Disaster Recovery Planning Under HIPAA – An Overview[1]

White Paper

Published October 2003 - Doug Thompson - MITG, Inc. - Quincy, IL

An Overview of Disaster Recovery Planning Under HIPPA Security Rules

---

Preface

MITG, Inc. (Midwest Information Technology Group is based in Quincy, IL and specializes in a variety of network and IT areas including data back-up, disaster recovery and alternate worksites. MITG is aware of the strain HIPAA laws place on providers and offers HIPAA compliant services covered by the Administrative and Security sections of the HIPAA law.

If your company is covered under HIPAA and/or relies on IT services to stay in business, this white paper is a must-read. For more information about MITG, see www.mitg.com.

I. Overview

On February 13, 2003, the Department of Health and Human Services announced the adoption of the **HIPAA Security Final Rule** (the Final Rule). The Final Rule, which establishes security standards to safe guard all electronic health information, was published in the February 20 Federal Register with an effective date of April 21, 2003. Most covered entities will have two full years, until **April 21, 2005** to comply with these standards.

In general, the intent of the Final Rule is to provide standards for the protection of electronic protected health information in accordance with HIPPA. In order to do this, covered entities are required to implement certain administrative, physical and technical safe guards. Those covered entities must ensure that data is protected to the extent feasible from inappropriate access, modification, dissemination and destruction.

As part of the Final Rule, covered entities must have a contingency plan in effect for emergencies. A contingency plan is the only way to protect the availability, integrity and security of data during unexpected events. The Final Rule calls for covered entities to consider how potential disasters could damage systems that contain electronic protected health information and to develop policies and procedures for responding to such disasters.

Typically, disaster recovery and business continuity planning is thought of simply as data backup and recovery. This is true, but not the only coverage. Just as important as data is the infrastructure related areas we more than likely take for granted. For example, where will people sit to do their job? How will they access a telephone, speak to clients, send and receive faxes and e-mail? Are there special requirements? Equipment, websites, tools or machines? All of these areas should be covered in a comprehensive Disaster Recovery/Business Continuity Plan.

While these things apply to any business dealing with client data, records, billing and other administrative tasks, it is now mandated by HIPPA for covered entities and compliance is not an option.

II. What is a Disaster Recovery Plan?

A disaster recovery plan (DRP) is a comprehensive list of actions to be performed before, during, and after any event that causes a significant loss of data resources. DRPs are the procedures for responding to an emergency, providing extended backup operations during the interruption, and managing recovery processes afterwards, should an organization experience a substantial loss of processing capability.

The primary goal of a DRP is to provide the ability to implement critical processes at an alternate site and return to the primary site and normal processing within a time frame that minimizes the loss to the organization, by executing rapid recover procedures.

Goals and Objectives of DRP

A major goal of DRP is to provide an organized way to make decisions if a catastrophe occurs. The purpose of the DRP is to reduce confusion and enhance the ability of the organization to deal with the crisis. DRP falls under two main categories:

- Data Processing Continuity Planning: Planning for a disaster and establishing plans to deal with it.

- Data Recovery Plan Maintenance: Keeping the plans up to date and relevant.

An *"if / then"* approach is used in building a comprehensive plan, taking into account both natural and un-natural eventualities that lead to loss of data. Natural elements such as lighting, fire, tornados or earthquakes can cause a loss of data as can equipment failure, disgruntled employee(s) or terrorist attack.

Severity of loss is also considered. What is the damage? Did we lose data, the system, our workspace, or our building? What is the recourse of each?

Data Processing Continuity Planning
There are several types of data processing continuity planning. The following, while not comprising all possibilities, gives a good idea of how an entity might cope with a disaster.

Hot Sites
Hot sites are defined as the combination of hardware, software, facilities, data communication lines and voice communication lines that are kept completely up to date and functional so that in the event that a disaster occurs personnel may simply transfer operations to the backup site and resume operations as if nothing ever happened.

This setup requires a high degree of maintenance and testing and, of course, is the most costly of all the types. What it offers is little chance of data loss or revenue from operations disruptions.

Warm Site
A warm site is a cross between a hot site and cold site. This setup consists of the facilities required to process data, but might not have the hardware, software, and other IT related configuration ready-made. The site may have servers/workstations, but not to the full extent that is required by the organization.

Cold Site
Cold sites are the most cost-effective type of the three, but rely on hardware, software, lines and other equipment to be brought in. This site simply provides the physical facilities required to continue operations, but none of the logical facilities.

The main benefit, again, to this type of site is the relatively low cost. However, the false sense of security that is built up when comparing this type of solution with others might lead to a detrimental collapse of operations when a disaster does strike.

Multiple Centers
Multiple centers rely on a technique known as shadowing, where all data is sent and/or processed at two or more locations. This allows organizations to continue operations in the event that one facility is struck by a disaster, albeit it will be under an increased workload. This setup is quite similar in design to a RAID setup on a server. Two systems work together to ensure operations are continued, complementing each other with some degree of redundancy. Should the primary site go down, the secondary site could continue all operations with little or no difficulty.

III. What is HIPAA?

"HIPAA" is The Health Insurance Portability & Accountability Act of 1996, Public Law 104-191, which amended the Internal Revenue Service Code of 1986. Also known as the Kennedy-Kassebaum Act, Congress passed this landmark law to provide consumers with greater access to health care insurance, to protect the privacy of health information, and to promote more standardization and efficiency in the health care industry.

While HIPAA covers a number of important health care issues, this paper focuses on the security requirements now codified in the Final Rule. These security standards support the protection of electronic information protected by HIPPA's privacy rules. As part of the administrative protocols under the Final Rule, HIPPA requires each covered entity to adopt and implement effective security measures to protect electronic data, including contingency plans to minimize the effects of a disaster.

IV. Who is covered by HIPAA?

The regulations define "covered entities" - those that must comply - to be:

- Healthcare providers (hospitals, doctor offices)
- Health plans (insurers, HMOs, group health plans)
- Healthcare clearinghouses (organizations that submit claims for providers)

Even if you are not one of these organizations, you still may be required to comply with HIPAA. If a covered entity does business with another organization, then that "business associate" is required to have the same level of security as the covered entity. The reason is that security is only as good as the weakest link. If a highly secure organization sends health data to a business associate with weak security, then the security of that data may be compromised. There are businesses that conduct business with covered entities that are not required to comply with HIPAA. For instance, if you are a housekeeping service that comes in and mops the floors at a covered entity, then you are not a business associate as defined by the regulations. The standard for whether you are a business associate or not is that you transmit individually identifiable health information. If you do not deal with health information, or if the health information is not individually identifiable, then you do not fall under the regulations.

V. What are the HIPAA Security Rules related to DRP?

The Security Standard, administrative procedures to guard data integrity, confidentiality, and availability, requires a "covered entity" to implement "*documented, formal practices to manage the selection and execution of security measures to protect data and to manage the conduct of personnel in relation to the protection of data.*" It further requires that these practices include a contingency plan, defined as "*a routinely updated plan for responding to a system emergency that includes performing backups, preparing critical facilities that can be used to facilitate continuity of operations in the event of an emergency, and recovering from a disaster.*"

VI. Creating a Plan

Ultimately, executive leadership of the "covered entity" is accountable. Their responsibility begins with effectively initiating the planning process by establishing a BCP/DRP Policy Statement naming the **Security Officer** and **Business Continuity Planner**, and providing a preliminary budget for the project. These measures must be documented and kept current and must include, at a minimum, the following requirements and implementation features:

- Conduct an "applications and data criticality analysis" (business impact analysis).
- Develop a data backup plan.
- You must have an emergency response plan.
- You must have a contingency plan.
- You must be able to recover applications and data in a reasonable amount of time.
- You must have a plan evaluation and revision program.
- An Evaluation/Accreditation - either internal or by third party
- A Chain of Trust Partner Agreement
  "Contract entered into by two business partners in which the partners agree to electronically exchange data and protect the integrity and confidentiality of the data exchanged."

Dept. of Health and Human Services: "Each organization would be required to evaluate its computer system(s) or network design(s) to certify that the appropriate security has been implemented. This evaluation could be performed internally or by an external accrediting agency (ex: **MITG**).

No specific recovery technology is required. Recovery is specified only in terms of a "reasonable" time frame with regard to your organization. It is very likely that over the next few years accepted standards would appear. As of this writing, based on legal opinions and various white papers researched, "reasonable" is defined as 12- 48 hours depending on the size of the entity and the depth of the interruption.

Section 164.316 requires covered entities to implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of the Security Rule. A covered entity may change its policies and procedures at any time. The section also requires covered entities to maintain the policies and procedures and any other required action, activity or assessment in written form (which may be electronic). Three required implementation specifications complete this standard, requiring that the covered entity must:

1. Maintain the documentation for six years from the date of its creation or the date it was last in effect, whichever is later;

2. Make the documentation available to those persons responsible for implementing the procedures to which the documentation pertains; and

3. Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information.

VII. Penalties

-For violations of transaction standards, penalties of up to $250 per person per violation and not more than $25,000 per person for violations of a single standard for a calendar year;

-Criminal penalties of up to $50,000 and one year in prison for obtaining or disclosing PHI;

-Criminal penalties of up to $100,000 and up to 5 years in prison for obtaining PHI under "false pretenses";

-Criminal penalties of up to $250,000 and up to 10 years in prison for obtaining or disclosing PHI with the intent to sell, transfer or use it for commercial advantage, personal gain or malicious harm.

VIII. Summary

Developing an effective, as well as compliant, Contingency Plan requires effort, planning, and commitment. Following an established guide that integrates the HIPAA standards will help to ensure compliance. Covered entities would be wise not to underestimate the effort involved in complying with the Final Rule. Since this is a major project requiring considerable resources from your organization, be sure to begin your planning now.

This plan should be dynamic and updated regularly to remain current with system enhancements and business process advances. Although the plan should be altered to stay up-to-date with the organization's processes, the "changes" themselves should be "change control managed" in order that appropriate review and approval protocols are followed prior to implementing all new changes.

MITG, Inc. (Midwest Information Technology Group)
PO Box 5208
Quincy, IL 62305
877-221-4253
217-214-7204 (fax)
www.mitg.com