

HIPAA Security Addresses Contingency Planning

By: James M. Myers

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) provides for the continuation of health insurance coverage to employees for a period of time, prior to their enrollment in a plan with a new employer. The latest rule published under HIPAA is the "Health Insurance Reform: Security Standards. This latest rule was published on February 20, 2003 and became law on April 20, 2003. For all "covered entities" with annual sales revenues greater than \$5M the new security rule becomes enforceable on April 20, 2005. The published security rule states "Covered entities, with the exception of small health plans, must comply with the requirements of this final rule 24 months after the effective date of this regulation. Small plans must comply with the requirements of this rule by 36 months after the effective date of the regulation." These dates are very important because the clock has already started for compliance – the clock is ticking. Failure to comply will result in both civil and criminal penalties for those covered entities caught in a non-compliance state. The below organizations that are included under Health & Human Services (HHS) definition of a "covered entity" (and thus required to comply with the law) comprise of the following:

- ◆ Indemnity insurers
- ◆ Health maintenance organizations
- ◆ Any organization that transmits health care claims
- ◆ Any organization that transmits health care payment and remittance advice
- ◆ Any organization involved with the coordination of health benefits
- ◆ Any organization that determines health care claim status
- ◆ Any organization that administers enrollment and dis-enrollment in a health plan
- ◆ Any organization that administers health plan premium payments
- ◆ Any organization that administers referral certification and authorization
- ◆ Any organization that administers first report of injury or health claims attachments
- ◆ Billing agents that handle the above activities on behalf of other covered entities

Contingency Planning

Within the final security rule is section 164.308 - Administrative Safeguards. A critical sub-part of section 164.308 is (7)(i) Standard: Contingency Plan. The contingency plan standard is:

"Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information."

Within the contingency plan standard there are five (5) implementation specifications that each covered entity must comply. These specifications are:

1. ***Data Backup Plan (Required)***
Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.
2. ***Disaster Recovery Plan (Required)***
Establish (and implement as needed) procedures to restore any loss of data.

3. *Emergency Mode Operation Plan (Required)*

Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.

4. *Testing and Revision Procedures (Addressable)*

Implement procedures for periodic testing and revision of contingency plans.

5. *Applications and Data Criticality Analysis (Addressable)*

Assess the relative criticality of specific applications and data in support of other contingency plan components.

A covered entity must analyze and assess whether each “addressable” specification should be implemented for each reasonable and appropriate situation. If the specification is reasonable and appropriate then it must be implemented. If it is not reasonable and appropriate, the covered entity must either implement another equivalent measure that is reasonable and appropriate or, if the standard can be met some other way, choose not to implement the specification. However, for each addressable specification not implemented the entity must document and validate the reasons for its choice.

Aligning each implementation specification with existing business contingency planning work efforts follows.

1. Data Backup Plan

Data backup is the ability to transfer existing business data from its host environment to a secondary environment. The intent of backing up data is to help ensure the availability of the second most critical element to any business - its data. The first most critical element to any business is its employees. At a minimum, every covered entity should support some form of data backup process. Backing up data should be viewed as storing the company data at a secondary location, and nothing more. Backing up data without verifying its integrity or the ability to re-store within a defined business time frame is a recipe for disaster. A recent survey stated that only 37% of companies that backup their data actually test its integrity and recoverability. However, of the 37% of companies approximately 77% of them fail to restore their data within the defined business recovery window or don't recover at all. Hence, less than 10% of companies succeed at data recovery based upon their existing data backup processes. Clearly, data backup falls short when attempting to recover vital business data. What's needed is a disaster recovery plan.

2. Disaster Recovery Plan (DRP)

In it's simplest form, one can say that disaster recovery is the ability for an enterprise to restore its vital and/or critical technology systems in the event of a business interruption event. The interruption event could be from human, technical or natural causes. The DRP is focused on Information Technology (IT) systems and encompasses vital and/or critical hardware, operating software, application software, plus any tertiary elements required to support the operating environment. The DRP must support the process requirements to re-store vital and/or critical company data inside the defined business requirements. However, the DRP is mainly focused on technology systems and does not take into consideration the overall

operating environment of the business. For this, an Emergency Mode Operation Plan is required.

3. Emergency Mode Operation Plan (COOP/BCP)

Think of your emergency operating plan as the umbrella action plan that defines how the business will operate under duress conditions. From a contingency planning perspective, this is normally called the Continuity of Operations Plan (COOP), or Business Continuity Plan (BCP). The intent of this action plan is to train and prepare employees of what they need to do when any level of business interruption event strikes. Key operating processes that link humans with technology are vital to the on-going operations of any business. The ability to proactively implement a defined action plan to maintain intra-company communications and access key emergency information is the impetus behind an effective emergency mode operating plan. Each action plan requires mock exercises inclusive with employee training.

4. Testing and Revision Procedures (BCP/DRP exercise)

A key goal of business continuity is to exercise each action plan to determine the covered entities vulnerabilities, and strive for continuous improvement to reduce those vulnerabilities. There's no such thing as a 100% guarantee that all business vulnerabilities will be eliminated. However, through a well-developed and process oriented exercise each entity can reduce the likelihood of unplanned business interruptions crippling their ability to maintain business operations. There are five (5) different types of exercises that can be performed.

1. Orientation
2. Tabletop
3. Internal Drill
4. Functional Drill
5. Full Scale

The questions that always come up are; how often should I perform an exercise and what type of exercise should I perform? Here are some guidelines.

1. Perform quarterly updates on resource information such as contact lists, equipment lists, vital records lists, etc. This type of information tends to change most frequently.
2. Perform semi-annual reviews on recovery strategies and procedures.
3. At a minimum, perform an exercise annually. An exercise should include alternate site tests (internal and functional), and walk through exercises (tabletop). Orientation should be done for each new employee and during the initial development of your contingency plan.
4. Reviews and updates should also be done whenever a significant change takes place, such as a reorganization, new HW or SW implementation, etc.

5. Applications and Data Criticality Analysis (BIA)

Professional contingency planners know that without performing a Business Impact Analysis (BIA) prior to developing either a BCP or DRP is a recipe for failure. The intent of a BIA is to identify, prioritize and assess technology systems, applications, data and processes within the daily operating environment. The BIA will identify the business's Recovery Time Objective

(RTO) and Recovery Point Objective (RPO) as defined by business deliverables. The RTO will state how much time a particular system or application is allowed to be “off-line” until this outage event negatively impacts the business. The RPO will state when the information recovery process begins and how much data may be lost between system backup timeframes. Also, the BIA should identify the “hard” financial losses incurred when experiencing a business interruption event. The output of the BIA is the cornerstone to developing an effective and efficient BCP and DRP.

Contingency planning is more than an Information Technology (IT) thing. It's a business mindset that should be infused across the operating environment of the enterprise. Yes, there is a mandated security rule that guides and directs covered entities to take action. However, Initiating appropriate action, identifying budget requirements, and integrating an action plan into the operating environment takes executive leadership and commitment. A vast number of business owners and executives today are either minimally prepared, have not reviewed their action plan in four to five years, are too busy to develop an action plan, are short on human resources, or simply don't know how or where to begin. The need for business continuity planning and support will continue to intensify, as business needs become more demanding. New and emerging technologies, customer and employee demands, and government regulation will further drive this need. Uncertain where to begin? Talk to a professional business continuity planner today to ensure tomorrow's business success.

James M. Myers is President and CEO of Contingency Now. A professional business contingency planning services company located in Overland Park, Kansas. You may contact Mr. Myers at 913-484-5317 or visit the web at www.contingencynow.com.