

Abstract

Treeno Software believes that document management without security and auditing puts your organization's business information at risk. Treeno understands the need for privacy and security of financial, employee, patient, financial, student information as well as business proprietary intellectual property. Let Treeno help you to address your companies obligations to regulatory compliance requirements like HIPAA, GLB, SEC, FDA and other regulatory demands..

Table of Contents

Introduction to Treeno Security	3
Security Methodology and Layers.....	4
About Treeno Software	7

Introduction

Treno Software believes that document management without security and detailed auditing puts organizations at risk of not being able to address regulatory compliance. Additional risk of exposure by non authorized parties can be mitigated with Treno's security practices. Treno's detailed auditing and security protects your business and its' information.

Treno's approach to security allows its solution to address the most stringent regulatory compliance requirements mandated by HIPAA and FDA. Treno address these requirements with its eight layer approach to security and it detailed auditing capability down to its ability to address file level chain of custody reporting.

The Health Insurance Portability and Accountability Act of 1996 Privacy and Security rules was designed to protect individuals identifiable health information. The primary objective of the security rule is to protect the confidentiality, integrity, and availability of electronic protected health information when it is stored, maintained and transmitted. The electronic protected health information must be protected against reasonably anticipated threats, hazards and impermissible use and or disclosure.

HIPAA consists of three parts

Privacy – designed to protect patients' medical details

Security – to ensure unauthorized persons cannot access data

Transaction – designed to have user s to submit claims electronically via x-12 based EDI submission

Other regulations require

Permission based access – authorized user access

Original files – must maintain original files in an unaltered format

Chain of Custody Reporting – File tracking of changes by user and date and time

Security of access – encrypted access to files

Treno allows organization to address regulatory compliance of security and auditing.

Treno Software
believes that document
management without
layered security and
detailed auditing puts
your business at risk.

Security Methodology and Layers

Treeno Software Security

Treeno Software has eight layers of security that add up to a very secure platform. Each layer is kept simple so that implementation, deployment, and maintenance are easy for the people involved in the upkeep of the system.

Secure Connection via the Public Internet (First Layer)

When the server is setup the only port that needs to open to the web is port 443. All other non essential services can be put behind a firewall or shutoff. In case of Treeno Software setup we turn off all services that have open ports to the web. Treeno then scans the server for open ports with a tool called 'nmap'. By eliminating all other ports exposed to the internet we reduce our chances of security being compromised by an unauthorized user. By running over SSL, Treeno also reduces your risk since all traffic is encrypted and passwords and sensitive data cannot be sniffed if someone were to place an in line sniffer on the internet connection.

Treeno Software Application (Second Layer)

All data for the software application is stored on the machine in a SESSION. The only data that is stored on the remote pc is the SESSION ID. All data to the server is posted over SSL to prevent people seeing data in the initial request strings. All files start with a check for 'if logged in' which prevents all access to the system if an unauthorized users tries to post to a page or open any web page.

Treeno securely encrypts connection from the user's desktop to the server through 128 bit SSL encryption.

Users are granted access only to departments, cabinets, folders and documents they are authorized to see. File level access is reported to address chain of custody reporting.

System level audits tracks on user login IP, information touched, action performed and date and time of activity.

Treeno Software User Security (Third Layer)

User security is maintained in the database or by active directory, ldap, or NDIS. If a user is not logged in all of the pages are set to display nothing. This prevents people from gaining knowledge of how pages work. The user security also checks if users belong to departments and or groups. When a user is logged in their user permissions are stored in their session on the server. Users do not have direct access to the user permissions object. There are also 4 types of users: Super Administrator, Department Admin, Read/Write User, and Read Only user. If a user is not granted access to an item they cannot access items by default.

Treeno Software Group Security (Fourth Layer)

Groups are used to manage large numbers of users without having to select each user and individually create permissions. Groups also can hide documents and subfolders from people not in that group.

Treeno Software Cabinet Security (Fifth Layer)

Each cabinet created in Treeno Software is positioned in a department and the permissions can be set by user and group to prevent unauthorized access. Documents that belong to a cabinet can be accessed and hidden by group permissions and granted access when there is none by workflow access.

Treeno Software Department Security (Sixth Layer)

Each Database that Treeno Creates on the SQL server is it's own unique department. Users are assigned to a default department and can be granted access to switch to another department if needed, but need to be granted further access to the cabinets and documents in that department.

SQL Database Security (Seven Layer)

The SQL based database is where all the meta data is stored with pointers to files on the file system. The database gets its own username and password and can be hosted remotely. The Treno Application is compiled and the username and password is not stored in plain text. Access to the database is also done over SSL so that all meta data is secure.

File System Security (Eighth Layer)

If access is gained to the Operating System the files can be stored in a EMC Centera device which is an object file system that can protect files from being viewed by not allowing operating system level access to the files. The files can only be access by the compiled Treno Application. Instead of storing paths to the files in the database Treno stores a hash value for retrieving the files from the Centera.

Security of Customer Facing Files

Treno understands that there are needs to share information with other parties. Treno understands this information cannot be forwarded via email. Therefore, Treno provides a secure publishing portal to allow for secure remote access for permissioned third parties to be invited to view the file via an encrypted portal. This access is based on permissions. To grant access you must be a privileged user with rights.

Treno understands the need for privacy and security of electronic protected health information and provide our client enhanced security capability so that they can better address the HIPAA regulatory demands. In review, Treno Software can secure access by department, cabinet, document type or tab, folder based on index field, and information on the page with redaction. Should a user not have rights to view, the user will not be able to see or view the file. All access is audited by user, date and time, information accessed and what was done with the file. This detail audit allows organization to prove access and security of their confidential business information. Treno Software's best practices of security auditing which helps our clients to address the security and privacy requirements of HIPAA.

About Treno Software

Established in 2002, Treno Software is a leader in the Enterprise Document Management (EDM) industry. Treno Software was one of the industry's first to embrace cloud computing with the Treno EDM Cloud (SaaS) and to provide web-based solutions offering secure global mobile access. Treno Software's mission is to provide their customers with operational workflow efficiencies and measurable return on investment (ROI) through the fast installation and implementation of their fully secure, highly reliable, and easy-to-use, web-based Enterprise Document Management (EDM) Software Solution.

Corporate Headquarters

951 Islington Street

Portsmouth, NH 03801

800-528-5005