AdRem Software's HIPAA Compliance

An AdRem Software White Paper

This document is written by AdRem Software and represents the views and opinions of AdRem Software regarding its content, as of the date the document was issued. The information contained in this document is subject to change without notice.

ADREM SOFTWARE MAKES NO WARRANTS, EITHER EXPRESS OR IMPLIED, IN THIS DOCUMENT. AdRem Software encourages the reader to evaluate all products personally.

AdRem Software, Inc.
410 Park Avenue, 15th Floor
New York, NY 10022
USA

Phone: +1 (212) 319-4114
Fax: +1 (212) 832-4114
Email: sales@adremsoft.com
Web site: http://www.adremsoft.com

Executive Overview

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a major regulatory initiative in the health industry aimed at defining standards for the portability of health information and for protecting the security and confidentiality of patient data. While the Privacy component of HIPAA was enforced on April 14, 2003, the security rule mandates compliance by April 20, 2005.

The section entitled General Rules of the Final Rule on security compliance, issued February 21, 2003, reads as following:

Sec. 164.306 Security Standards
a. General requirements. Covered entities must do the following:

> i. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits.
>
> ii. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.

Sec. 164.308 Administrative Safeguards
A covered entity must, in accordance with [164.306]:
[…] Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

For an IT organization managing a Novell NetWare-centric infrastructure the implications of HIPAA are evident as the network is the backbone of every organization – it is the medium through which its data is accessed. Therefore, controlling the way the network impacts internal policies is the best and only way to avoid compliance violations.

AdRem’s solution to HIPAA’s security component

To help NetWare maintenance organizations within covered entities address chief HIPAA security compliance issues, AdRem Software delivers two award-winning solutions designed specifically for the NetWare-centric network environments, AdRem sfConsole and AdRem Server Manager. Both of these tools enable IT teams to support HIPAA requirements by embedding the functionality that is necessary to ensure centralized user provisioning and access administration (i.e. ensuring that only authorized individuals may have access to and modify only those information systems, resources and processes that are appropriate to them) as well as security auditing (i.e. recording for future reference all access to those systems, resources and processes, whether authorized or unauthorized).

In many healthcare organizations, these server security solutions have been instrumental in reducing the exposure of network assets to internal or external attacks that might compromise patient information. They also considerably reduce human error in information systems and greatly improve administrator productivity and server manageability. All these benefits are a consequence of the state-of-the-art capabilities and technologies applied in both tools such as control of network users’ and administrators’ access to server resources, data transmission encryption, centralized and automated processes, as well as user/process verification. As a result, IT managers can ensure that transparent and accountable practices are utilized to manage the covered entity’s information assets and ensure strict compliance with security-related regulatory directives.

sfConsole and Server Manager focus on two different aspects of server security and manageability. While the former protects access to the server console and is concerned chiefly with how IT personnel accesses and uses the server resources, Server Manager safeguards server files and other resources from the network user’s perspective. As a result, both solutions complement each other, offering a definitive, all-encompassing enterprise-class solution for administering NetWare shops in a secure and efficient way.

AdRem sfConsole

AdRem sfConsole addresses the commonly overlooked question of assuring supervision of maintenance personnel mentioned in Part 142 called "Security and Electronic Signature Standards". This security solution is dedicated to the security of the work environment of network personnel, which can be especially important in large organizations with multiple network supervisors in multiple locations. The program safeguards remote console access forcing users to authenticate to eDirectory and encrypting remote operations with three industry-standard encryption keys. It also ensures high-level security of the local console by providing mandatory eDirectory authentication, a keyboard lock and a screen saver. Using sfConsole's proxy server users can safely connect to the server through the firewall, while in the event of eDirectory inaccessibility they can use sfConsole to connect to the server and transfer files. On top of that, the program empowers authorized administrators to log users' activity on the console and centrally delegate enterprise-wide, role-based access rights to the server console resources such as screens and commands.

As a result covered entities can protect their servers from being accessed by unauthorized entities (disgruntled internal employees, hackers or business partners) as well as health data and patients/clients' identities while allowing IT supervisors to securely access their servers to perform maintenance, security and administration tasks.

Why you need to secure your NetWare servers?

- NetWare consoles operate over unencrypted connections which means the data is transferred as plain text.
- Administrator passwords are stored in an unencrypted text file, making it easy for an attacker to capture them and gain control of the server in the process.
- The NetWare operating system provides no way to define and delegate levels of access on a per-user or group basis. This means that all administrators in an organization – regardless of their job duties – have unlimited access to server resources.
- NetWare administrators have no way of auditing user activity on the server console

AdRem sfConsole

AdRem sfConsole supports HIPAA requirements in these areas:

Section	Standard	Specification	sfConsole capability
164.308 Administrative safeguards	Security Management Process	Risk management	sfConsole eliminates and rectifies risks and vulnerabilities inherent in NetWare through: • Protection of the remote NetWare server console via strong data encryption and Directory authentication. • Protection of the local NetWare console by means of eDirectory authentication, A keyboard lock and a password-protected screensaver
		Information system activity review	**User activity auditing** sfConsole enables in-house review of records of console activity by providing an audit trail of where and when the change was made, and who made it. The program's special log contains the exact date and time of the beginning or end of console operation, user name and address of the computer from which the connection was made. Benefits: • Enhanced console event visibility and server accountability • Shorter intrusion response time • Quicker response to attacks and reduced forensics time • Better ability to evaluate the impact of an incident

	Workforce security	Authorization and/or supervision *and* Access authorization, establishment, modification and termination	**1. Mandatory eDirectory authentication** In all options for remote server access available in sfConsole, the program forces remote users to authenticate to eDirectory. This is the case when you access the server from your Windows desktop, from the Web or from your Linux machine. As a result, operating and maintenance personnel have proper access authorization. **2. Centralized role- and scope-based access control.** From a central location, administrator can control access rights to particular users or groups, define console start-up scripts, or even restrict users' rights to selected screens or commands. In addition, this capability ensures the user termination when the employment of a workforce member ends. **3. Snap-ins for the essential eDirectory management tools, ConsoleOne and NWAdmin.** This way users can manage access privileges to console commands and screens directly from eDirectory. Benefits: • Full server protection against incompetent console usage or unauthorized access • The possibility to share the administrative tasks among several people by granting rights to carry out certain server tasks to particular users or groups of users (e.g. archiving resources, running selected scripts or monitoring server operation) • The possibility to limit console access for users with administrative rights • Many users may work on the server console simultaneously (remotely and locally), and

			each one of them will have appropriate access rights.
		Workforce Clearance Procedures	The console access rights management module in sfConsole allows covered entities to easily assign to IT workforce members varying levels of access to the server based on their roles.
		Termination procedures	The console access rights management module in sfConsole allows covered entities to easily revoke access rights to console resources after the termination of employment of a worker.
	Security incident procedures	Response and Reporting	For details on this issue, please see the Risk Management specification described above.
164.312 Technical safeguards	Access control and validation procedures	Emergency access procedure	**1. Emergency connection and file transfer** (also via the Web). In the event of eDirectory inaccessibility, sfConsole gives authorized administrators necessary access to the server to restore general access to electronic health information. **2. Role-based access administration,** see "Workforce security" in 164.308 (Administrative safeguards) **3. Multiple options for eDirectory-enabled and encrypted remote access to the console:** • from beyond the firewall • from the Web • from the NetWare Remote Manager portal • from a Linux or Windows workstation
		Automatic logoff	sfConsole delivers keyboard lock and a password-protected screensaver that "terminates an electronic session after a

			predetermined time of inactivity.” This helps prevent unauthorized physical access to the server.
	Transmission security	Encryption and decryption	**Data encryption** sfConsole can encrypt all remote administrative sessions (from a Windows or Linux workstation, via the Web, from behind firewall) with 128-bit, 168-bit or 256-bit encryption key in order to protect all transmitted information. This eliminates password hacking or sniffing. **Single sign-on technology** sfConsole uses safe connections between the workstation and eDirectory which enhances the security level of the console operation.

AdRem Server Manager

AdRem Server Manager is AdRem Software's most recognized solution that offers support in all aspects of Novell NetWare server management and monitoring, from user activity, connections, opened files to very advanced file and directory management. It facilitates and automates many click-intensive routine tasks, while its ergonomics and intuitive navigation substantially streamline daily server maintenance.

In addition, AdRem Software's tool offers many powerful, unique functions such as automated software distribution, extensive trustee rights management along with periodic reporting on server performance and utilization. As a result, even a novice administrator can effectively tune, manage and secure the NetWare environment as well as anticipate and prevent network emergencies and compliance violations before they escalate to a serious crisis.

Section 164.312 of General Rules of the Final Rule on security compliance stipulates that:

> a covered entity must in accordance with section 164.306: A, 1, Standard: Access control. Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights.

Server Manager is an application that will allow covered entities to centrally supervise and quickly set up user access rights to various applications, documents, data, servers and devices, thus complying with the above ordinance.

In a nutshell, Server Manager supports HIPAA requirements by allowing network organizations to:

- restrict access to server files/directories through trustee rights management (ability to modify, review and terminate user privileges on the server in compliance with security guidelines)
- centrally control user activity over the network
- provide encryption in remote communication sessions with the server
- prevent unauthorized use of specific server resources
- monitor user activity and connections to the server
- centrally and automatically deploy configuration changes, software and updates across multiple servers
- modify and distribute server SET parameters and configuration files
- perform advanced operations on files, directories and volumes
- trend server performance.

AdRem Server Manager

AdRem Server Manager can be used to meet HIPAA requirements in these areas:

Section	Standard	Specification	Server Manager Capability
164.308 Administrative safeguards	Security management process	Risk analysis	**Trend viewing and reporting** Server Manager allows covered entities to view how the server performance changed over a period of time (a day, a week, a month). Server behavior can be analyzed using trend, distribution, or comparison facilities. Historical information helps determine how individual computers make use of resources, and makes it easy to predict potential risks and vulnerabilities.
		Risk Management	**Risk management** Using Server Manager, covered entities can automatically distribute and maintain best practice guidelines regarding server security configuration management. The program substantially reduces the risk of manual errors and server failures by providing automated processes to distribute software upgrades and patches as well as configuration and system file changes, console commands, NLMs, server parameters, and more, on a one-to-many basis. Server supervisors can also compare multiple server configurations or single server configuration after changes (such as new software or patch installation, and also after system parameter change). As a result, it is easy to push out HIPAA-compliant security policies and software patches to multiple servers thus maintaining a unified and consistent IS environment.
		Information system activity review	Server Manager allows covered entities to review and monitor information system activity from a centralized graphical environment. The following server entities can be tracked that may

have decisive influence on the system activity:

1. System logs

Server Manager enables viewing the logs that are generated by the server or executed programs. The program displays system logs located in SYS:SYSTEM and SYS:ETC directories.

Crucial log content:

- Server abend errors – critical errors during server operation
- Bootstrap errors – server startup errors
- Console log – messages displayed on server console
- System errors – non critical system errors
- TTS errors – transaction tracking (TTS) system errors.

2. Centralized view of server configuration and activity

- Server SET parameters
  Ability to change server parameters (SET commands) in an automated and graphical environment.
- Viewing and editing server configuration files and NCF scripts.

3. Server performance and connection monitoring

Server Manager allows server supervisors to view in real-time any of the charts presenting the 150 server statistical parameters and loaded NLMs. This enables the monitoring of crucial statistics such as memory, cache hits, processor or NLM utilization, and many more.

4. Active connections

The program monitors both station (user) server connections and connections opened by the programs running on the server.

5. File user administration

With Server Manager, NetWare supervisors can effortlessly monitor logged-in users from the user side and file side alike. They can also quickly search files and

			check volume capacity utilization. As a result, it is easy to pinpoint users who for example hog the network with MP3 files thus preventing other users from access to health information. **6. Disk management** Disk manager allows you to modify the properties of volumes, directories and files and establish disk space quotas for users. Specific file/directory operations can be easily performed such as copying retained Netware attributes and setting the attributes for a certain file/directory recursively or purging/salvaging file/directory operations.
	Workforce security	Authorization and/or supervision	**Trustee rights management** Server Manager allows covered entities to set-up and manage role-based access to server files and directories. It displays the complete hierarchy of files/directories with various users' access rights, and enables the tracking and management of all inheritance masks and trustee rights to a given directory and its subdirectories. That way NetWare administrators can easily check whether the access rights a given user has been granted matches the HIPAA regulations.
		Workforce Clearance Procedures	The trustee rights management module of Server Manager allows covered entities to easily assign to workforce members varying levels of access to server files and directories based on their roles.
		Termination procedures	The trustee rights management module of Server Manager allows covered entities to easily revoke access rights to selected files and directories after the termination of employment of a worker.

	Information access management	Access establishment and modification	**Advanced file, directory and user management** Server Manager allows server supervisors to centrally establish, document, review, and modify a user's right of access to a file/directory as the employee’s role changes. In addition, they can modify file and directory properties and attributes and set new attributes for all subdirectories.
	Security awareness and training	Security reminders	With Server Manager, NetWare administrators can effortlessly monitor logged-in users from the user side and file side alike. By right-clicking the mouse, they can send messages communicating periodic security updates to network users.
	Contingency plan	Data backup plan	**Backup copy of the access rights** With Server Manager, access rights to a particular directory (including subdirectories and files) can be saved to a retrievable file.
		Disaster recovery plan	Server Manager enables covered entities to restore lost data. They can quickly reconstruct and restore access rights to files and directories e.g. following the replacement or failure of the hard disk.
		Applications and data criticality analysis	**Trustee rights reports** IT staff can track one person's privileges across the entire NetWare server infrastructure thus assessing the relative criticality of specific data in relation to a specific contingency plan.
164.312 Technical safeguards	Person or entity authentication	Access authorization	**1. NDS/eDirectory authentication in remote access to the server** **2. Role-based access administration**

			see “Workforce security” in 164.308 (Administrative safeguards)
	Transmission security	Encryption and decryption	**Data encryption** Server Manager provides a remote console, which can be used as the faster and more secure replacement for the NetWare consoles. The program’s remote console is safeguarded by 128-bit key encryption and NDS/eDirectory authentication. Additionally, thanks to our custom data compression algorithm, the Server Manager’s remote console is much faster than the NetWare consoles.

About AdRem Software

AdRem Software provides rapidly-deployable software solutions for monitoring, managing, troubleshooting and securing enterprise networks. Since its inception in 1998, the company has been at the forefront of Novell network management development. AdRem's efforts to create multi-task and easy-to-use solutions were quickly noticed and appreciated, resulting in the prestigious "Best Commercial Application" award from the Novell Developers' Contest in 1999 for AdRem Server Manager.

With AdRem Software's flagship solution, AdRem NetCrunch, businesses can automatically visualize and monitor their multi-technology networks and proactively ensure system, application and service availability to customers, employees and partners. AdRem NetCrunch is noted for delivering integrated, proactive network and systems management at the price of a point product.

The company's products target IT departments in small and mid-size companies, along with VARs, system integrators and networking services firms. By using AdRem's solutions customers can maximize returns on their IT infrastructures by boosting network/systems performance and availability, optimizing IT asset utilization and reducing maintenance overhead. The company's solutions are deployed on over 400,000 servers worldwide and are sold through AdRem's online store, resellers, distributors and system integrators in more than 50 countries.