IT Contingency Plan to Meet HIPAA Security Standards

Save to myBoK

by Sandra Nutten and Chris Mansueti

HIPAA security standards require your organization to have a contingency plan. Here's the how-to for a plan that measures up.

The final rule for HIPAA security standards, published in the *Federal Register* on February 20, 2003, clearly states that a covered entity must protect the integrity, confidentiality, and availability of electronic protected health information (PHI). With the compliance dates on the horizon, this article explains how HIM staff can develop, maintain, and test a contingency plan to meet the security standards.

The One-minute HIPAA Security Pre-Test

1. What is your deadline for complying with HIPAA's security standards?
2. Why do you need a contingency plan for HIPAA security?
3. Who is responsible for making sure that your entity is in compliance with the security standards?
4. Where is your contingency plan—physically, where is it?
5. When do you invoke the contingency plan?
6. How do you prove that your contingency plan will work?

Kudos to anyone who can answer all six questions right now in 10 seconds or less. Most of us, however, are in the planning stage of HIPAA security compliance and may only have the answers to the first three questions.

By April 21, 2006, if you are a small health plan (under HIPAA, a plan with annual receipts of $5 million or less), or by April 21, 2005, for all other covered entities, you should know the answers to all six questions.

The Contingency Planning Process

The Centers for Medicare and Medicaid Services (CMS) define a contingency plan as "an alternate way of doing business when established routines are disrupted." CMS offers the following seven steps as general guidelines for creating that plan: (1) assess your situation, (2) identify risks, (3) formulate an action plan, (4) decide if and when to activate your plan, (5) communicate the plan, (6) test your plan, and (7) treat your contingency plan as an evolving process.[1]

In addition to planning against disruptions in routines, healthcare entities are required to develop a HIPAA security contingency plan in the event of a security breach that jeopardizes PHI. HIPAA security standards require covered entities to "ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits" (§164.306(a)(1)) and to "protect against any reasonably anticipated threats or hazards to the security or integrity of such information" (§164.306(a)(2)).

But HIPAA regulations specifically direct healthcare entities to develop and implement a number of safeguards that are categorized according to operational focus areas. References to contingency planning and contingency operations can be found in the sections on administrative safeguards (§164.308) and physical safeguards (§164.310). While there is no mention of contingency planning in the section covering technical safeguards (§164.312), it is this section that provides the standards that actually provide the secure environment.

Prior to HIPAA, there was no universal means with which to identify whether a healthcare business was securing information to the best of its ability. That is the crux of what HIPAA asks of healthcare providers now: secure electronic PHI to the best

of their ability, within reason and without bias. Defining, documenting, and demonstrating ability, reason, and nonbiased approach to electronic health information security is the cornerstone of HIPAA compliance.

The following HIPAA security contingency planning process has six fundamental components, usually taken in the following sequence:

1. Appoint members to the HIPAA security task force
2. Name a project manager from the task force membership
3. Establish task force protocols
4. Identify milestone dates, working backward from your internal compliance date
5. Define your method of analyzing risk for your entity
6. Develop, test, and maintain the contingency plan

Applying the principles of "define, document, and demonstrate," let's lay out the framework for the plan. Project plans can be created in very sophisticated and user-friendly software, but unless every member of the task force has mastered the application, you will find yourself wasting precious meeting time navigating the tool instead of navigating the content. A simple table or spreadsheet will suffice for initial contingency plan development. An example using the first five components of the planning process is shown in "The Contingency Planning Process, Parts 1–5".

Contingency Plan Standards

As noted above, the HIPAA security standard states that a covered entity must ensure the confidentially, integrity, and availability of electronic PHI. The standard also states that a contingency plan must be put in place and the implementation specifications of the contingency plan support one or more of the confidentially, integrity, or availability requirements.

"The Contingency Planning Process, Part 6" presents a continuation of the preceding plan, mapping out the process to completion using both required and addressable standards. Underneath each required action item is a section specifically illustrating how an HIM department can apply the law to its work.

A Practical Approach to Contingency Planning

In addition to the complying with the contingency planning standard within HIPAA security, healthcare organizations must also approach contingency planning with an eye on sound business practices. Organizations should implement a business continuity plan that fits their business operations, allowing them to continue to deliver care in case of disaster or system outage. Within an overall business continuity plan, a technology contingency plan must be implemented and tested to ensure that mission-critical systems, networks, applications, and data are available to support the business operations.

Complementary to the technology contingency plan, organizations must also develop contingency plans related to nontechnical aspects of their operations (e.g., work flow, staffing, physical facilities) as part of their overall business continuity plan. These aspects must be addressed to ensure they can continue to deliver quality patient care during a disaster or system outage. The following discussion focuses on the technology contingency plan related to systems, networks, applications, and data.

Business Impact Analysis and Risk Assessment

Most organizations do not have unlimited funds to invest in technical contingency plans. Limited funds must be spent wisely to ensure that organizational risk is minimized and that mission-critical applications and data are available in the case of an emergency.

To determine the best investment in a contingency plan, organizations should first conduct a business impact analysis (BIA) and risk assessment. This process also supports compliance with the HIPAA application and data criticality analysis (§164.308 (a)(7)(ii)(E)). During the BIA, each mission-critical application, system, and business process is inventoried and prioritized. This step, in turn, assists in determining the sequence of their recovery. The cost of down time is calculated for each entry on the list.

A risk assessment should be conducted to determine the business risk associated with the inoperability of each of these systems. Once organizations understand the risks and costs associated with down time, they can determine where to spend limited funds to ensure that the availability of the most critical applications is maximized and the business risk is minimized.

Disaster Recovery Planning

Upon completion of the BIA and the risk assessment, organizations are then in a position to develop a cost-effective disaster recovery plan (DRP). This plan supports compliance with the HIPAA requirement in §164.308 (a)(7)(ii)(B). At a base level, the proper policies, processes, and technologies must be put in place to ensure that electronic PHI is backed up regularly and can be restored (this supports compliance with the HIPAA requirement for a data backup plan in §164.308 (a)(7)(ii)(A)). Processes and solutions for good backup and recovery are well documented and should be standard procedure within IT departments.

The approaches and options for developing a DRP are much more diverse than those for backup and recovery. Consequently, it is a valuable exercise to assess the various disaster recovery options applicable to an organization's environment. Based on the BIA and the risk assessment, the most appropriate disaster recovery approach can be selected to ensure that critical applications are recoverable at acceptable levels of risk. This approach must cover emergency procedures, business and technical processes, organizational and staffing requirements, duplication and continued access to required physical assets. It must also address technical solutions that include duplicated systems, applications, networks, and data and the ability to switch processing from a failed system to the duplicate system.

Disaster Recovery Plan Implementation

After development, review, and approval of the DRP, the plan is ready for implementation. This stage verifies that all features are in place, preparing the organization against disasters.

Implementation includes the following components:

- **Technical implementation**—including backup and recovery systems, high-availability systems, duplicate networks, business partner and technology service provider availability (e.g., telecommunications providers), and sites to which processing for systems and staffing can be switched in the case of a failure
- **Procedural implementation**—including off-site storage of the DRP, backup and recovery procedures, off-site backup facilities, escalation procedures, recovery and fail-over procedures, and technical and nontechnical manual processes required when systems are unavailable (in compliance with the HIPAA requirement for a emergency mode operations plan, §164.308 (a)(7)(ii)(C))
- **Organizational implementation**—addressing organizational issues to ensure adequate response to a disaster, such as:
    - Assignment of specific roles and responsibilities in the case of an emergency
    - Proper training of all staff members on their roles in case of disaster or outage—both staff directly involved in the recovery process and those delivering healthcare services

Disaster Recovery Plan Testing

Testing the DRP is a crucial step, and further, it complies with the HIPAA requirement for testing and revision procedures (§164.308 (a)(7)(ii)(D)). On a basic level, testing backup and recovery of data must occur periodically and when new systems and applications come online.

Organizations must take a very structured approach to testing their plans. Testing must occur on a scale much larger than simply recovering information from a failed disk drive. Appropriate testing includes simulation of a disaster or major system outage. By nature, such tests may be disruptive to the healthcare delivery process, but there is no substitute to testing the DRP in order to uncover issues and problems that could occur in a real emergency. It is far less costly in time, money, and human capital to discover these issues during a simulated test than during a real disaster.

After issues and problems are identified and assessed, the DRP can be adjusted to correct the issues or minimize their impact. The DRP related to systems, applications, and networks should be tested on a periodic basis, with a portion tested every year.

For example, an organization may test their entire DRP every three years and one-third of the systems, applications, and network annually.

In addition to periodic testing, the DRP must be maintained and updated as organizational environments change. Facilities may be changed or added, new applications may be implemented, service providers may change, or the technical infrastructure may be upgraded. When these events occur, the DRP must be updated to reflect these changes. It may mean revisiting the BIA, or it may be as simple as retesting the DRP to ensure that the change has not altered recovery capabilities. Changes must be addressed in the context of the DRP, verifying that the DRP can accommodate the additions and changes in the case of a disaster or system outage.

Disaster Recovery Plan Executions

Once the DRP has been implemented, the organization is in a position to execute the plan in case of a disaster or system outage. Backup and recovery of data should occur on a regular basis as part of normal IT operations. Hardware failures are a regular occurrence, and recovery of data from these situations will occur. These are relatively normal, ongoing activities.

Executing a DRP in an emergency situation is an activity that most organizations would prefer to avoid. A sound DRP addresses “disasters” in all shapes and sizes—a system going down, telecommunication lines being severed by construction crews, a fire in the data center, a hurricane or earthquake, or an act of terrorism. Each of these events will trigger the DRP, and the organization will respond as the plan dictates.

The depth of planning and testing that went into the DRP will quickly become apparent during the emergency. After recovery is complete, organizations should assess their performance and identify areas for improvement. Incorporating improvements into the DRP is essential to ensuring improved performance in the case of another disaster or system outage.

Take the pre-test again with your HIM work force. As you carry out your compliance and contingency planning, document each action in your process. Your efforts will be rewarded if your organization ever finds itself enacting a contingency plan.

The Contingency Planning Process, Parts 1-5

	Action Item	**Definition**	**Documentation**	**Demonstration of Compliance**
1.	Appoint task force	a. Appointments to task force by the security officer (named by the CEO and endorsed by the board) b. Appointment shall be for a duration of at least 15 months c. Appointee shall be a full-time work force member or business associate	i. E-mail request with task force member’s response confirmed ii. Appointee will acknowledge time commitment in acceptance response iii. Task force appointment shall be included in job performance evaluation or business associate agreement (BAA)	Correspondence from work force participants and BAAs on file. Due Date: March 1, 2004
2.	Name project manager	a. Appointment by executive leadership or task force election	i. Project manager for HIPAA security contingency plan job description	Duties of project manager listed in job description, evaluated by executive leadership

				Due Date: March 15, 2004
3.	Establish task force protocols	a. Empower task force to develop HIPAA security contingency plan b. Task force may be identified as permanent or project-specific body c. Recurring, mandatory meeting dates and times to be established d. Authority to create, edit or amend policies and procedures specific to HIPAA security e. Define limits of authority: monetary or scope of change f. Define project documentation requirements and format—create status report template	i. Written task force charter, endorsed by executive leadership and/or board ii. Charter to include scope and limits of task force iii. Meeting dates and times agreed upon during initial session published (15 months minimum) iv. Task force charter validates approving body for HIPAA security contingency plan policies and procedures v. Limits of task force to be declared in charter—scope of task force identified vi. Written status reports will be submitted for each project deliverable	Task force charter published and kept with HIPAA security contingency plan documents Due Date: March 15, 2004
4.	Identify project milestones	a. Select end date for HIPAA security contingency plan compliance, preferably 30 to 60 days prior to the mandatory date b. Build project due dates to correspond to the internal compliance due date	i. Project plan documentation will be date specific	Project plan deliverables and variances will be documented in status reports
5.	Define risk analysis method	a. Task force will identify method to assign a risk value to each HIPAA security standard (both required and addressable)	i. Method will be published in task force meeting minutes and incorporated into a policy; associated procedures will be declared prior to security standard review	Each security standard will be analyzed for its risk value to the entity. Assignment of risk will be matched to each standard

The Contingency Planning Process, Part 6

	Action Item	Definition	Documentation	Demonstration of Compliance
6.	Contingency planning			
§164.308 (a)(2)	Assigned security responsibility	Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity	Task force charter will require members of the task force to acknowledge and support the security official with a public endorsement	Security official assignment
	HIM department	Name the person within your department that will be called by your entity's security official when a threat to your department occurs and establish a call-out roster to be used if more personnel are required to handle the emergency. Include volunteers in this list, if they already work in your department	Address the emergency call-out list in your monthly department meetings. Keep the list posted in the department, in the security official's office, and in an off-site location accessible to an HIM department staff member	Meeting minutes
§164.308 (a)(7)(i)	Administrative safeguards: Contingency plan	Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (e.g., fire, vandalism, system failure, or natural disaster) that damages systems containing electronic PHI	HIPAA security policy, *Emergency Response to Disasters Impacting Electronic PHI*	Policies and procedures written and approved by task force. Training of work force on policies and procedures to this policy completed. Procedures of the contingency plan tested on a regular basis, no less than annually
	HIM department	Identify what, if anything, is evacuated with	Add HIM-specificaction items to entity contingency	

		personnel if a direct threat occurs in the department	plan. Discuss all procedures in department meetings	
§164.308 (a)(7)(ii) (A)	Administrative safeguards: Contingency plan: Implementation specification: Data backup plan (required)	Establish and implement procedures to create and maintain retrievable exact copies of electronic PHI	Backup and recovery procedures	Implement backup and recovery procedures Test backup and recovery procedures on a regular basis
	HIM department	Identify where backup systems are located. Name the personnel who will be held accountable for assisting with the capture of redundant information back to operations	Add HIM specific action items to entity contingency plan. Discuss all procedures in department meetings.	Consider adding line items into HIM position descriptions that identify what the individual's duty will be in disaster recovery mode, including working at other entity locations until normal business functions are restored
§164.308 (a)(7)(ii) (B)	Administrative safeguards: Contingency plan: Implementation specification: Disaster recovery plan (required)	Establish (and implement as needed) procedures to restore any loss of data	Disaster recovery plan	Implement a disaster recovery plan Test the disaster recovery plan
	HIM department	Identify if any HIM staff will actually be required in the restoration process	Name personnel by position, name, and contact information. The duties of these personnel will be reassigned to other HIM staff until restoration process is complete	List of personnel who will be dedicated to the actual recovery actions to be given to security official
§164.308 (a)(7)(ii) (C)	Administrative safeguards: Contingency plan: Implementation specification: Emergency mode operations plan (required)	Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic PHI while operating in emergency mode	Emergency mode operations plan	Implement an emergency mode operations plan. Test the emergency mode operations plan

	HIM department	Inventory all HIM applications Rank each application as mission critical or mission noncritical	Mission-critical applications will be reviewed for HIPAA protections as they come back online by IT department, validated by HIM personnel Mission-noncritical applications in HIM will not be addressed	During a threat to PHI, all HIM staff will double check validity of data requests that are not via mission-critical applications Maintain a log of PHI requests, disclosures, and refusals during the emergency operations mode
§164.308 (a)(7)(ii) (D)	Administrative safeguards: Contingency plan: Implementation specification: Testing and revision procedures (addressable)	Implement procedures for periodic testing and revision of contingency plans	Contingency plan ongoing test plan Contingency plan ongoing maintenance plan	Test the contingency plan on a regular basis and document the results Execute the ongoing maintenance plan with input from the ongoing test plan
§164.308 (a)(7)(ii) (E)	Administrative safeguards: Contingency plan: Implementation specification: Application and data criticality analysis (addressable)	Assess the relative criticality of specific applications and data in support of other contingency plan components	Business impact analysis and risk assessment	Complete and document the business impact analysis and risk assessment
§164.310 (a)(2)(i)	Physical safeguards: Facilities access control: Implementation specification: Contingency operations (addressable)	Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency	Emergency facility access control plan	Test and document results of the emergency facility access control plan on a periodic basis
§164.312 (a)(2)(ii)	Technical safeguards: Access control: emergency access procedures (required)	Establish (and implement as needed) procedures for obtaining necessary electronic PHI during an emergency	Emergency access control procedures	
	HIM department	Inventory all HIM applications Establish role-based access procedure	Publish list of the HIM personnel by position and name, with contact	Role-based access during emergency operations will be defined as those

		for emergency operations	information, who are permitted to access electronic PHI during an emergency operation mode	HIM personnel who are permitted to function as gatekeepers of PHI--maintaining a disclosure log and tracking activity

Note

1. The CMS steps, which specifically targeted the October 16, 2003, deadline for transactions and code set compliance, may be found on the CMS Web site at www.cms.hhs.gov/hipaa/ hipaa2/general/default.asp#contingency_guide. See "Steps for Contingency Planning."

Sandra Nutten *(sandra_nutten@superiorconsultant.com) is senior management consultant and* ***Chris Mansueti*** *(chris_mansueti@superiorconsultant.com) is executive director at Superior Consultant Company, Inc.*

Article citation:
Nutten, Sandra and Chris Mansueti. "An IT Contingency Plan to Meet HIPAA Security Standards." *Journal of AHIMA* 75, no.2 (February 2004): 30-37.