

Whitepaper

HEROware's™ ROLE IN THE HIPAA-REGULATED HEALTHCARE INDUSTRY

Abstract

This document addresses the contingency plan and physical access control requirements of the Administrative Simplification security provision of HIPAA. It will assist health care providers (doctors, hospitals, pharmacies, health insurers, clearinghouses, or any organization directly handling patients' health care information), in understanding how HERO (BCA) can be implemented to fulfill some of these requirements.

The Administrative Simplification Security Provision

Doctors, hospitals, pharmacies, health insurers, and other health care entities process and track billions of health care bills, records, and other transactions each year. With so many different types of health insurance, doctors and hospitals must spend time and money ensuring that claims processed electronically contains the format and content required by each insurer. Additionally, health insurers spend time and money ensuring their systems can handle electronic transactions from numerous health care providers. Uniform national standards could save the health care industry billions of dollars by lowering the costs of developing and maintaining software and reducing the time and expense needed to handle electronic health care transactions. The Health Insurance Portability and Accountability Act (HIPAA) enacted by the United States Congress in 1996 included a wide variety of provisions designed to make health insurance more affordable and accessible by establishing standard formats and data content for electronic transactions between all health care providers. One section of HIPAA, Administrative Simplification, has multiple parts: transactions standards and code sets, electronic signatures, security, privacy, and unique health identifiers. Focusing just on the Administrative Simplification security provision, HIPAA requires the development and implementation of administrative, technical, and physical safeguards to ensure the security of electronic transactions containing patients' health information.

1. These safeguards include contingency planning and physical access controls. Each security safeguard has required implementation steps including, but not limited to, disaster recovery, emergency mode operation, data backup, and access restrictions.
2. It is with these security implementation steps that the right technology can simplify and ease the strategy for becoming HIPAA compliant.

The words security should not be confused with either privacy or confidentiality. Privacy refers to the rights of an individual to control his personal information and not to have it divulged or used by others against his wishes. Confidentiality is a means of protecting an individual's personal information from unauthorized disclosure after the information has been received by another entity. Security applies to the actual physical, technical, and administrative safeguards that are put in to place to protect the integrity, availability, and confidentiality of information. For a complete listing of all of the requirements and the mandatory implementation steps to meet each requirement, see the Security and Electronic Signature Standards rule published by the Department of Health and Human Services at: <http://aspe.hhs.gov/admsimp/bannerps.htm#security>. Department of Health and Human Services.

Solution: HERO (BCA) as part of a compliance strategy

HERO from HEROware (powered by Double-Take Software) can fulfill the backup, disaster recovery and emergency mode operations that are required for HIPAA security implementation. HERO is a real-time data replication and failover appliance that augments an existing Microsoft Small Business Server network environment by providing a data protection mechanism that has minimal impact on users or network resources. HERO allows the administrator to specify that mission-critical data, in this case patients' records, stored on a



SBS server, be protected by creating a second copy of the data on another system, the HERO appliance, and then a third copy (HEROguard) is for off-site disaster recovery at the HERO datacenter. HERO (BCA) monitors any changes to the production copy of the data and replicates those changes to the secondary server. This second copy of the data is synchronized in real-time with the first, making the data accessible in the event of a major disaster or system outage. What does that mean to a health provider? Let's take a look at several of the Administrative Simplification security provisions in closer detail.

Administrative Contingency Plan

The administrative safeguards "require a contingency plan to be in effect for responding to system emergencies. The organization is required to perform periodic tape backups of data, have available critical facilities for continuing operations in the event of an emergency, and have disaster recovery procedures in place." HERO (BCA) automates some of these processes by providing a disaster recovery implementation that saves time and resources. For example, an SBS server that contains patient records is known as your production server because these records are the main files that are updated by your personnel. To implement a disaster recovery process, you need another full back-up server HERO (BCA), located on-site or off-site, which contains an exact copy of the data on the production server. Unlike backup technologies that create only a daily or weekly copy of the data, HERO (BCA) is designed to create and maintain an up-to-the-second copy of the data on a secondary server HERO, designated for recovery.

Off-Site Disaster Recovery, Billing and Insurance Records, Health Records, Appointment Management System Off-site Disaster Recovery Server

The administrative contingency plan also calls for a data backup plan. Unlike tape backups which run periodically to provide archival data, HERO continuously captures changes as they occur and makes them immediately available. This real-time capability of HERO removes the need for existing tape backup strategies and saves both time and money.

Off-site Disaster Recovery with Data Backup

A third implementation requirement of the administrative contingency plan is an emergency mode operation plan. This requirement states that your office needs to ensure a copy of the production data is always available on the disaster recovery server.

Emergency Mode Operation (Local High Availability)

HERO's flexibility allows you to combine these configurations to suit your needs. If you want a local high availability server and an off-site disaster recovery plan, HERO plus HEROguard gives you 100% protection of your data and a true disaster recovery plan that is easily implemented and cost effective.

Local High Availability with Data Backup and Off-site Disaster Recovery: Physical Access Controls

The physical safeguards require "limiting physical access to an entity while ensuring that properly authorized access is allowed." The same implementation requirements (disaster recovery, data backup, and emergency mode operation) are mandatory. While the physical aspects of security are unique to every building and physical environment, HERO also has access controls in place. HERO builds on the proven reliability of Microsoft by using native Windows operating system security features. As long as proper security processes are in place (such as physical restriction to servers, proper Windows security policies and procedures, and other HIPAA security requirements), HERO will compliment the access restrictions required for HIPAA compliance.



Summary

The Health Insurance Portability and Accountability Act (HIPAA) established standard formats and data content for electronic transactions between all health care providers. The Administrative Simplification security provision of HIPAA requires health care providers to develop and implement safeguards to ensure the security of electronic transactions containing patients' health information. HEROware offers many features and benefits that can enhance and optimize compliance strategies. HEROware, along with your trusted technical advisor, can deliver and implement effective data availability and disaster recovery solutions. For questions on HEROware, including pricing and product features call toll free (866) 810-HERO(4376) or send e-mail to info@heroware.com.

About HEROware® Inc.

HEROware® Inc. provides the world's most relied upon solution for accessible and affordable data protection for Microsoft® Small Business Server (SBS). The HERO product is the standard in data replication, enabling customers to protect business-critical data that resides throughout their Microsoft Small Business server environment. With its partner programs and service offerings, HERO delivers unparalleled data protection, back-up, high availability, and recoverability. It's the solution of choice for finance, legal services, retail, manufacturing, government, education and healthcare markets. HERO is an integral part of their disaster recovery, business continuity and overall storage strategies. For more information, please visit www.heroware.com.

© HEROware, Inc. All rights reserved.

HEROware, HERO, HERO BCA AND HEROguard are Trademarks of HEROware, Inc. Double-Take, is a registered trademark of Double-Take Software, Inc. Microsoft, Microsoft Windows Small Business Server, and the Windows logo are trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries.

All other trademarks are the property of their respective companies.

