

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Device and Media Controls - Disposal

Alan R. Mercer

GIAC HIPAA Security Certificate (GHSC)

Practical Assignment - Version 1.0 (Option B)

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Table of Contents

Abstract 3
Assignment 1 – Define the Environment: 4
Assignment 2 – Explanation 5
Specification - Disposal 5
Standard – Devices and Media 5
Explanation of the Specification 5
Assignment 3 – Policy 6
1.0 Overview 6
2.0 Purpose 6
3.0 Scope 6
4.0 Policy 6
4.1 Covered Media and Devices: 7
4.2 Acceptable Methods of disposal: 7
4.3 Unacceptable Methods of disposal: 7
4.4 Documentation 7
4.5 Training 7
4.6 Business Associate Agreements 8
4.7 Audit 8
5.0 Enforcement 8
6.0 Definitions 8
7.0 Revision History 8
Assignment 4 (Option B) – Procedures 9
A. Authorization, custody, and documentation: 9
B. Fixed Disks – including removable: 9
C. Other Removable drive media: 10
D. Optical media: 10
E. Non Volatile memory storage: 10
F. Personal Digital Assistants (PDA): 10
G. Magnetic Tape: 11
References 13

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Abstract

This document discusses the HIPAA Security Rule specification 164.310(d)(2)(i) which covers the disposal of devices and media. The discussion centers on the environment of a fictional nursing home, GIAC Health. The first section of the paper describes the environment in which GIAC Health operates. This is followed by an explanation of the disposal specification and a sample device and media disposal policy. The paper concludes by describing procedures to implement the requirements of the specification and policy.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Assignment 1 – Define the Environment:

GIAC Health is a 200 bed non-profit nursing home that provides residential nursing and rehabilitation care to the elderly. The organization is wholly owned by GIAC Social Services (GSS), a 503(C)(3) non-profit organization. GIAC Health's is classified as a large covered entity under HIPAA regulations since its' annual revenues of ten million dollars exceed the floor of five million dollars [1]. Computer and network equipment, software and facilities are owned by GIAC Health, but are acquired, maintained, and disposed through the Information Technology (IT) department of GSS.

GSS and GIAC Health are considered associated entities under 164.105(b)(1) and the name GIAC Health will be considered to cover both entities. Associated entities are treated as a single covered entity for Subpart C of HIPPA, which covers security standards 164.308 through 164.318 [2]. Accordingly, GIAC Health's technology, security, and usage policies are based upon those used by GSS. This provides consistency in procedures and policies that form the foundation for a trustworthy association.

GIAC Health operates in a heterogeneous Windows 2000 environment comprised of five servers, 45 desktop computers, 15 laptop computers, and a dozen Windows based PDAs (Appendix – figure 1). The usage policy dictates that workstations are to store applications only, all data is to be stored on the network servers. Ten of the fifteen laptops are secured to nurses' carts and run wireless network connections and Citrix remote access with 128 bit encryption to access the GIAC Health systems. The five servers each are segregated by functional role: Authentication and access control, database services, remote access, file and print services, and a physical access control application server. Policy states that Electronic Protected Health Information (ePHI) shall be stored only on the file and print server and database server. These two servers have their own independent backup devices and media. The remaining servers are backed up by a third network attached backup device.

It is important to note that ePHI is processed on the Citrix server as well as workstations and laptops. Though policy dictates that data is not to be stored on these devices, the possibility remains that ePHI may exist on local workstations and laptops. Similarly, since PDAs are synchronized with server data via workstation connections, it is also possible that ePHI exists on these devices as well. Workstations, laptops, and PDAs are not systematically backed up given the presumption that these devices contain only applications and can be restored by use of standard disk imaging or resynchronization.

Other important items to note are that GIAC Health's database and file print servers use encrypted file systems (EFS), as do all laptops. PDA's are protected by encryption software resident on the PDA's and controlled by centralized policy. Access to all devices is controlled in compliance with policy and HIPAA requirements 164.308(a)(4), 164.310(b), 164.312(a)(1) and through logon processes, automatic logoff or locking screen savers, and unique user identification [3].

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Assignment 2 – Explanation

Specification - Disposal

The disposal of media and devices is covered by the HIPAA required specification 164.310(d)(2)(1) which states:

> "Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored."

Standard – Devices and Media

Furthermore, this specification is part of the HIPAA standard 164.310(d)(1) which states:

> "Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within a facility."

Explanation of the Specification

The specification on device and media disposal addresses the need to securely remove ePHI data from storage media and devices containing or used to process ePHI prior to disposal. The scope of the specification is restricted to the permanent retirement of media and devices as is indicated by the phrase "final disposition". This measure is a physical safeguard that requires control over the access to media and devices [4]. The specification requires that ePHI exposure at disposal be minimized through policy and procedures [5]. The act of careless disposal can lead to unintended disclosures of ePHI data. Recovery of ePHI data from retired media and equipment should be prevented by thorough cleansing or destruction of the storage media.

The authors of the HIPAA legislation intended that covered entities take up best practices as recognized in the information security field. These practices should be incorporated in the development of policies and procedures that address the disposal of media and devices [6]. Since the standard governs the receipt, removal and movement of devices and media pertaining to a facility, documentation of such activities is strongly indicated and is in accordance with best practices [7].

Specifically, the ultimate goal of the specification is the elimination of ePHI to the extent that it can not be retrieved by conventional systems and commercially available software. Conventional methods of erasure and formatting do not provide this degree of security [8]. Media must be overwritten, degaussed, or physically destroyed in such a manner to eliminate the possibility that any media may not be reused and expose old data [9]. Such devices include hard disks, removable media such as floppy disks, zip drives, CD-ROM, magnetic tape, and memory devices such as Smart Cards and PDAs.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Assignment 3 – Policy

A sample policy following the format used by SANS and found in other sample policies at http://www.sans.org/resources/policies is presented below. This policy is designed to comply with the required HIPAA specification CFR 164.310(2)(d)(i) concerning the disposal of devices and media. The focus upon HIPAA requirements does not preclude the adaptation of this policy by other organizations not subject to HIPAA requirements and is intended to follow best practices regarding the disposal of media and destruction of data.

Devices and Media – Disposal Policy

1.0 Overview

The Device and Media – Disposal Policy is intended to provide guidance on the requirements of secure disposal of devices and media to ensure that ePHI data is not disclosed as a result of inadequate measures to remove ePHI data. Unless secure measures are undertaken to ensure the complete removal of ePHI data from media and devices, unintended disclosures may occur. All employees of <Company Name> (including business associates of <Company Name) must be aware of the requirements that disposal of media and hardware is to be accomplished in conformance with the guidelines below.

2.0 Purpose

This policy is intended to establish a process through which all the secure removal of ePHI data is accomplished on any media used by <Company Name> prior to disposal.

3.0 Scope

The scope of this policy includes all <Company Name> employees and agreements with business associates who authorize the disposal, handle media or devices destined for disposal, or are directly responsible for the disposal. This includes data owners and the end-users of removable media devices.

4.0 Policy

All media containing <Company Name> owned ePHI (or believed to potentially contain ePHI) must have all data removed prior to disposal, in a manner that precludes the possible recovery and disclosure of the data by conventional means or commercially available software. Such measures should be in agreement with information security best practices for data destruction, while considering cost-effectiveness and the safety of the employees responsible for the destruction of the data. Documentation of the authorization, custody, and final disposition of data is mandatory.

© SANS Institute 2004, Author retains full rights.

4.1 Covered Media and Devices:

All fixed and removable storage devices owned by <Company Name> are covered by this policy. This includes, but is not limited to: magnetic media (including fixed disks, magnetic tape, floppy, and other removable drive disks), optical disks, and non-volatile memory devices (including memory sticks and cards or USB memory storage), and PDAs. Any storage devices currently available but not used by <Company Name> or that become available in the future due to new technology are also covered by this policy.

4.2 Acceptable Methods of disposal:

Data disposal may occur through the use of complete overwriting of data, degaussing, or physical destruction in accordance with information security best practices. Physical destruction is required for non-functioning and/or non-writable media, except when prohibited by hardware vendor warranty replacement policies. Overwriting or degaussing methods should be used on any functioning media that may be disposed in a manner that does not prevent media reuse by a third party as may be required with leased equipment, exchanges (including warranty replacement), trade-ins, or resale of used equipment and media.

4.3 Unacceptable Methods of disposal:

Such methods shall not place undue cost overhead upon <Company Name> nor place employees of <Company Name> at physical risk. Use of dangerous equipment, toxic, flammable, or dangerous substances shall not be used to accomplish secure disposal.

4.4 Documentation

The disposal of media and devices containing ePHI shall be documented from authorization for destruction to final disposal. The chain of custody of the data shall be established and maintained in the disposal documentation and shall clearly identify the asset or media to be disposed and include the dates and means of authorization, removal of media, removal of data, and disposal of the device and/or media. This documentation shall be maintained for a period not less than six years in agreement with HIPAA documentation requirements.

4.5 Training

All employees responsible for disposal activities will receive training on the policies and procedures on the use of software and tools used to prepare and audit media and devices for disposal.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

4.6 Business Associate Agreements

All disposal activities outsourced through third parties, including related organizations, shall be conducted in accordance with a Business Associate agreement that requires disposal procedures and policies that provide equal or greater security standards than those required by this policy. Transfer of devices and media to business associates shall be documented by signed transfer forms and certificates of destruction provided by the business associate. Such agreements shall provide for audits by <Company Name> or auditor acting under the direction of <Company Name>.

4.7 Audit

Disposal activities will be periodically audited by <Company Name> or auditor acting under the direction of <Company name> HIPAA Security Officer to verify compliance with the Devices and Media – Disposal Policy.

5.0 Enforcement

All <Company Name> employees authorizing or disposing of devices or media that potentially contain ePHI data are responsible for compliance with this policy. Violations are subject to disciplinary procedures up to and including termination as described in the <Company Name> employee handbook.

6.0 Definitions

Business Associate – A third party that provides or receives services from <Company Name> that may require transmission or receipt of ePHI data.

ePHI – electronic Protected Health Information. Information classified as PHI under HIPAA rules that is stored electronically.

Secure disposal – media and device disposal that is preceded by the complete removal of sensitive data in a manner to prevent recovery using conventional and commercially available software.

7.0 Revision History

© SANS Institute 2004, Author retains full rights.

Assignment 4 (Option B) – Procedures

GIAC Health will use the following procedures to securely remove data from media and devices prior to disposal in compliance with the GIAC Health Devices and Media – Disposal Policy. These procedures will be used as the basis for minimum requirements to be incorporated into all agreements for disposal services by Business Associates. The procedures specify the methods to track authorization for disposal, maintain custody of media through disposal, disposal sanitization activities, and documentation of these activities.

Each media class (magnetic media, optical storage, non-volatile memory, and PDA's) disposal procedures are discussed in the following sections and discuss disposal activities regarding non-functional media and functioning media that will no longer be used by GIAC Health. Differing procedures are required since functioning media may potentially be resold, traded-in, returned to leasing companies, or exchanged. Within each class certain media and devices may require differing procedures; these exceptions are identified by classifying procedures by media type.

A. Authorization, custody, and documentation:

Disposal of media requires authorization by the data owner of record. In addition the owner of the physical media must also authorize disposal involving hardware or magnetic tapes. When hardware or tape media disposal occurs, documentation of such disposal must be entered into the IT Support Call Tracking software and identify the parties authorizing disposal, all custodians of the media or device until disposal, and certification of disposal. This information must include the dates of authorization, transfer of custody, and disposal. GIAC Health uses the HEAT system for tracking support calls and technology assets [10]. Since this system is owned and operated by GSS and also used by their technology support staff, this provides for a single document to track each disposal activity. Disposal of other removable media is to be documented by the data owner and certification of the disposal is to be sent to the mailbox datacert@giachealth.org [11] which is managed by GSS Information Technology, who maintains all messages received for a minimum of six years

B. Fixed Disks – including removable:

The secure disposal of fixed disks is to be accomplished by complete overwriting if the disk is to be reused by anyone, per the Device and Media – Reuse policy. Overwriting is to be accomplished by use of Darik's Boot and Nuke Program (DBAN) [12] set at the DoD 5220.22-M method of overwrite [13]. The computer is to be detached from the network and booted from either a floppy disk or CD containing DBAN. At the boot prompt, press enter to use interactive mode to select the drive and method. Allow the system to run to completion and review logs to ensure completion. Repeat the procedure for each physical drive in the system. Restart the system without the floppy or CD to ensure the system fails to start. Note: DBAN does not support RAID controllers [14]. Systems using RAID must be reconfigured prior to using DBAN to connect each drive to a non-RAID SCSI controller before using the above procedures.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Damaged, non-writeable, or non-functioning disks must be physically destroyed unless prohibited by warranty or lease conditions. Remove the drive from the system and protective case. Cut all cable and power connections to the drive. Remove the drive heads from the mechanism. Drill holes in the platters at random intervals and distances from center, then pound the drive platters with a ball peen hammer to distort the platters [15]. Finally, cut the platters using tin snips at least four times from the outside to the inside of the platter.

For malfunctioning drives that must remain intact per service or warranty agreements, attempt the use of the DBAN program to overwrite the drive. Document the return of the failed component to the business associate and reference the support call.

C. Other Removable drive media:

Due to the low cost and remanence exhibited by floppy disks and similar media, physical destruction of the media is recommended. First run format to erase all files and directories, followed by PGP Free Space wipe using at least one full pass. Remove the media from the casing, cut the metal spindle from the media if present. Discard the spindle and run the media through a paper shredder to destroy the media. For exceptions, see the Devices and Media – Reuse policy.

D. Optical media:

The disposal of optical media including CD-ROM, CD-R, DVD, and other optical storage media is to be accomplished by physically destroying the optical media. The media is be repeatedly gouged using a nail, screwdriver, or awl. This is to be followed by abrasion to the media surface using course sandpaper (100 grit or lower), then breaking or cutting of the media into at least eight pieces. For exceptions, see the Devices and Media – Reuse policy.

E. Non Volatile memory storage:

Memory storage devices such as Compact Flash, SmartMedia, memory sticks, and USB memory drives are viewed by computers as drives. Preparation of the media for disposal requires the minimum necessary steps defined in the Device and Media – Reuse policy. Disposal of such media is to be accomplished using PGP Wipe File set at a single pass to securely erase all files and directories on the media. This is to be followed by using PGP Free Space Wipe set at a single pass. For final disposal, the media should be physically destroyed by mutilation; repeated hammering of the device is recommended.

F. Personal Digital Assistants (PDA):

The preparation of PDAs for disposal is comprised of an automated wiping of data by the encryption software, resetting to factory defaults, removal of power, and physical destruction. The first three steps correspond to the Device and Media – Reuse policy for PDAs. First enter an incorrect password repeatedly into the PDA until the PDA

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Secure software policy forces a bit-wipe of all data on the PDA. Secondly, reset the PDA to factory defaults per the manufacturer's instructions. Next remove the battery from the PDA for several hours. Prior to physically destroying the unit, either remove the display screen from the PDA or place the PDA in a soft case, then place the unit in a sealed bag wrapped in cloth in order to prevent injury during destruction. Hammer the unit repeatly to damage and destroy circuitry and chips inside the unit. Disposal of PDAs must be recorded in HEAT to document these activities.

G. Magnetic Tape:

GIAC Health does not maintain facilities to dispose of magnetic tape at reasonable cost and safe manner. Specialized equipment is required to degauss the Type III DAT, DLT, and LTO tapes used by GIAC Health [16]. Disposal of magnetic tape media is to be accomplished through third parties contracted to perform the physical destruction of magnetic media by chemical process, melting, or incineration. These contracts are to be established in compliance with GIAC Health policies on Business Associations and subject to the audit provisions of this policy. Subsequent to the authorization for disposal, the tape is to be removed from service, placed in secure storage awaiting transfer to the disposal contractor. Signed transfer records and disposal certificates are to be received from the contractor and filed with the disposal history for the media and the transfer and destruction document information is to be recorded in HEAT.

© SANS Institute 2004, Author retains full rights.

Footnotes

[1] Grenert et al p. 14

[2] Federal Register 2/20/2003 Part II: P 8375-8376

[3] Federal Register 2/20/2003 Part II: P8377-8378

[4] Grenert et al p. 14 p.33.

[5] Grenert et al p. 14 p 189.

[6] Federal Register 2/20/2003 Part II: P8337.

[7] Grenert et al p. 14 p 188.

[8] Edwards: Wiping Old Hard Disks Clean

[9] Gutmann: Secure Deletion of Data From Magnetic and Solid-State Memory

[10] Front Range Inc. HEAT Service and Support

[11] Fictitious e-mail address created for this paper

[12] Darik's Boot and Nuke: Product Feature Checklist

[13] File Extinguisher Wiping Methods: Grade 10

[14] Darik's Boot and Nuke: Frequently Asked Questions

[15] Commonwealth of Virginia: Removal of Commonwealth Data from Surplus Computer Hardrives and Other Electronic Media Standard B.3.b and B.3.c

[16] Shaefer, Eric. DoD Specifications and Guidance For Sanitizing High Capacity Storage Media.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

References

Commonwealth of Virginia – Virginia Information Technologies Agency. Information Technology Resource Management Standard - Removal of Commonwealth Data from Surplus Computer Hardrives and Other Electronic Media Standard. 29 October 2003 http://216.239.39.104/search?q=cache:dMr-sLZ1ELEJ:www.vita.virginia.gov/docs/psg/SMS_COV_ITRM_Std_SEC2003-02-1.pdf+disk+wipe+standard&hl=en (11 June 2004)

Edwards, Mark Joseph. Wiping Old Hard Disks Clean. 31 March 2004. http://www.winnetmag.com/WindowsSecurity/Article/ArticleID/42207/42207.html (1 June 2004)

Federal Register: Part II – Dept. of Health and Human Services: 45 CFR Parts 160, 162, and 164 Health Insurance Reform: Security Standards: Final Rule. Thursday, 20 February 2003. http://www.cms.hhs.gov/hipaa/hipaa2/regulations/security/03-3877.pdf (21 February 2003)

Front Range, Inc. HEAT: Achieve Differentiation Through Superior Support. November 2003 http://www.frontrange.com/pdf/HEAT_ServiceManagement_11_03.pdf (13 June 2004)

Grenert, Robert Happy et al. HIPAA Security Implementation 1st Ed. Version 1.0. Bethesda, Md.: SANS Press Inc. January 2004

Gutmann, Peter. Secure Deletion of Data From Magnetic and Solid-State Memory. 22-25 July 1996. http://www.usenix.org/publications/library/proceedings/sec96/full_papers/gutmann/ (13 June 2004)

Horn, Darik. Darik's Boot and Nuke. 30 May 2004 http://dban.sourceforge.net/ (15 June 2004).

LC Tech. Filextinguisher Wiping Methods. 2004 http://www.lc-tech.com/flx-definitions.htm. (11 June 2004)

Shaefer, Eric. DoD Specifications and Guidance For Sanitizing High Capacity Storage Media. 12 October 1999. http://www.thic.org/pdf/Oct00/datasecurityinc.eschafer.001003.pdf. (15 June 2004).

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.