewing applications only. Shared users may also view existing comments and enter new comments for the shared patient folder.

- The “Download” permission enables the contact to download images and any attached documents through the quentry.com website, or using provided file transfer applications.

The “Add” permission enables the contact to upload additional images or documents to the shared patient folder. When adding a user as a member of a CareTeam group, the user is by default granted permission to view and download all datasets (patient folders) owned by the CareTeam.

- Download permission can be disabled for any CareTeam member by the account or CareTeam administrator.

Moving Patient Folders

Users can move a patient folder to another user or CareTeam. This action transfers ownership of the data to the selected user or CareTeam.

- Users may only move patient folders to users (contacts) or CareTeams which have granted them “Allow Upload” permission.

Individual and Group Privacy Settings

Quentry is a private and protected platform, prohibiting user and group information from appearing on Internet search engines or being accessible in any other manner without valid Quentry credentials. Privacy settings are controlled by the individual users, while account administrators can control group settings.

- Individual users may choose to prevent their contact information from appearing in Quentry Connect (contact) search results. The user may continue to invite others to become contacts, and existing contact relationships are preserved. Users will be informed about their contact visibility and the possibility to modify their visibility to other users.

- Individual users must be able to identify any individual or CareTeam requesting to be a contact before accepting the request. Details of the contact requestor, whether it is a user or a CareTeam, are displayed prior to accepting the request for identification purposes.

- CareTeam (group) member information cannot be viewed by other Quentry users until a contact connection has been approved by the CareTeam administrator. CareTeam contact lists are only visible to group members.

- CareTeam (group) administrators may choose to prevent their CareTeam's contact information from appearing in Quentry Connect (contact) search results. The administrator may continue to invite others to become members or contacts, and existing contact relationships are preserved.

- CareTeam (group) administrators must identify any individual or CareTeam request to be a contact before accepting it. Details of the contact requestor, whether it is a user or another CareTeam, are displayed prior to accepting the request for identification purposes.

Data Protection and Privacy

Quentry is compliant with HIPAA privacy and security rules. Quentry is also designed in accordance with EU Data Protection Directives.

- User access to patient data in Quentry is audited. Audit logs are accessible to the data owner.
- Patient data for European customers is processed and stored only on servers located within the EU.
- Patient data for US customers is processed and stored only on servers located within the US.

Users are responsible for ensuring that their granting of permission to other users or CareTeams to view or download data, or moving of data to another user or CareTeam is in compliance with their country's data protection laws.

Cloud Technology Providers

Quentry is built on a robust and scalable cloud infrastructure. As a suite of integrated services, Quentry leverages industry-leading cloud platform technologies. These technologies were selected for their known scalability, reliability, security, and established trust amongst large organizations in healthcare and other sectors.

Quentry is built on Amazon Web Services and Salesforce.com, both of which have received certifications and accreditations through the following international standards:

Amazon Web Services
ISO 27001, SOC 1/SSAE 16/ISAE 3402 (formerly SAS70), SOC 2, SOC 3, PCI DSS Level 1, FedRAMP, DICACAP, FISMA, FIPS 140-2, CSA
http://aws.amazon.com/security
http://aws.amazon.com/compliance/

Salesforce.com
EU/EEA and Switzerland Safe Harbor, TRUSTe EU Safe Harbor, TRUSTe Certified Privacy Seal, Japan Privacy Seal, ISO 27001, SOC 1/SSAE 16/ISAE 3402 (formerly SAS70), SysTrust (SOC-3), FISMA, PCI-DSS, TUV Certificate
http://www.salesforce.com/company/privacy/security.jsp
https://trust.salesforce.com/trust/security/

BRAINLAB