



# Contingency Plan

HIPAA Security ♦ November 2003

## Standard Requirement

As part of their administrative safeguards, covered entities must implement a contingency plan. The [Security Rule](#) defines a contingency plan as “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 \(EPHI\)](#).” In the modern world, organizations that deploy computerized patient record systems should assume that disasters happen. Thus, a contingency plan is a very important element in a covered entity’s risk management plan. This standard requires a covered entity to create and periodically update a contingency plan.

This standard includes five [implementation specifications](#). The first three are required, and the last two addressable:

- data backup plan;
- disaster recovery plan;
- emergency mode operation plan;
- testing and revision procedures; and
- applications and data criticality analysis.

## Implementation Specifications

The first required implementation specification under this standard is data backup plan. This is to ensure that information will not be lost in the event of a major system loss. Under this specification, a covered entity is required to determine what information requires backup, determine the appropriate way to backup the information (magnetic tapes, paper, or other form), determine a way to maintain the backups (offsite, in an air conditioned compartment or other conditions), and determine how long the backups should be maintained. The contingency plan must document the backup policies and procedures and covered entities should review and update them as necessary.

The second required implementation specification is disaster recovery plan. This requires a covered entity to establish, and possibly implement procedures to restore any loss of data. Each covered entity must have a plan for recovering from a disaster. Possible disasters include fire, vandalism, natural disaster and system failure. Any one of these events could damage PHI and ultimately, threaten patient care and healthcare operations. Covered entities must include in their contingency plans a strategy and method for recovering lost or inaccessible PHI in a timely manner after a disaster.

The third required implementation specification is emergency mode operation plan. This requires a covered entity to establish, and possibly implement procedures to protect



# Contingency Plan

## HIPAA Security ♦ November 2003

electronic PHI even while operating in emergency mode. Fire, vandalism, natural disaster or system failure sometimes damage the safeguards put in place to protect information or prevent their use. This implementation specification requires covered entities to develop and implement when needed, alternate means of protecting health information during an emergency.

The fourth implementation specification addresses procedures for periodic testing of written contingency plans to look for weaknesses, and then revise the plan if necessary. Because this implementation specification is addressable, compliance depends on the outcome of a covered entity's risk assessment. Covered entities should test their plans on a periodic basis to refresh the training and to ensure that the plans remain appropriate as business processes and the environment change over time. If covered entities do not include a testing and revision process in their contingency plan, they must explain their reasons in their risk management plan.

The last implementation specification is applications and data criticality analysis. This assesses the relative importance of specific applications and data that support other contingency plan elements. The results of this analysis help to assign priority to information resources and determine the best strategy to protect those resources. While this specification is addressable, it is hard to believe that an emergency mode operation plan would not include this.

Like all the other standards, the elements of these implementation specifications should be based on each covered entity's particular circumstances. "Each entity needs to determine its own risk in the event of an emergency that would result in a loss of operations. A contingency plan may involve highly complex processes in one processing site, or simple manual processes in another." ([Final Rule, p.8351](#))

See also:

[45 CFR 164.308\(a\)\(7\)](#)

Federal and DoD regulations that support this standard

[OMB A-130 App. III](#)

[DoDI 5200.40](#)

[DoD 8510.1-M](#)

[DoDI 8500.2](#)