IMPLEMENTING HIPAA

WITH SCRIPTLOGIC AND DEERWOOD TECHNOLOGIES

ScriptLogic's software solutions provide the power to implement, maintain and report on internal access and security controls with minimal additional administrative burden.

INTRODUCTION

Deerwood Technologies has teamed with ScriptLogic to help provide many different types of enterprises comply with the requirements that arise from government legislation.

ScriptLogic is a leading global provider of systems lifecycle management solutions spanning, physical, virtual and terminal server environments, enabling IT professionals to proactively save time, increase security and maintain regulatory compliance through the seamless management of Windows desktops, servers and Active Directory. More than 22,000 customers of varying size and industry use SpriptLogic solutions to manage approximately 5.2 million desktops and servers every day.

The aim of this document is to highlight ways in which ScriptLogic solutions can be used to bring Microsoft Windows-based IT systems into line with the requirements of the Health Insurance Portability and Accountability Act.

HIPAA - BACKGROUND

The Health Insurance Portability and Accountability Act (HIPAA) was passed into law in August 1996, placing new requirements on thousands of US organizations involved with the provision of health care. Its two principal aims are:

1) To increase availability of healthcare by standardizing the exchange of healthcare information

2) To protect the confidentiality and security of patient records. Organizations that must comply with HIPAA are known as covered entities. These include health plans (e.g., HMOs, group health plans), health care clearinghouses (e.g. billing and re-pricing companies) and health care providers (e.g. doctors, dentists, hospitals).

However, the HIPAA Security Rule is much more demanding from an IT perspective since it covers the handling of individually identifiable health information where it is held in electronic form – referred to as Electronic Protected Health Information (EPHI).

This covers all aspects of information relating to an individual's healthcare, with the goal of protecting the confidentiality, integrity and availability of EPHI whenever it is stored, maintained or transmitted.

The HIPAA Security Rule sets out standards requiring the physical safeguard of EPHI in addition to administrative and technical safeguards that lean heavily on IT systems. Software solutions from ScriptLogic play a key role in helping Covered Entities achieve compliance with these standards by giving IT administrators the power and control they need over their Windows-based networks to enforce appropriate safeguards.

SCRIPTLOGIC

Deerwood TECHNOLOGIES *IT Solutions for Business*

Compliance has emerged as a top priority among many healthcare related businesses. Insufficient data security, inadequate contingency planning and the possibility of inappropriate access to medical records are key concerns.

ADMINISTRATIVE AND TECHNICAL SAFEGUARDS

The Administrative and technical safeguard requirements of the HIPAA Security Rule include a number of standards that ScriptLogic software solutions help Covered Entities to comply with. The table on below highlights some of the required safeguards together with examples of typical operations IT administrators would perform in order to enforce those safeguards:

Control	Safeguard	HIPAA Security Rule Section	Action Required
Security Management Process	Risk Analysis	164.308 (a)(1)(ii)(A)	Inspect permission settings for users and groups; ensure access levels are correct. Scan systems to ensure up-to-date patches have been applied.
	Risk Management	164.308 (a)(1)(ii)(B)	Correctly apply security policies and patches to desktops
	Information System Activity Review	164.308 (a)(1)(ii)(D)	Audit usage of Active Directory
Workforce Security	Authorization and/or Supervision	164.308 (a)(3)(ii)(A)	Establish consistent Active Directory delegations And Report on access to resources
Information Access Management	Access Establishment and Notification	164.308 (a)(4)(ii)(C)	Centrally establish File System and Windows Share permissions
Security Awareness and Training	Periodic Security Updates	164.308 (a)(5)(ii)(A)	Apply patches to Windows desktops and servers
	Protection from Malicious Software	164.308 (a)(5)(ii)(B)	Actively scan for known Spyware on desktops
	Log On Monitoring	164.308 (a)(5)(ii)(C)	Report on desktop log on activity
	Password Management	164.308 (a)(5)(ii)(D)	Manage service account passwords
Contingency Plan	Disaster Recovery Plan	164.308 (a)(7)(ii)(B)	Be able to restore AD and AD Security Be able to restore NTFS and Share Security
	Emergency Mode Operation Plan	164.308 (a)(7)(ii)(C)	Centralize desktop configuration to facilitate emergency operations
Access Control	Automatic Logoff	164.312(a)(2)(iii)	Logoff inactive users
Audit Controls	Record and Examine Activity	164.312(b)	Audit file system usage