

An Assessment of HIPAA Security Requirements On Disaster Recovery Planning

By VIRGINIA MILLER, CBCP, GCP & KIMBERLEY LEHMAN, CBCP

Although not yet published in its final form, the “proposed” Rule CFR 45 Part 142 Security and Electronic Signature Standards associated with the Health Insurance Portability and Accountability Act (HIPAA) addresses physical safeguards to “guard data integrity, confidentiality, and availability.” The mandates described in the proposed rule have been considered “best business practices” in the discipline of business and disaster recovery for decades.

As dependence on automated data is becoming the norm within most healthcare entities, organizations often only consider the recovery requirements of data centers. However, the recovery of automated systems is only one aspect in preparing for recovery and/or continuity of critical business processes. The Security And Electronic Signature Standards require “contingency planning” include conducting a risk analysis, determining critical applications and data, emergency operation plans, and plan testing and revisions. All affected entities – healthcare providers, health plans, and clearinghouses – must plan to implement all aspects of contingency planning.

Background

The proposed Part 142 Security and Electronic Signature Standards of HIPAA requires that all health plans, healthcare providers and health care clearinghouses that “maintain or transmit health information electronically establish and maintain reasonable and appropriate administrative, technical, and physical safeguards to ensure integrity, confidentiali-

ality, and the availability of the information.”

This white paper addresses the issues associated with the methodology of assessing system and data vulnerabilities, identifying critical business processes and data, determining recovery and continuity requirements, and designing recovery strategies.

PROPOSITION
The proposed Part 142 Security and Electronic Signature Standards of HIPAA requires that all health plans, healthcare providers and health care clearinghouses that “maintain or transmit health information electronically establish and maintain reasonable and appropriate administrative, technical, and physical safeguards to ensure integrity, confidentiality, and the availability of the information.”

security and electronic signature standards have taken that traditional approach and required it be expanded to include not only backup and off-site storage, but also, conducting risk assessments to determine vulnerabilities, validating safeguards, ranking applications and data as critical and sensitive, and developing a contingency plan.

Approach

Disaster recovery planning is a catch-all that includes all aspects of ensuring an organization and its relevant automated systems are protected and available. Businesses, whether healthcare or not, assume that the recovery of its computers constitutes a viable approach to

getting back in business after a catastrophic event such as fire, vandalism, natural disaster, or some other system failure. Disaster recovery should not be considered an IT responsibility or challenge. It is an enterprise-wide responsibility.

Except for the smallest of healthcare providers, there is a significant dependence on electronic data and information to conduct day-to-day operations for all “covered entities.”

Therefore, it is imperative that each organization conduct a risk assessment to determine where systems and data are vulnerable; quantify and qualify the impact to the business if the systems and data are not available; and, develop strategies to ensure recovery and continuity address the recovery of the critical business processes.

Challenge

Most organizations, whether they are defined as healthcare providers, payers, or clearinghouses, have discussed and/or developed strategies for addressing catastrophic events associated with data centers and networks. Disaster recovery planning is often a function and responsibility of the information technology departments, and is usually an unfunded mandate. Traditionally, data backup and off-site storage have been considered acceptable recovery strategies. The proposed

Definitions

Before embarking on the explanation of developing a “disaster recovery plan,” it is important to define the terminology used within the disaster recovery planning discipline and that, which has been described in the HIPAA Rule.

Disaster Recovery Planning: The technological aspect of business continuity planning. The advance planning and preparations that are necessary to minimize loss and ensure continuity of the critical business functions of an organization in the event of disaster.

CFR 45 Part 142 Proposed Security and Electronic Signature Standard defines a disaster recovery plan as “part of an overall contingency plan. The plan for a process whereby an enterprise would restore any loss of data in the event of fire, vandalism, natural disaster, or system failure.”

The difference in the two definitions is the primary reason most “disaster recovery plans” fall short. Disaster recovery is the “advance planning and preparation to minimize loss and ensure continuity of the critical business functions of an organization.”

The HIPAA definition does not address the need to determine the critical business processes that must be restored, and the priority of their restoration. This determination and prioritization of business processes is tantamount to ensuring the successful and cost-effective recovery of



an organization.

In addition, the Proposed Security and Electronic Signature Standard contradicts typical disaster recovery planning practices, by suggesting that a disaster recovery plan is “part of an overall contingency plan.”

This “part” suggests only to “restore any loss of data in the event of fire, vandalism, natural disaster, or system failure.”

It is unlikely that most healthcare organizations subjected to the scenarios above (excluding system failure) could effectively restore operations within a minimal timeframe. If a disaster recovery plan is designed to only recover the loss of data, there is no protection against loss of revenue or the negative exposure to its customer base and other business associates.

HIPAA does not recommend the determination of recovery time objectives (RTOs) for business processes, yet this step is essential to developing a viable disaster recovery plan that when activated, will provide restoration capabilities for more than the organization’s automated systems.

Automated systems are of little value to an organization if there are no accommodations made to recover the user community. Automated systems and data support the business enterprise.

The recovery guidelines described in the HIPAA Rule do not consider the need for advanced planning and preparation to minimize loss and ensure continuity of critical business functions.

Risk Analysis

The first step in designing a comprehensive, viable, and valid disaster recovery plan is to conduct a risk analysis. The purpose is to determine if existing security precautions and countermeasures are adequate to protect the healthcare organization’s mission critical data and assets as well as protected health information (PHI).

The assessment must consider the current physical and technological security environment in order to determine areas of risk that threaten the ability to operate. Data and information exchange internally and externally among the healthcare organization’s employees and business associates can present considerable privacy and data security issues.

HIPAA compliance requirements underscore the need to identify and mitigate areas of vulnerability that have been either assumed or overlooked by management in the past.

Risk mitigation strategies must be implemented to ensure the probability of vulnerabilities is reduced. A properly-completed risk analysis should provide a complete overview of the healthcare organization’s current security posture.

Business Impact Analysis

The next step in developing a disaster recovery plan is to conduct a business impact analysis (BIA). The BIA is referenced in the proposed HIPAA Rule as an “applications and data criticality analysis.” The purposes of a BIA is to specifically define and prioritize the healthcare organization’s business processes to determine which is most critical and define the minimum amount of tolerable downtime before significant impact. This minimum tolerable downtime becomes the RTO.

Typically, organizations focus only on the recovery of automated systems. The recovery of the systems does not constitute the recovery of the business.

Healthcare entities must consider the ramifications of only identifying and documenting critical applications and data, and not addressing mission-critical business functions, especially as patient records and data become increasingly automated. Once the mission-critical business processes and the associated automated systems are identified, then and only then can the best recovery (or continuity) strategy be determined.

Recovery Planning Strategies

Recovery requirements and strategies vary and should be selected based on the mission of the organization. Some organizations require continuous availability to patient information and data (e.g., hospitals); some organizations can tolerate a prolonged interruption (e.g., physicians’ offices). Therefore, a “one size fits all” strategy does not apply.

Backup tapes are not a recovery strategy. Strategies may include hot sites, mobile recovery units, electronic vaulting, equipment replacement, mirrored systems, alternate sites, etc. The disaster recovery plan must also include the

details associated with getting the business back up.

This includes identifying who will implement the recovery plan and emergency operations, where will staff report if the facility is destroyed (in whole or in part), what paper files are critical, what equipment is needed, (i.e., desktops, telecommunications equipment, printers, fax machines, etc.).

Once the strategy is determined and the plan written, it must be exercised to ensure it is viable and practical.

Conclusion

The Security and Electronic Signature Standards is a step in the right direction for ensuring that information security and recovery planning are considered as an integral part of protecting PHI and patient information.

However, the healthcare industry should closely evaluate the resources and expenditures incurred in order to satisfy the HIPAA requirements, remembering that HIPAA establishes the minimum requirements for protecting electronic healthcare information.

Limiting the recovery planning to “data backup and data storage” will not ensure the ability to recover critical information unless a means of accessing the information and recovering the user community is included.

All too often disaster recovery plans are confined to the data center. This is only one facet of “contingency planning.” Recovery planning must consider and include the entire organization and enable the users to access critical patient information in order to ensure timely patient care can be provided.



Virginia Miller is the director of technical solutions for Metro IT Solutions, headquartered in Virginia Beach, Va. A Certified Business Continuity Professional and a Gartner Certified Professional, she is responsible for Metro’s national HIPAA practice as well as the business continuity and project management practices.



Kimberley Lehman is a business recovery planning consultant for Metro IT Solutions headquartered in Virginia Beach, Va. She is a Certified Business Continuity Professional, and is one of the senior project managers of the business recovery planning team and the HIPAA compliance assessment team.

To comment on this article, go to 1501-10 at www.drj.com/feedback.