White Paper

HIPAA implementation Policies Procedures and compliance at different security levels.

How much we care our customer's privacy and security needs

TECHNOSOFT
Instill Excellence

Technosoft Solutions Inc. | Offshore Development
w: www.techno-soft.com
e: info@techno-soft.com
t: (203) 676-8299

Abstract:

In this document, we provide details about how we implement HIPAA as a vendor and at our software application level. We also provide details about HIPAA related soft configuration options that are available when our app is deployed at a client site.

Technosoft as a Vendor

Internal Policies & Procedures:

Technosoft takes HIPAA related security and privacy responsibilities very seriously. Our HIPAA policies and procedures are reviewed by third party HIPAA experts, periodically. Our HIPAA policies are procedures and routinely communicated to all employees. All new and existing employees go through a rigorous HIPAA training. All employee access to PHI is logged and monitored. Special procedures are in place for all System Administrators and Help Desk professionals who usually have direct exposure to PHI. Breach reporting mechanism is in place and strictly followed by all employees.

Further details can be acquired by requesting set of our HIPAA policies and procedures. Anis Siddiqy, our Chief Security and Privacy Officer, will be happy to answer further question you may have.

HIPAA at Software Development:

We design and develop Healthcare software with extensive focus on HIPAA privacy and security compliance. Following are details of HIPAA implementation and compliance at different security levels.

1. Employees & Organization Level:

Technosoft has HIPAA policies and procedures in place for all its employees and sub-contractors. These policies are rigorously followed and enforced. Please see section (Technosoft as Vendor) for details.

2. System Physical Security:

Our Applications and Data reside on servers that are hosted in the Amazon AWS

environment or other third party vendors who provide HIPAA compliant hosting solutions with BAA protection. All these servers are hosted in the special data centers specifically designed for high availability and highly secured Healthcare customers. These servers are physically inaccessible to anyone except the vendor's employees. Our customers have Business Associate Agreement in place with Amazon and other vendors. These servers are backed up on a periodic basis. All these servers can be located in a redundant server pool helping our customer provide high availability.

3. Network & Server Security:

Our solutions are hosted in redundant data centers. And are placed in a private secure subnet accessible only to our customer's employees only. Except for the HTTP and HTTPS ports (80, 443), all access to this subnet is restricted at the IP level and all remote access to this subnet is logged.

All OS level access is done through RDP/Linux Bastian host. Direct remote OS level access is strictly prohibited except for System updates and patch management. All help desk support is done using a tool that can directly communicate with OS level. Patches and security updates are updated at regular intervals, depending on the security requirements.

4. Data at Rest Security:

All our customer's data are stored in an RDBMS, Relational Database Management System. No direct access to the RDBMS files is allowed except to the system administrator. And all OS level remote access is screen captured. All data stored in the RDBMS is in encrypted format and all access is controlled through RDBMS' authentication and authorization mechanism.

5. Application Server Security:

All access to the RDBMS is served through an application server (Tomcat, IIS, Websphere, etc.). Role based security is implemented at the application server level and all access is authenticated and authorized using **oAuth** or other authentication frameworks. All user access is logged in the RDBMS. We have soft configuration options available for each client to select their password strength, auto logout and other addressable features.

Technosoft favors object based access and layered approach to each action called. Each action, when called, logs user access of that action implicitly.

6. Application Client Security, Smart Phone level:

For clients who have a mobile client application, we have additional security built in to the client application to secure data from theft and loss of these movable devices. We develop Android and iOS based HIPAA compliant m-health applications.

7. Data in Transit Security:

All Technosoft Healthcare application can be deployed over HTTPS, with SSL encryption.

8. Security Options in the Customer Environment

We do provide second and third level helpdesk support to our healthcare customers. We have extensive helpdesk support security mechanism and procedures in place. Please contact our privacy officer to request a copy of our HIPAA help desk support procedures.

Technosoft Solutions: Aligning with HIPAA Objectives

Technosoft has been involved with major healthcare software providers to make their solutions HIPAA compliant since early 2000.

We have senior HIMSS Certified Healthcare Security Professionals in our staff. We have intimate knowledge of HIPAA privacy and security regulations and its local implementations/interpretations. We have pre-developed many software frameworks that help us quickly deliver HIPAA compliant solution. All our healthcare software goes through a rigorous HIPAA check list. We have HIPAA policies implemented throughout our organization and we will be glad to sign a HIPAA Business Associate Agreement for software development or support service contracts.