Global Information Assurance Certification Paper

Robert Happy Grenert
GHSC v1.0
Practical
Second Submission
April 22, 2004

Abstract

This purpose of this document is to address the *Data Backup Plan* implementation specification of the Contingency Plan Standard, a requirement of the HIPAA Security regulations. This implementation specification (IS) will be applied to the covered entity (CE) "GIAC Health", a fictitious hospital and medical center. This document will explain what the IS requires of GIAC Health to comply with the regulation, a sample policy to be used by GIAC Health for compliance, the reasoning and support documentation that lead to creation of this policy, and the procedures this CE will use to implement the policy. The goal for GIAC Health is to update and upgrade its current backup strategy to maintain availability to patient data in the event of an emergency, hardware failure, disaster, and so on.

Assignment 1 – Define the Environment

The fictitious covered entity is GIAC Health, a 59 bed hospital and medical center, set in a rural environment. This medical center has 150 desktop PC's running Windows 2K or XP Pro, 10 Windows servers, a UNIX-Ware 7 server, 2 Windows web servers, an Apache web server, and an Exchange e-mail server in a Windows 2003 Active Directory environment.

Most patient data, or "electronic protected health information" (ePHI) generated by users is stored on the UNIX server, which is supported and maintained by a hospital information system (HIS) vendor. This server runs a RAID 1 configuration on its four primary hard drives, each of which is mirrored to one of four secondary drives. There is also a "snap shot" hard drive, which is used with Veritas software to backup all data from the mirrored drives during the overnight CRON process. The software prevents any new data from being written to the drive being backed-up, but holds this data in a queue until the backup is completed. The software then writes the new data to the drive. A SuperDLT tape drive is then used to backup the data copied to the snap shot drive. Two weeks worth of daily backup tapes are used MON-SAT, with a weekly tape used each Sunday for three weeks, and a monthly tape used the last Sunday of each month for three months. The monthly tape is sent to the HIS vendor for verification and any emergency restoration needs.

Other ePHI, created by end users with application software, is kept on a Windows 2003 Server (2K3-SERVER) along with all other user files. This server has four hard drives in a RAID 1+0 configuration, with striping and mirroring. While the server has an internal DLT tape drive, it is no longer used in favor of a network attached storage (NAS) appliance. Built-in Linux-based backup software allows the NAS to copy all data from the 2K3-SERVER nightly. There is sufficient storage on the NAS to hold 7 full days of daily backups.

Other servers, including the Exchange e-mail server, web servers, and domain controllers do not contain ePHI, but are also critical enough to be backed up each night onto the NAS. All use "Acronis TrueImage" to image each hard drive and copy the image files to the NAS. Again, there is sufficient storage on the NAS to hold 7 full days of daily backups of these other servers.

Finally, with the goal of providing an Electronic Medical Record (EMR) by scanning all paper-based patient data, GIAC Health has purchased high-speed scanners and content management software to scan, store, index and provide access to this ePHI in its new digital format. As this information will be mission-critical, GIAC Health must look at redundant hardware, policies and procedures that maintain availability to this data.

The HIPAA Security steering committee at GIAC Health has determined that after security, "availability" to ePHI during emergencies is the most critical issue regarding patient care. GIAC Health wishes to maintain availability to all ePHI on all primary information systems at all times, and within identified budgetary guidelines. GIAC Health has purchased and implemented various technologies for maintaining instantly accessible "exact copies" of ePHI through the use of duplicate and redundant information systems, servers, and other storage hardware. This Plan addresses how these systems will function to maintain exact copies of ePHI, where this data will be kept, how it will be secured, how it will be tested for reliability, and how it will be accessed in emergency situations.

The following upgrades to facilities, backup systems and servers were made to provide for mission-critical availability to all ePHI:

Backup Data Center - GIAC Health built up a secure walled and locked area in the basement of a medical office building on the medical center campus, about 50 years from the main building, for a backup data center. This building (as with all out buildings on the campus) is connected by fiber optic cable to the server room in the main building. A server cabinet was located in this area, complete with a uninterruptible power supply (UPS) for power stand-by. The plan is for all backup servers, NAS drives and external tape drives to be housed in this cabinet in the backup data center.

NAS – moved to the rack in the backup data center. Other servers, including the Exchange e-mail server, web servers, and domain controllers are still backed up each night onto the NAS. This device had an external SuperDLT tape drive attached to run tape backups of all files on the NAS each morning. This is an additional level of backup using a tape drive that was previously shelved when the NAS was put into place.

POC BACKUP – rack-mount PC provided by the HIS vendor to backup current in-patient data (Point-of-Care data) on an hourly basis was also moved to the rack in the backup data center.

UNIX Server - a "warm server" was purchased from the HIS vendor, which is a duplicate server. Cost was an issue, as it would be with any redundancy plan. The warm server was located in the backup data center. On an hourly set schedule a copy of the entire UNIX system is sent to the warm server. In the event of an emergency, server crash, and so on, the GIAC Health IT department need only swap the IP addresses, making the "warm server" live, and continuing ePHI availability. The tape drive backup process will continued on a once-a-month basis with the tape sent to the HIS vendor for verification on their systems.

2K3-SERVER – This server was already being backed up to the NAS each evening, only the location of the NAS was changed.

EMR SERVER – A recommended configuration provided by the EMR vendor was installed, with the specific intent to create "retrievable exact copies" of ePHI and have this data available in the event of a problem with the main server. The primary EMR Server was located in the rack of the main server room. This server uses a RAID 5 configuration for its three data drives which hold the log files, RAID 1 for the two O/S drives, and a single drive each for the O/S page files and the EMR statistic files. This server is attached to an EMC high-speed drive array which holds all the EMR data files (ePHI). This drive array uses RAID 5 on its five hard drives, with a sixth drive available as a hot swap. "Double-take" software, which as been referred to as "poor man's clustering software," is used to make an exact live duplicate of the EMR file system from the source server. The target server for the Double-take files is a less expensive rack-mounted server located in the backup data center. This server has a RAID 5 configuration on its three hard drives. The EMR vendor has provided a special "emergency license key" to allow the EMR backup server to act as the primary server in the event of a failure or problem with the main EMR server.

Assignment 2 – Explanation

HIPAA Security Standard – Contingency Plan, CFR 164.308(a)(7)(i)
Implementation Specifications - *Data Backup Plan* (ii)(A)

(7)(i) *Standard: Contingency plan.*
"Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information."
(ii) *Implementation specifications:*
(A) *Data backup plan* (Required).
"Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information."

A Data Backup Plan is a required IS of the HIPAA Security regulations. It is amazing to some to learn that heretofore there has been no requirement or mandate that digitally stored patient data be safeguarded by the use of backup procedures. This IS requires the CE to establish and implement procedures to create and maintain retrievable exact copies of ePHI.

The Data Back-up Plan must be documented, and the decision process that took place to form this Plan must also be documented. The Plan must take into account all ePHI, to identify the data, where it is located, and make sure it is included in the Plan. The Plan should include back-up verification, appropriate retention policies, appropriate media rotation and security, and logging procedures. In addition to HIPAA Security regulations, there may also be federal and state regulatory requirements or other contract or agreements that must be considered to make the Plan as comprehensive as possible.

Back-up media should be stored in a secure, environmentally sound off-site location. Special care and procedures should be taken in the transporting of this media to and from source and storage locations. Strict controls should be implemented over access to and retrieval of back-up data so that only appropriate staff with password, token, or other type of authorization key can obtain access. Care should be taken so that backup media is not damaged, particularly before any retrieval or recovery process is run. A procedure for verification reading and test restoring of back-up media should be carried out with some regularity to ensure the quality of data for emergency recovery needs.

The Data Backup Plan is a sub-process of the entire HIPAA Security Contingency Plan. This Standard also includes two addressable implementation specifications for "applications and data criticality analysis" and "testing and revision procedures." It is obvious by reading this rule that to ensure all-inclusive backups that are verified as retrievable, applications and data criticality must be

analyzed and there must be testing procedures for the data, with revisions to the process made as needed.

Similarly, the Data Backup Plan is an integral part of any Disaster Recovery Plan and Emergency Mode Operation Plan as well. These plans together must protect the "confidentiality availability, and integrity" of ePHI before, during, and after incidents such as floods, fires, natural disasters, terrorist activities, and so on. Because it is during these times that much of a security infrastructure may not be functioning, especially if electrical power is lost, security measures must be implemented to first and foremost protect the ePHI. Eventually, when the data is required for patient care, it needs to be made available in a secure fashion. Determining the level of preparedness and the steps involved in this preparation should be done under the guidelines of what is "reasonable and appropriate" for each covered entity, to protect against any "reasonably anticipated" threats, hazards, unauthorized uses, or disclosures of ePHI.

As a part of the Contingency Plan Standard, the Data Backup Plan is scalable based upon the size of a CE, their vulnerabilities, and identified threats, among many factors. In some instances, tape backups done daily and stored off-site may be sufficient for a small clinic, dentist or chiropractor's office, while clustered servers with NAS storage may be minimally sufficient for large medical centers and other providers.

In a situation where systems storing ePHI are damaged by some incident, the CE will fall back on the policies and procedures developed as part of the Contingency Plan Standard to respond to this type of instance. While the CE must take appropriate precautionary steps to identify potential occurrences, it should be noted that natural disasters will probably be deemed as a low priority in many instances.

Assignment 3 – Policy

GIAC Health Data Backup Plan

1. Overview

The GIAC Health Data Backup Plan will meet the requirements of the HIPAA Security Rule, which is part of a required Contingency Plan for protecting and accessing "electronic protected health information" (ePHI) during and after emergency situations.

2. Purpose

The purpose of the Data Backup Plan is to establish and implement policies and procedures, as an integral part of the GIAC Health Contingency Plan, for responding to an emergency or other occurrence (fire, vandalism, system failure, natural disaster, etc.) that damages systems that contain ePHI by way of making routine backups of ePHI from all appropriate locations and to test the reliability of the backups for emergency retrieval.

3. Scope

The scope of this Plan is to establish and implement procedures to create and maintain retrievable exact copies of ePHI.

4. Policy

It will be the policy of GIAC Health that exact retrievable copies of all electronic protected health information (ePHI) as defined by the HIPAA Security Rule will be created, and this information will be made instantly available on duplicate servers in case of emergency. Copies of ePHI will be created live and concurrent with original data, on a daily basis for end user data, and on an hourly basis for current in-patient ePHI. This backup data is to be maintained in a backup data center and tested for integrity and reliability on a monthly basis. Redundant hardware will also be routinely tested for emergency use.

Assignment 4 – Procedures

These procedures address how GIAC Health systems containing or storing ePHI will function to maintain exact copies of ePHI, where this data will be kept, how it will be tested for reliability, and how it will be accessed in emergency situations.

The following is the data backup, emergency data access, and testing procedure for each server or system:

A) UNIX Server – all files will be scheduled to back up on an hourly basis to the "warm server" located in the backup data center. In the event of an emergency, the network administrator or designee will swap IP addresses making the "warm server" live. A tape backup will be made on the evening of the last Sunday of each month, with the tape sent to the HIS vendor for verification. The warm server will be tested on the last Friday of each month by IT staff, who will attempt to access ePHI data on this server through the HIS application.

B) NAS – the Exchange e-mail server, all web servers, and domain controllers will be backed up each night onto the NAS. A tape backup of the NAS files will be schedule to run after the server files are backed up, with the tape being swapped by Security staff each morning. In the event of an emergency, the network administrator or designee will have access to files on the NAS or tape for purposes of retrieving lost or deleted user files. A "test folder" stored on the 2K3-SERVER will be restored on the last Friday of each month by IT staff to test the integrity of both the NAS and backup tapes.

C) POC BACKUP – this PC will be configured to backup current in-patient data on an hourly basis. In the event of an emergency, the network administrator or designee will print all current in-patient data to a laser printer in the IT office and distribute these pages to the appropriate nursing staff. In the event of data loss from the UNIX Server, the HIS vendor will be contacted to retrieve data from the POC BACKUP. IT staff will test print five pages of this data on the last Friday of each month.

D) 2K3-SERVER – this server will be backed up to the NAS each evening. Emergency and testing procedures for the copied data are the same as those for the NAS. In the event of an emergency with this server, the network administrator or designee will give end users access to their files directly from NAS until such time as this server is again functional.

E) EMR SERVER – this server and its attached drive array will be connected to a stand-by server using "Double-take" software to make an exact live duplicate of the EMR file system from the source server to the target server. In the event of an emergency, the network administrator or

designee will install the vendor-provided “emergency license key” making the backup server the temporary primary server. The data on this server will be tested on the last Friday of each month using the EMR web interface software pointed to the stand-by server data drive. No testing of the hardware is needed as this is a live server and the Double-take software will alert IT if there are any errors on either server.

Summary

This document addressed the *Data Backup Plan* implementation specification of the Contingency Plan Standard, which is required by the HIPAA Security regulations. The fictitious covered entity “GIAC Health”, complied with this requirement with a written policy and specific procedures used to implement the policy.