

ClientSuite Security

Communications Security

Verisign's 128-bit SSL (Secure Socket Layer) Digital Server ID/Certificate.

SSL is the industry-standard method developed by Netscape Communications Corporation for protecting Web communications. Verisign is recognized as the worldwide leader in providing SSL certificates. Any software with encryption features having key lengths over 40 bits is considered "strong encryption" by the U.S. Government for export purposes. The cryptographic keys contained within 128-bit SSL Certificates are virtually unbreakable. 128-bit encrypted messages are 309,485,009,821,345,068,724,781,056 times harder to break than 40-bit messages. Thus, it would take the same technology used to crack a 40-bit encrypted message 1 trillion x 1 trillion years to crack a 128-bit message. That's several trillion times longer than the age of the Earth.

Data Security

Firewall

Web servers running the application as well as the database servers are all protected behind a secure Cisco Pix firewall.

Server

Authorized and Unauthorized access attempts are logged for administrator review.

Database

Certain pieces of data that could potentially identify a person will be encrypted within the database itself. Therefore, in the event a potential hacker does gain access to the database, identifiable pieces of information will be encrypted and deemed useless to the intruder.

Confidentiality

All client data is deemed proprietary to the client and is treated in the strictest of confidence. All Dataquest employees and vendors having access to client applications and data are required to abide by signed confidentiality agreements in order to protect proprietary information.

HIPAA – Health Insurance Portability and Accountability Act

Dataquest is actively providing employee education and researching existing and future HIPAA requirements to ensure full HIPAA compliancy within applications, data structures and I.T. practices.

Physical Security

Web Hosting

Please refer to the "Web Hosting Specifications" document for details.

Application Security

User Logins

Users will be required to “login” prior to gaining access to fully use the application.

Designated IP Addresses

Access to the application can be limited by identifiable IP addresses. Therefore, it would only be possible for users to access the application from predefined locations or facilities.

User Audit Trails

Each time a user logs in to use the application an audit trail will be logged that includes the User ID, IP address and usage timeframes.

Each time a user adds or modifies a record in the database an audit trail will be logged to that specific record and will include the User ID as well as the date and time and the type of modification made.

An audit trail will be logged each time the user views information for a client (patient). Therefore, if the client submits a request for a list of employees who have viewed the client’s information a report can be produced for that particular client.

User Logoffs and Timeouts

Users are strongly encouraged to “logoff” the application when finished using it. However, the application will automatically terminate (logoff) any user session when a given user has not performed an action within the application for at least 60 minutes.

User ID Sessions

Only one session at a time is permitted for each User ID. Therefore, in the event users elect to share IDs against recommended security guidelines then they will not be permitted to use the application simultaneously with the same User ID.

Company Level Security

The term “company” refers to a Dataquest client. One company will not be granted permission to access data belonging to another company without first providing written consent to Dataquest.

Company-Module Level Permissions

The application will consist of several different modules or components. For example, the Clinical Assessment module is separate from the Billing module. Companies will only be able to access application modules for which they have purchased service.

User-Module Level Permissions

Each company or client’s administrator will have the ability to grant users access to only the application modules for which they desire those users to have access. For example, it may be desired to permit a given user to access the Clinical Assessment module but not the Billing module.

User-Page Level Permissions

Each company or client's administrator will have the ability to grant users access to only the pages (or sections) of the application for which they desire those users to have access.

User ID-Level Permissions

Each User ID will be assigned a user type that is associated with a permission level. For example, a user type of "admin" will have full access to the application and the ability to administer various features of the application. Other user types may include "full access" and "view only" access.