U.S. DEPARTMENT OF
HEALTH AND HUMAN SERVICES
OFFICE FOR
CIVIL RIGHTS

March 2018

Plan A… B… Contingency Plan!

The purpose of any contingency plan is to allow an organization to return to its daily operations as quickly as possible after an unforeseen event. The contingency plan protects resources, minimizes customer inconvenience and identifies key staff, assigning specific responsibilities in the context of the recovery.

Contingency plans are critical to protecting the availability, integrity, and security of data during unexpected adverse events. Contingency plans should consider not only how to respond to disasters such as fires and floods, but also how to respond to cyberattacks. Cyberattacks using malicious software such as ransomware may render an organization's data unreadable or unusable. In the event data is compromised due to a cyberattack, restoring the data from backups may be the only option to recover the data and restore normal business operations.

What Does a Contingency Plan Do?

✓ **Contingency Plan:** Focused on the steps to respond and recover operations in the event of an emergency or other disruption to normal operations. Its major objectives are to ensure: ***(1)*** the containment of damage or injury to, or loss of, property, personnel, and data; and ***(2)*** the continuity of the key operations of the organization.

Contingency plans aren't just a good idea; regulations for certain industries require contingency planning. For example, the HIPAA Security Rule requires that HIPAA covered entities and business associates establish and implement a contingency plan.[1]

What's Required for a HIPAA Contingency Plan?

✓ **Disaster Recovery Plan:** Focused on restoring an organization's protected health data.

✓ **Emergency Mode Operation Plan** (or ***Continuity of Operations***): Focused on ***maintaining and protecting critical functions*** that protect the security of protected health data.

✓ **Data Backup Plan:** Focused on ***regularly copying protected health data*** to ensure it can be restored in the event of a loss or disruption.

[1] 45 CFR § 164.308(a)(7).

Items to Address as Part of a HIPAA Contingency Plan

- ✓ **Applications and Data Criticality Analysis:** Focused on ***identifying*** what applications and data are ***critical for the contingency plan***.
- ✓ **Testing and Revisions:** Focused on testing your contingency plan and revising any identified deficiencies.

Key Steps on the road to Contingency Planning:

Make it Policy: A formal policy provides the authority and guidance necessary to develop an effective contingency plan.

Identify what is Critical: Knowing what systems and data are critical to operations will help **prioritize** contingency planning and minimize losses.

Identify Risks, Threats and Preventative Controls: Perform a risk analysis to identify the various risks that your business may face. What has the potential to significantly disrupt or harm your operations and data?

> **Contingency Plans & Risk Analysis:** The need for contingency plans appears as a result of a thorough and accurate analysis of the risks that your organization faces. The end result of a risk analysis can provide a list of potential threats, risks, and preventative controls. Prioritization of critical systems and information will help identify where to focus planning efforts.

Create Contingency Procedures: Establish the specific guidelines, parameters, and procedures when enacting the contingency plan and for the recovery of systems and data. Here's where the Disaster Recovery Plan, Emergency Mode Operation Plan and Data Backup Plan will fill in the overarching contingency plan. ***Keep in mind:***

- The goal is to maintain critical operations and minimize loss.
- Define time periods – What must be done during the first hour, day, or week?
- Establish Plan Activation – What event(s) will cause the activation of the contingency plan? Who has the authority to activate the contingency plan?
- Use plain language – the plan should be understandable to all types of employees.

Operationalize & Maintain the Plan: Integrate the plan into normal business operations.

- Communicate and share the plan and roles and responsibilities with the organization.

- Establish a testing (exercise) schedule for the plan, to identify gaps and ensure updates for plan effectiveness and increase organizational awareness.
- Review the plan on a regular basis and situationally when there are technical, operational, environmental, or personnel changes in the organization.

Don't wait for a disaster to happen before designing and implementing a contingency plan.

Additional Contingency Planning Resources:

Office for Civil Rights (OCR):

- https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/adminsafeguards.pdf?language=es

National Institute of Standards and Technology (NIST):

- https://csrc.nist.gov/Topics/Security-and-Privacy/security-programs-and-operations/contingency-planning
- https://csrc.nist.gov/publications/detail/sp/800-34/rev-1/final **(SP 800-34 rev1 and Supplemental Material)**

Assistant Secretary for Preparedness and Response:

- https://www.phe.gov/Preparedness/planning/hpp/reports/Documents/hc-coop2-recovery.pdf