GIAC
CERTIFICATIONS

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.

Table of Contents 1
Kyle_Cunningham_GHSC.doc 2

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.

Procedures for Establishing Emergency Mode Operation Plan for Electronic Protected Health Information

HIPAA Security Rule, Administrative Safeguards, 45 CFR 164.308(a)(7)(ii)(C)

GIAC HIPAA Security Certificate (GHSC) Practical Assignment (v1.0, option B)

Kyle Cunningham, CISSP
7 January 2005

Abstract

Emergency Mode Operation Plan is one of the HIPAA Security Rule implementation specifications supporting the Contingency Plan standard. Falling in the Administrative Safeguards facet (vice Technical or Physical), numerous Government policy documents and guide references are cited. Initial policy and a procedural framework to achieve this implementation specification are proposed for the fictitious entity *GIAC Health*.

Forward

The topics of disaster, disruption, and tragedy have been highlighted by events of late December 2004. Two contrasting themes can be drawn from two independent events. First, the tremendous power of Mother Nature can quickly trifle the works of man. The December 26th undersea earthquake and tsunami [USGS, 2004] that has devastated the Indian Ocean region elevates the topic of contingency planning in many people's minds. Second, the complete disruption of operations at feeder airline Comair on December 25th, attributed to a critical computer application that failed [Pilcher 2005], reminds Information Technology (IT) managers that a system can suddenly quit. Bad publicity and lost customer goodwill amplifies the corporate loss. Just because the system worked yesterday does not mean it will work tomorrow.

For a Health Insurance Portability and Accountability Act (HIPAA) covered entity seeking compliance with the security rule, adhering to the requirements related to contingency planning is an important endeavor.

Assignment 1 — Define the Environment

© SANS Institute 2005 Author retains full rights.

For the purpose of this treatise, the fictional enterprise *GIAC Health* will be used. GIAC Health is a major medical center, providing a comprehensive array of patient treatment. There are several buildings hosting GIAC Health activities, but they are all on one single geographic campus.

GIAC Health has a large enough staff to include a dedicated IT branch. They work at coordinating the requirements for new or upgraded systems; administering and maintaining GIAC Health owned IT resources; or coordinating outside IT support. The procurement / contracting staff buys for the IT branch when major purchases are made. A small computer security staff (augmented with hired consultants when major audits are performed) is separate from the IT branch, but maintains close liaison.

Assignment 2 — Explanation

The topic, Emergency Mode Operation Plan, is a HIPAA Security Rule implementation specification, one of five supporting the Contingency Plan standard. This is a required (vice addressable) specification. The Security Standards Matrix, published as appendix A to the Security Rule, lists all of the 36 specifications that support the 18 standards. (The Security Rule is actually subpart C "Security Standards for the Protection of Electronic Protected Health Information" – 45 CFR part 164 "Security and Privacy.") The Contingency Plan standard is part of the Administrative Safeguards facet of the Security Rule. The other two facets are Physical Safeguards and Technical Safeguards.

An Emergency Mode Operation Plan is expected "to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in the emergency mode." [45 CFR 164.308(a)(7)(ii)(C)] The regulator's choice of words can be a bit confusing, especially when read by health professionals who have their own expectations of the terms "operating" and "emergency." The focus is not the Emergency Room or Operating (surgical) venues.

In fact, the more common term for a plan of this sort is Continuity Plan or Business Continuity Plan (BCP), where the purpose is described as "Provide procedures for sustaining essential business operations while recovering from significant disruption." [NIST SP 800-34, table 2-1] Further amplification: "A BCP identifies and defines an organization's overall capability to continue functioning when its normal operations are disrupted ..." [Weil, pg. 1].

Specifically, HIPAA enacted regulations do seek a narrower focus for the Emergency Mode Operation Plan: "... this is a mandate for continuing processes involving the use and protection of EPHI [electronic protected health information] during and immediately after a crisis situation ..." [Northcutt, pg. 166] The regulators themselves clarified: "... it only involves those critical business processes that must

© SANS Institute 2005 Author retains full rights.

occur to protect the security of electronic protected health information during and immediately after a crisis situation." [Federal Register, para. III.E.7.d., pg. 8351]

The Contingency Planning Guide for IT Systems, National Institute of Standards and Technology (NIST) Special Publication 800-34, provides a comprehensive look at the framework for a BCP and supporting components. The BCP is frequently used as the centerpiece to organize related plans. One set of these are the Continuity of Support Plan (when a general support system) and IT Contingency Plan (when a major application). Here, the Executive branch of the US Government uses two plan titles for two flavors of IT system. [NIST, pg. 8]

It is proposed to best satisfy Emergency Mode Operation Plan requirements with a set of modular plan components, that plug into a BCP-like framework. There are two dimensions that define these components: 1) the facility or department within GIAC Health where the system delivers service, and 2) the functional category (flavor) of the component.

The purpose behind preparing a tailored plan component to each location is to enable the plan text to be specific for that work environment. References to facility locations, department titles or telephone numbers, and care-delivery processes can be specific. This will help GIAC Health staff make direct reference to the plan for use in a crisis situation.

The functional category follows the Information Assurance model recently adopted by the Department of Defense (DoD). They organize and manage all information systems according to four categories: "... automated information system (AIS) applications, enclaves (which include networks), outsourced IT-based processes, and platform IT interconnections." [DoDD 8500.1, para. 4.2] Here: AIS application maps to "major application;" and enclave includes the network, host platforms, and fundamental software titled "general support system" by the Executive branch. Instead of platform IT interconnections (where a DoD ship, tank, or plane talks to the net), GIAC Health employs medical equipment that connects to the enclave (such as: a heart monitor feed to the nurse's station over the local network).

Further borrowing from DoD, GIAC Health will stratify IT systems similar to the Mission Assurance Category (MAC) I through III. Defined: "The consequences of loss of integrity or availability of a MAC I system are unacceptable and could include the immediate and sustained loss of mission effectiveness. MAC I systems require the most stringent protection measures." [DoDD 8500.1, para. E2.1.25.1.] MAC II is "Systems handling information that is important to the support of deployed and contingency forces. The consequences of loss of integrity are unacceptable. Loss of availability is difficult to deal with and can only be tolerated for a short time. The consequences could include delay or degradation in providing important support services or commodities that may seriously impact mission effectiveness or operational readiness." [DoDD 8500.1, para. E2.1.25.2.] And finally MAC III described, "Systems handling information that is necessary for the conduct of day-to-

© SANS Institute 2005 Author retains full rights.

day business, but does not materially effect support to deployed or contingency forces in the short-term. The consequences of loss of integrity or availability can be tolerated or overcome without significant impacts on mission effectiveness or operational readiness." [DoDD 8500.1, para. E2.1.25.3.]

Assignment 3 — Policy

1.0 Purpose

The purpose of this GIAC Health policy is to meet the needs of Emergency Mode Operation Plan (EMOP) implementation specification [45 CFR 164.308(a)(7)(C)] of the HIPAA Security Rule. EMOP is a component of the Contingency Plan standard within Administrative Safeguards.

2.0 Scope

This policy covers GIAC Health Information Technology (IT) systems hosting Electronic Protected Health Information (EPHI). Systems can be categorized and bounded via both of the attributes in the tables below:

Table 1: GIAC Health IT Systems Functional Categories

Functional Category	Description
Enclave	IT network, boundary protection, host platforms, operating systems, and general-use application software.
EPHI Application	Single or multiple (bundled) software that relate to a specific GIAC Health function (processes or stores EPHI), hosted on a GIAC Health enclave.
Outsourced EPHI handler	EPHI Application not hosted on a GIAC Health enclave.
Medical Device Interconnection	Device or family of devices providing a medical function that connect to GIAC Health enclave.

Table 2: Medical Delivery Assurance Category (MDAC)

MDAC Designation	Description
MDAC I	Consequences of loss of integrity or availability of a MDAC I system are unacceptable and could include the immediate and sustained loss of effective patient care delivery.
MDAC II	Important to the support of caregivers. The consequences of loss of integrity are unacceptable. Loss of availability is difficult to deal with and can only be tolerated for a short time.
MDAC III	Necessary for the conduct of day-to-day business, but does not materially effect support to patients in the short-term.

© SANS Institute 2005 Author retains full rights.

3.0 Policy

GIAC Health will implement an EMOP library of modular plan components. The purpose of these components is to implement critical processes that must occur to protect the security (confidentiality, integrity, and availability) of electronic protected health information during and immediately after a contingency.

Checklist-like procedural guide pages will be developed and maintained for each MDAC I system. The guide pages will be tailored to each GIAC Health department (floor) or facility. Guide pages will be inserted to tabbed EMOP binders maintained at key locations (such as: nurse stations) throughout GIAC Health campus. Core EMOP data will be consolidated into binder front-matter or annexes. Table of contents and tabs will direct users to plan components for each system present in that location.

A document management system may be used to organize and generate EMOP components, to include on-line access to EMOP components for training and contingency use. However, all MDAC I system EMOP components will be physically distributed and provisioned in the plan hard-copy binders.

EMOP components for MDAC II systems will also be developed. The plan components may reside entirely on-line, but in redundant systems for retrieval or on-demand printing. The department/facility granularity for MDAC II components of the EMOP may be broader: like work areas may be grouped together into fewer plan components.

EMOP components for MDAC III systems are optional, depending on available resources at GIAC Health (to generate and maintain plan). If a MDAC III system is determined to require EMOP coverage, it will be treated as if it were MDAC II.

4.0 Enforcement

EMOP components for MDAC I systems will be evaluated via exercise or audit every six months. Procedural or information errors will be corrected as soon as possible, but within 45 days of discovery.

The exercise/audit interval for MDAC II level EMOP components is annual, with corrections within 90 days.

An annual census audit will verify there are appropriate EMOP components for each EPHI system at GIAC Health.

© SANS Institute 2005 Author retains full rights.

Assignment 4 (option B) — Procedures

The stepwise outline below is tailored from NIST SP 800-34, section 3, “IT Contingency Planning Process.” Project Management methodology is applied to define these steps toward a successful implementation.

Step 1 - Emergency Mode Operation Plan (EMOP) Policy

The policy outlined in assignment 3, above, must be benchmarked against the GIAC Health HIPAA Security Rule gap analysis. Following the tenants of *SANS HIPAA Security Implementation* [Northcutt, chapter 6] a situation inventory was prepared. A quick-look assessment of the identified systems against the policy will suggest any policy deficiencies or errors.

The newly proposed policy will require staff vetting and then approval by GIAC Health leadership. This will start in the IT branch and continue through the Security office up to the executive level. Cost estimates and a draft EMOP project plan to achieve compliance will need to accompany the approval package so appropriate resource decisions can be made concurrent with policy approval.

Step 2 - Impact/Risk Analysis Refined

The broad Business Impact and Risk Analysis (already on-hand) will need to be refined under the direction of the newly appointed EMOP project manager. The refined census of systems and break out of EMOP components, shaped by updated impact assessments, will suggest a project sequence and tempo. Significant vulnerabilities will be addressed first. This project manager will be assigned a cross-functional team so EMOP procedural development and training planning will mesh with the “ground truth” throughout the GIAC Health organization.

Step 3 - Identify Preventive Controls, Develop Recovery Strategies

A material solution may be available to close or reduce a vulnerability. For example, adding an Uninterruptible Power Supply (UPS). These opportunities to reduce the need for EMOP procedures will be passed over to the IT branch in a systematic manner.

Step 4 - Develop Emergency Mode Operation Plan (EMOP) components

© SANS Institute 2005 Author retains full rights.

In cases where a material solution is not available or not yet installed: the non-material (procedural) EMOP component is needed. The three dimensional EMOP component stack (see figure below) has lateral width (left) according to the various system functional categories, depth (right) by the departments or facilities where deployed, and height according to Medical Assurance Delivery Category (MDAC). Any enclave system hosting a MDAC I system is elevated to become MDAC I itself. Figure 1, below, shows this concept.

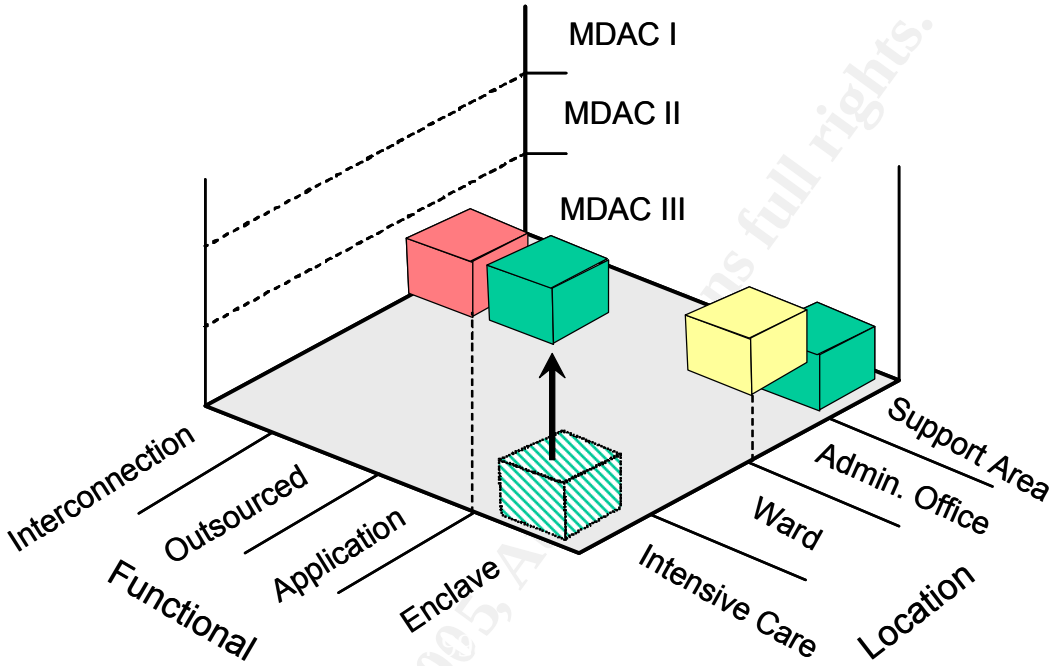

Figure 1: EMOP Component Topography

Requirements for any new systems to be implemented at GIAC Health will include delivery of EMOP components, to mesh into the fielded EMOP system. Outsourced development of EMOP components may be conducted via the procurement/contracting staff.

Step 5 - Testing, Training, and Exercises

As EMOP components are completed, they must be tested for accuracy and fielded with appropriate staff training. Continuing training opportunities for newly assigned staff, and to refresh existing staff, must be conducted.

The Security office will implement a tracking system to ensure semi-annual and annual exercises or audits of the plan components are conducted according to the policy. Identified EMOP deficiencies will be recorded, reported, and tracked for

© SANS Institute 2005 Author retains full rights.

corrective action completed in a timely manner.

Step 6 - Plan Maintenance

The EMOP project will conduct or supervise plan component maintenance. “Burn down” of deficiencies (identified per step 5, above) will be monitored to meet policy time limits. Implementing an effective system for user feedback will enable GIAC Health staff to easily report EMOP component defects noted on-the-spot. Continuous improvement processes will improve the probability of smooth operations and spotless exercises and audits.

Summary

This document addressed the Emergency Mode Operation Plan implementation specification of the Contingency Plan standard, required by HIPAA motivated Security regulations. The approach outlined for fictitious GIAC Health medical center illustrates the issues and frames a suggested approach to achieve compliance.

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.

References

1. HIPAA Security Rule: 45 CFR parts 160, 162, and 164. “Health Insurance Reform: Security Standards: Final Rule.” *Federal Register*, vol. 68, no. 34: 8334-8381 (20 February 2003) URL: http://www.cms.hhs.gov/hipaa/hipaa2/regulations/security/default.asp

2. U.S. Geological Survey, 2004. “Magnitude 9.0 - Sumatra-Andaman Islands Earthquake Off the West Coast of Northern Sumatra, 2004 December 26 00:58:53 UTC” URL: http://earthquake.usgs.gov/eqinthenews/2004/usslav/

3. James Pilcher. “The Grounding of Comair, Why the airline computer system wasn’t replaced sooner isn’t clear” *Cincinnati Enquirer*, 2 January 2005. URL: http://news.enquirer.com/apps/pbcs.dll/article?AID=/20050102/BIZ01/501020362

4. NIST Special Publication 800-34, *Contingency Planning Guide for Information Technology Systems*. National Institute of Standards and Technology, US Department of Commerce. June 2002. URL: http://csrc.nist.gov/publications/nistpubs/index.html

5. Stephen Weil, Stephen Northcutt, and Mark T. Edmead. *Disaster Recovery and Business Continuity, Version 2.1*. SANS Press: 2004. URL: https://store.sans.org/

6. Stephen Northcutt, ed. *HIPAA Security Implementation, Version 1.1*. SANS Press: 2004. URL: https://store.sans.org/

7. Department of Defense Directive number 8500.1: *Information Assurance (IA)*. 24 October 2002. URL: http://www.dtic.mil/whs/directives/corres/html/85001.htm

8. Department of Defense Instruction number 8500.2: *Information Assurance (IA) Implementation*. 6 February 2003. URL: http://www.dtic.mil/whs/directives/corres/html/85002.htm

9. Department of Defense Manual number 8510.1-M: *Department of Defense Information Technology Security Certification and Accreditation (DITSCAP) Application Manual*. 31 July 2000. URL: http://www.dtic.mil/whs/directives/corres/html/85101m.htm

10. A Guide to the Project Management Body of Knowledge (PMBOK Guide) Third Edition. Project Management Institute: 2004. URL: http://www.pmibookstore.org/

11. *The 9/11 Commission Report, Final Report of the National Commission on Terrorist Attacks Upon the United States*. GPO: 22 July 2004. URL: http://www.gpoaccess.gov/911/

12. *NFPA 1600, Standard on Disaster/Emergency Management and Continuity Programs, 2004 Edition*. National Fire Protection Association. URL: http://www.nfpa.org/pdf/nfpa1600.pdf

© SANS Institute 2005 Author retains full rights.