

GUIDE TO CONTINGENCY PLANNING

An Instructional Document Written by WorkSmart MD, Inc.

Extracted from the HIPAA Rx™ Compliance Software

The security rule outlined in the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act (HIPAA) requires covered entities to provide reasonable and appropriate administrative, technical, and physical safeguards to ensure the integrity and confidentiality of and protect the information against any reasonably anticipated threats or hazards to its security, integrity, unauthorized use, and disclosure. This includes a written contingency plan that addresses emergency situations.

As required in section 164.308(a)(7)(i) covered entities must develop a contingency plan that includes the following:

- Data backup plans
- Disaster recovery plans
- Emergency mode operation plan
- Testing and revision

While most healthcare organizations never experience a disaster, being prepared for such a disaster is of utmost importance in terms of both patient care and organizational survival. Should a disaster strike, however, a well-designed action plan will protect health information from damage, minimize disruption, ensure stability, and provide for orderly recovery. Not only does it help ensure compliance with HIPAA, but proper contingency planning can help healthcare organizations rise to other challenges facing the industry.

The purpose of this instructional document is to provide guidance in the formulation of a facility's disaster plan relative to the collection and protection of health information. This paper will outline the disaster recovery impacts of HIPAA and other issues on the healthcare landscape.

HIPAA: Contingency Planning and Disaster Recovery Requirements

A PRIMER ON CONTINGENCY PLANNING

The Role of the Contingency Planner

As the “Contingency Planner” of the HIPAA compliance team you are responsible for developing, implementing, and maintaining the business contingency planning program for the covered entity.

Contingency planners act as a focal point for their organizations in any situation involving contingency planning or emergency response. The contingency planner plans the integration of a series of tasks, procedures, and information that direct actions at the time of a business interruption in order to reduce confusion, improve communications, and achieve a timely continuation/resumption of business. Your skills and projects are essential assets for the covered entity.

The contingency planner's roles and responsibilities include:

- Setting strategic direction and plans for the organization to ensure effective emergency management.
- Integrating the contingency planning process across the organization when the nature of the business requires it.
- Coordinating and integrating the activation of emergency response organizations.
- Developing and maintaining testing and maintenance programs for all contingency planning functions.
- Providing training, maintenance, and support for approved contingency planning tools.
- Providing primary contact for their company to handle coordination response during a business interruption.
- Acting as a resource for contingency planning efforts within the company area of responsibility.
- Securing appointment, training, and backup of all contingency planning and response teams.
- Assisting in the design and maintenance of alternate sites.
- Maintaining currency of all contingency planning documentation, including all deliverables.

Introduction to the Planning Process

A business contingency plan is a set of procedures that defines how a business will continue or recover its critical functions in the event of an unplanned disruption to normal processing. The HIPAA security standards initiate business contingency planning to protect electronic health information and ensure that there is minimum disruption to business processes in the event of an emergency situation.

The basic steps to developing and exercising a business contingency plan include:

- Project initiation and management
- Risk analysis/reduction
- Business impact analysis
- Recovery strategies
- Developing the plan
- Exercise and maintenance of the plan
- Training and awareness program

Get Started

A viable business contingency plan cannot be developed overnight. Adopting a phased approach to planning in order to provide the most protection for the organization in the least amount of time is better. The process to formulate a viable contingency plan is shown in the following table.

Formulating the Plan

Emergency Notification List: Immediately

To respond to an emergency situation at all, you must first be able to reach the people in the covered entity who can and will respond.

Vital Records Backup And Recovery: Immediately

To be able to recover from a disaster situation, you must have access to your vital records at the time of need.

Business Impact Analysis: First Three Months

Identify business functions, the capability of each business unit to handle outages, and the priority and sequence of functions and applications.

Strategy Development: One To Six Months

Identify process, assess priorities, identify processes to be supported, document department strategies for recovery, identify resources required for recovery, and coordinate interdependencies.

Alternate Site Selection: One To 12 Months**Contingency Plan Development: One To 12 Months**

Including emergency response, restoring of critical business functions to normal business operations.

Testing, Plan Maintenance, Periodic Audit: Annually

Before the project can even start, it must have support of the principals of the organization. You must work with them to define and agree on the scope of the project. Once the scope is determined, you can estimate the project resource requirements and define a timeline and deliverables.

Make sure all employees are aware of the plan and its contents. Make certain they know and understand their business function classifications as they will be used during emergency situations. Build contingency planning awareness into your new hire orientation. Conduct tests with different groups. Awareness by all is the key. Share the responsibility.

Analyze Risk

Identify the risks for which you must plan. There are three primary elements in the risk equation: threats, assets, and mitigating factors.

Threats are events or situations that would cause financial or operational impact to the organization. These are measured in probabilities, such as "may occur one time in 10 years." Each threat has a duration of time that the business or operation would not be able to function in its normal manner, if at all.

Assets are composed of the physical assets that are owned by the organization and its financial assets as well. Revenues lost for the duration of the incident, additional costs to recover, fines

and penalties incurred, lost good will or competitive advantages all are components in the assets figure.

Mitigating factors are the protection devices, safeguards, and procedures in place that reduce the effects of the threats. They do not reduce the threat; they only reduce the **effect** of the threat. Examples of mitigating factors in use include uninterruptible power supplies (UPS) and generator backups for replacement power, sprinkler systems to control the spread of fire, and access card readers to control physical access to company space.

Some things to review during this process are the facility infrastructure, computer and communication recovery, and business function processes and components to help identify the kinds of risks and controls in place. During this phase, additional controls may be recommended to mitigate the effects of a particular risk identified.

Analyze Business Impact

The impact to the covered entity should be measured in operating impact, financial impact, and legal and regulatory impact. the covered entity will be forced to operate in a manual mode for a significant period of time following the business interruption. Information normally available at the touch of a button will require tedious research and manual labor. The efficiency of the covered entity will suffer, and management will be faced with making vital decisions to carry the operation through the crisis.

The covered entity may experience some serious financial losses as a result of the business interruption and many of those losses may not be covered by insurance. Should billing, receivable, and collections business functions be crippled by inaccessibility of information, cash flow will suffer. Management will not be able to manage working capital if they cannot determine what it is in a timely fashion. Risks are that lost patients will never return, the business' credit rating may suffer, and significant costs may be incurred for hiring temporary help.

The covered entity has contracts with outside suppliers, customers, and vendors. After a disaster, will you be able to fulfill the legal requirements of these contracts and pay the penalties if you can't? If your business is unable to meet reporting or filing deadlines to regulatory agencies (FDIC, state, federal), your business will incur penalties.

During this phase of the business contingency planning process, the planner will need to identify the critical functions within the business. These can be identified by listing all functions performed, determining the impact an incident would have on that function, and an estimate of the business loss for the duration of an outage. This process is often completed by conducting interviews with business functional managers and employees and/or by survey or questionnaire to the functional managers.

Remember financial assets as well as the physical. Lost revenues, additional costs to recover, fines and penalties, lost good will, and delayed collection of funds could be impacted in a disaster. Once you have determined the impact of an incident on a business function, you can

determine the recommended recovery timeframe for the function. Each function should be classified by the following:

- AAA: Immediate recovery. No down time allowed. Requires implementing an in-place, fully equipped, and staffed alternate site.
- AA: Up to four hours to recover but requires installed, in-place, functional alternate site which can be staffed and functional within four hours.
- A: Same day recovery required but can be set up anywhere (hotel room, home, etc.)
- B: Up to 24 hours downtime
- C: 24 to 72 hours recovery
- D: 72 hours or greater

As part of this process you also must identify the technologies that are owned and supported by the covered entity. This would include their network, servers, client/server based applications, etc. These must be identified as a business function, prioritized, and, if critical, must have a recovery strategy and procedures.

It is crucial that the internal and external dependencies for the business function be understood and documented. This includes identifying all the inputs to the function and where they come from, all the outputs of the function and where they go to, as well as system application dependencies.

Once the critical and necessary business functions have been identified, the next step is to establish the resources that are required to continue to perform those functions. In recovering from a disaster, there are normally two phases defined:

- Response — in the period immediately following the disaster, the emphasis will be to keep the business running at the minimum acceptable level.
- Recovery — in the longer term, the business will need to be restored to its original performance. Identification of all resources required to support the function is required to facilitate the longer-term recovery.

Plan Recovery Strategies

Once the critical and necessary business functions have been identified and their recovery requirements known, the next step is to establish the resources that are required to continue to perform those functions. During this phase of the business contingency planning process, you will use the information gathered in the business impact analysis to identify potential recovery options and their associated costs, present the options to management, and get agreement on the approach to be taken and to spend the required amount.

The options for achieving the recovery must be investigated, assigned a cost, and compared against the potential cost of failing to recover. Recovery strategies will be driven by the recovery timeframe of the function. Recovery options might include the following:

- Self-service: A business unit can transfer work to another of its own locations which has available facilities.

- Internal arrangement: Training rooms, cafeterias, conference rooms, etc. May be equipped to support business functions.
- Reciprocal agreements: Other business units may be able to accommodate those affected. This could involve the temporary suspension of non-critical functions at the business units not affected by the outage.
- Dedicated alternate sites: Third party location to accommodate critical function recovery.
- External suppliers: A number of external companies offer facilities covering a wide range of business recovery needs.
- No arrangement: For low priority business functions it may not be cost-justified to plan to a detailed level. Provided good business judgment is used and the risks are understood and accepted, it is reasonable to have no formal arrangements in place.

The minimum requirement would be to record a description of the functions, the maximum allowable lapse time for recovery, and a list of the resources required. The above options relate first to the availability of space and second to the availability of equipment and supplies with which to perform business functions. With some it also will be necessary to have arrangements with suppliers to provide equipment, supplies, services, and personnel. In all cases, arrangements must be in place for the recovery of vital records and documents.

The backup and protection of all vital/critical records is necessary to ensure their availability after a disaster occurs. The storing of vital/critical records offsite in a time-synchronized way allows management to have information with which to rebuild their business functions. During this phase of the planning process you need to determine:

- What are your business' vital records?
- Where are they stored?
- Are they backed up? How?
- How frequent are the backups?
- What is included in the backups?
- How can you obtain the backups?
- Who is authorized to retrieve them?
- How long will it take to retrieve them?
- Where will they be delivered?
- How long will it take to restore them?
- Who will restore them?

Document the Plan

Once the recovery strategies have been agreed on, the plan must be defined and documented. The organization should be flexible enough to respond to any type of incident. The two major scenarios you must plan for are as follows:

- The building you physically do your work in is not available to you and you must recover at an alternate site.
- The systems services you depend upon are not available and you must continue the critical functions without them.

The plan must include the following:

- An introduction, explaining why the plan is necessary and detailing its scope: who is included, and the range of events covered.
- A definition of the crisis management structure, giving details on the roles and responsibilities of everybody included.
- Procedures to be followed in the event of the disaster. These would include an alert process when an incident is first discovered, incident or damage assessment, declaration procedures, notification procedures, and team procedures.
- Location and procedures to be followed to activate the command center.

The contingency planner must define the teams necessary to support the recovery. A combination of one or more of the following teams is generally used, depending on the size of your organization and the number of critical functions to be recovered.

- Executive team: senior executives in the business unit who have overall responsibility to your company for the recovery of the critical functions.
- Management team(s): operate in the command center and are responsible for managing and controlling the recovery efforts.
- Response team(s): generally one team for each critical function. These people go to the alternate site and/or execute the recovery procedures.

Each organization must have an emergency notification list. This list contains the phone numbers, beeper numbers, home numbers, etc. of each team member, as well as the contact list for internal and external vendors, internal or external customers, and other commonly used numbers that may be needed in a disaster (corporate travel agent, alternate site contacts, security, corporate communications, offsite storage vendors, etc.).

Each plan must have documented procedures for handling an incident that may result in the activation of the business resumption plan. It must document how an incident is identified; who is notified; how and by whom damage assessment or business impact are determined; who can make the decision to declare a disaster; and procedures for declaring the disaster. The plan activation procedures must include procedures for alternate site notification, offsite storage retrieval, emergency notification to the teams, and procedures for activating the command center(s).

Once the plan has been activated, a general action plan that summarizes the tasks to be executed to implement the recovery process should be included in the plan. In addition, a checklist for each team member, detailing recovery procedures for each critical business function need to be developed. These procedures need to be detailed enough that someone with a similar skill set should be able to execute them without having ever performed the task before.

Documentation on how communication will be handled both to internal customers and to external customers or clients is critical during the recovery process. It is very important that employees understand how to deal with the media and how to discuss the incident with customers on the phone or in person. Procedures for handling media and customer communications must be included in the plan.

For insurance purposes, it is important that costs associated with the recovery effort be tracked as well as payment for purchases of needed supplies and replacement equipment be expedited. Procedures for handling finance issues must be included in the plan.

Human resource issues such as employee injuries, fatalities, family issues, trauma, etc. must be managed during the disaster. Procedures for handling these issues must also be included in the document. Appendices can be used to contain common procedures, alternate site locations and directions, company-approved hotels, and any other information that may be useful in a disaster.

Exercise, Maintain, and Train

The plan should be exercised and tested on a regular schedule. Exercises also provide the opportunity to train the staff on the procedures documented in the plan. Plan reviews should be performed on a regularly scheduled basis and must occur at least annually. These reviews should be linked where possible to ensure the details of significant business changes are correctly incorporated into the plan. Results of the review should be formally reported and, where appropriate, the plan should be updated.

Emergency Response Steps for Contingency Planners

After you receive notification of an incident or potential business interruption:

1. Write down any specific information that will be helpful when you need to relay the facts to others, including building, location, area of impact (i.e. third floor of 260 Franklin, mailroom area, six people in area).
2. Ask the caller if they know how long the situation is expected to last/continue (power outage, picketers, water leak, etc.).
3. If the caller does not confirm that security is aware of the situation, initiate the call to the company security or contingency planning.
4. Escalate to executive management as appropriate (determine the need for implementing the business resumption plan). Keep a log of all people you contact with approximate times listed for each contact.
5. Assess the situation and determine if a command center meeting is necessary.
6. Verify if the command center will be used (see notification list for locations).
7. Inform contingency planning of your current location (i.e. town) and estimated time of arrival at the command center location. Review communication modes (i.e. pager number, CNS, conference bridge, command center number, etc.) for yourself and the caller.
8. Inform the caller of the other names that you will be contacting regarding the situation.
9. Contact the other names on the notification list.
10. Remind them to bring a copy of their contingency plan.
11. Verify the communication modes and arrival times at the command center.
12. Proceed to the command center.
13. Ensure that all critical functions and roles are covered. If not, appoint alternatives and supply them with instructions and copies of the appropriate plan(s).
14. Update senior management of actions taken/to be taken.

15. Review the progress and future actions of the command center coordinator to ensure adequate coverage.

Contingency Buzz Words

Critical Business Functions

- Those functions considered essential to the ongoing operation of the company or business unit.
- If these functions could not operate, there would be a significant adverse impact upon the products/services provided by finance and administration.
- Also includes anything that might significantly impair the financial integrity of the company.

Command Center

- Location set up for management and BCP to operate from during emergency situations.
- Maintain contingency plan document and other needed resources at command center.

Alternate Site

- A location where critical business functions can resume processing in the event of a business interruption.

Vital Records

- All data and information required to support a business function, i.e., historical, regulatory requirements. Includes:
 - Policy and procedures manuals
 - Input documents or data
 - Manuals for software and other applications
 - Vendor/customer list
 - Telephone/rolodex
 - Backup tape files
- Should be maintained off-site at third party vendor or command center.

Every company, and each of its locations, is susceptible to disaster. Disk crashes, power outages, and communication losses are all minor disasters that happen on an occasional basis, and most of us have a backup plan ready to put into effect.

The Blueprint for an Effective Plan

1. Identify business representatives.

Business unit plans should identify a business representative authorized to determine recovery requirements. This person should also have the power to approve funding.

2. Establish client participation and user acceptance.

The recovery team will consist of individuals who are currently assigned to the day-to-day support of the product or the application being recovered. This team will also need the support from the infrastructure engineering teams, as well as the application development organization. Client participation in plan development and user acceptance testing is required in order to obtain successful results.

3. Locate vulnerabilities in the technology infrastructure.

In the past, the words "risk analysis" have meant the process of identifying and minimizing the exposures to certain threats that an organization may experience. Traditionally, this process would not include vulnerabilities in the technology infrastructure. With today's businesses relying on technology, a good risk analysis is fundamental to a successful business continuity program.

4. Perform a business impact analysis.

A business impact analysis (BIA) outlines the consequences of an interruption to the business and other interdependent applications and serves as a benchmark for funding decisions and strategy development. Some of the criteria used are public image, customer confidence, market share, and regulatory and financial penalties. The critical functions, their recovery priorities, and their interdependencies must be established so that the recovery time objective (RTO) can be set.

5. Identify technology requirements.

The technology requirements for a successful recovery must include hardware and software equivalents to production. Careful calculations during this phase will ensure that the contingency environment mirrors the production environment.

6. Develop a recovery strategy.

The business needs will dictate the recovery strategies and recovery time objectives. Recovery time objective is defined by the business as the amount of down time their application can endure. The recovery time requirements of interdependent applications must be taken into consideration. Two key components to any contingency program should include a strategy to back up and restore vital records.

7. Create vital records and provide offsite storage.

A critical component in plan development is the selection of backup and restoration software capable of storing and successfully retrieving data. Without this, there is no business continuity program. Backup scheduling must include an off-site storage location.

Once the data is carefully backed up, it must be accessible in the event that the facility is not accessible. There are bonded commercial storage vendors that provide security and offsite data storage. Data is usually retrieved for daily restores as well as disaster recovery testing.

8. Build the plan.

A critical step in plan development is actually building the plan. Full cooperation from all of the teams is necessary to create a viable recovery plan. This is where the majority of the work will be performed. Any group or individual providing a product or service on a day-to-day basis should also be responsible for supporting the service during a contingency event.

9. Perform a functionality test.

Once requirements have been defined, a strategy has been developed, and the plan has been built, it is time to test the functionality of the plan. This effort will involve most of the teams that have business continuity plans and is designed to demonstrate whether or not the predefined business objectives could be met within the recovery time objective. Each team representative will then verify its portion of the plan. The next and most critical step of all is user acceptance testing.

10. Conduct user acceptance testing.

Each user should create a test script designed to validate the accuracy and performance of its application in a contingency environment. The test scripts should not be a bare bones representation of the production environment. The script should give a clear indication of whether or not they can do business as usual as stated in their recovery requirements.

11. Obtain user evaluation sign-off.

Users should be asked to provide their views on the testing process, as well as on the results of the test. The users should also provide comments regarding lessons learned and improvements and modifications that they would like to see as a result of the test. A user sign-off sheet should be provided for this purpose and must be signed off by a manager of the business. The business contingency manager should compose a post-test report stating if the objectives of the test were achieved. All plans must be tested on a regular basis in order to be contingency compliant.

The business contingency plan should consist of several interdependent parts, described below.

Part 1: The Business Impact Analysis (BIA)

The business impact analysis identifies critical functions the business needs to perform to stay in business (make money, provide mandated services); identifies risks to critical business functions and rates the risks according to probability of occurrence and impact on the business; recommends avoidance, mitigation, or absorption of the risk; and identifies ways to avoid or to mitigate the risk.

Identifying critical business functions requires management input. Identifying risks, prioritizing risks, and determining measures to avoid or to mitigate risks is done with help from the people performing the functions, the subject matter experts (SMEs). These people know most of the risks on both sides of the function—the functions that feed their function, and the functions their function feeds. The business continuity planner—the planning SME—makes certain to discover all risks.

Once the risks are discovered and prioritized, the planner recommends what he or she considers an appropriate approach. **Avoiding** a risk is an obvious option, but often is not the best option. It usually is the most expensive to implement and to maintain. Redundant operations or a "ready-to-do-business" hot site are typical avoidance options. **Mitigating** a risk also is an obvious choice. Less expensive than avoidance, mitigation typically puts work-around procedures in place while resources are restored to a "business-as-usual" condition (which may be the same as, or better than, prior to the disaster condition). **Absorbing** a risk is a viable option when resources are outdated or when a business function is due for a major revision, replacement, or termination. With insurance absorbing some of the replacement costs, the aftermath of a disaster event may be the most cost-effective time to replace outdated resources.

While management makes the avoid-mitigate-absorb decision based on a number of factors outside the scope of this paper, the BIA should include primary and alternate recommendations based on each business function's criticality.

Phase 2: The Disaster Recovery Plan

The Disaster Recovery plan includes identification of disaster recovery primary and alternate team members and their specific duties, including executive management roles; notification procedures and alternate meeting site locations; work-around processes to keep the function operational while damaged resources are being restored to a "business-as-usual" condition; a contact list of all personnel and the functions they are qualified to perform; identification of all internal and external vendors and each vendor's primary and alternate contacts; and report forms (expenses, activities, etc.).

The disaster recovery plan design is as critical as the information. The people using the plan will be under pressure from the disaster condition; it must be easily accessible and grouped logically.

Phase 3: Training and Testing

Training and testing includes developing a test methodology; simultaneous testing and training of the disaster recovery team; business contingency plan revision; and simultaneous testing and training of the disaster recovery team. In addition to assure that the disaster recovery team members—both primary and alternate—know what to do, testing under increasingly realistic conditions helps to develop confidence. The best way to avoid panic during a disaster event is to be thoroughly trained and confident.

Testing is an ongoing event; there should be scheduled exercises and surprise exercises. Since testing interrupts business functions (if only by the absence of certain personnel), executive management support is critical. However, the price for not testing is a worsened disaster condition.

Maintenance

Maintenance requires a policy that defines a two-prong schedule. Maintenance, plan review, and updating are performed on a regular basis. Frequency is determined by the business' dynamics. Annual review is the minimum. Maintenance also is performed when triggered by certain events. These events include changes to equipment, personnel, policies, procedures, product, vendors, and any other areas that impact a critical business function.

Vendors

All businesses depend on vendors—from utilities and suppliers to distribution channels. Vendors directly or indirectly impact most critical business functions. The business continuity plan must include a "gap analysis" of each vendor's business continuity plan. Your plan is defective if the vendor lacks a plan, has never tested its plan, fails to maintain its plan, and fails to perform a gap analysis on its vendors' plans (ripple effect).

SUMMARY AND CONCLUSION

Contingency planning is required by the HIPAA security rule and is a critical business component. Disasters can strike anywhere and effect any organization. Threatened by fire or flood, malicious attack or targeted sabotage, the world today is a volatile and risky place.

To operate successfully in this environment, covered entities must consciously consider and implement disaster tolerant solutions that allow them to protect the valuable information assets of their organizations and to keep doing business throughout a crisis.

Your organization may want to seek outside help if it does not have the technical expertise or time to develop its business contingency plans. This help can include professional consultants, system vendors or service providers, or all three. The great benefit of this approach is that the work gets down on time. Using outside help allows internal people to focus on day-to-day operations.

For the most part, most disasters can be organized under one of the following three categories: loss of information, loss of access, or loss of personnel. Most contingency planning is based on common sense, and need not become a bureaucratic drill. By carefully reviewing your organization's vulnerability to a series of likely contingencies, it is possible to reduce risks to a manageable whole.