


Access Control and HIPAA regulations

A white paper for Security professionals



Thousands of U.S. organizations must comply with the Health Insurance Portability and Accountability Act (HIPAA) Security Rule or face fines of up to \$250,000. This applies to any business that deals with electronic health information, including:

Health Plans

Health Care Clearing houses

Health Care Providers

Insurance Companies

The HIPAA regulations include mandates for physical safeguards to prevent unauthorized individuals from gaining access to electronic information.

More now than ever before, a security system must do much more than control access.

C-CURE 800 does.

SOFTWARE HOUSE

Table of Contents

HIPAA Overview.....	3
Physical Safeguards.....	4
Technical Safeguards.....	6
Summary.....	8

HIPAA Overview

The Health Insurance Portability and Accountability Act (HIPAA) was passed into law in 1996 and applies to thousands of US organizations. The overall purpose of the act is to enable better access to health insurance, reduce fraud and abuse, and lower the overall cost of health care in the United States. It includes a mandate for standards that ensure the security and integrity of health information that is maintained or transmitted electronically.

Businesses that are affected by HIPAA (“Covered Entities”) are required to:

- Assess potential risks and vulnerabilities
- Protect against threats to information security or integrity, and against unauthorized use or disclosure
- Implement and maintain security measures that are appropriate to their needs, capabilities and circumstances
- Ensure compliance with these safeguards by all staff

The HIPAA safeguards focus on protecting “data integrity, confidentiality and availability” of individually identifiable health information through the following:

- Administrative Procedures – documented, formal practices to manage the selection and execution of security measures
- Physical Safeguards – protection of computer systems and related buildings and equipment from hazards and intrusion
- Technical Security Services – processes that protect and monitor information access
- Technical Security Mechanisms – processes that prevent unauthorized access to data that is transmitted over a network.

The C-CURE 800 security management system is uniquely positioned to help Covered Entities comply with portions of the Physical Safeguard and Technical Security Services focus.

Physical Safeguards

The physical safeguards are a series of requirements meant to protect a Covered Entity's electronic information systems and Electronic Protected Health Information (EPHI) from unauthorized physical access. Covered Entities must limit physical access while permitting properly authorized access. The specific standards are:

Facility access controls An overall requirement to implement policies, procedures and processes that limit physical access to electronic information systems while ensuring that properly authorized access is allowed.

C-CURE 800/8000 is a scalable security management solution encompassing complete access control, advanced event monitoring, escort management and badging.

Workstation use Policies and procedures must be developed and implemented that specify appropriate use of workstations and the characteristics of the physical environment of workstations that can access EPHI.

Workstation security Covered Entities must implement physical safeguards for all workstations that can access EPHI in order to limit access to only authorized users.

C-CURE 800/8000 includes important administrative and monitoring station privileges that restrict who can perform specific actions. Two advanced features address this directly:

Manual Action Challenge – effective in version 8.2 of C-CURE 800/8000, this feature implements additional security at the Monitoring Station. Administrators can configure the system to prompt a user to enter a Username/Password when attempting to perform specific manual actions (i.e. momentarily unlocking a door, or arming/disarming an input).

Enhanced IT-based Password Protection – this feature moves the authentication process from C•CURE 800 to the operating system and also provides tools for locking or terminating C•CURE 800 applications when a station is left unattended.

When the C•CURE Enhanced Password Protection feature is used in conjunction with the policy management system provided by the operating system, administrators can create highly secure systems that:

- Meet the demands of most applications that require extensive security***
- Comply with organizational standards for computer security***

Device/media controls

Policies, procedures, and processes must be developed and implemented for the receipt and removal of hardware and electronic media that contain EPHI into and out of a Covered Entity, and the movement of those items within a Covered Entity.

Technical Safeguards

The Technical Safeguards of HIPAA include several requirements for using technology to protect EPHI, particularly controlling access to it. The specific standards are:

Access control Policies, procedures, and processes must be developed and implemented for electronic information systems that contain EPHI to only allow access to persons or software programs that have appropriate access rights.

Audit controls Mechanisms must be implemented to record and examine activity in information systems that contain or use EPHI.

C-CURE 800/8000 includes field-level audit trail capabilities for all security objects, including configuration and personnel clearances data. Everything from “Assets” to “Keypad Commands” can be audited for the following information:

“Who changed the data?”

“When was the data changed?”

“What was the data changed from?”

“What was the data changed to?”

Beyond protecting the personnel records, the audit trail feature provides irrefutable evidence if organizational insiders collude to change configuration information.

Integrity Policies, procedures, and processes must be developed and implemented that protect EPHI from improper modification or destruction.

Person or entity authentication

Policies, procedures, and processes must be developed and implemented that verify persons or entities seeking access to EPHI are who or what they claim to be.

Transmission security

Policies, procedures, and processes must be developed and implemented that prevent unauthorized access to EPHI that is being transmitted over an electronic communications network (e.g., the Internet).

Summary

Complying with HIPAA can require significant time and resources. There are more than 36 implementation specifications that must be met by the imposed deadline (no later than April 21, 2006).

It is imperative that Covered Entities understand the numerous rules and mandates and take the necessary steps toward compliance. Application manufacturers, like Software House, can help by providing solutions that address some of the requirements.

C-CURE 800 is a comprehensive access control system. However, with critical features like audit trail, enhanced password protection, and manual action challenge, C-CURE 800 does much more than provide access control; it enables corporations to have greater control over their entire security and business processes.

About Software House

Software House is a leading access control brand of Tyco Fire & Security. Software House designs, markets and supports integrated security management systems, including its flagship product C-CURE 800/8000.

From entry-level single-door access control systems to state-of-the-art integrated security management systems operating on enterprise-wide networks, Software House can provide you with a complete range of field-proven and innovative products.

For more information on Software House products,

1-800-550-6660

www.swhouse.com

SOFTWARE HOUSE