Data Security Policy - Contingency Plan

PURPOSE

To provide principles and guidelines for how emergency response procedures and contingency plans will be created, adopted, followed, and maintained.

SCOPE

The Contingency Plan Policy will cover Organization's**:**

- Data backup plan
- Disaster recovery plan
- Emergency Mode Operation plan
- Roles and Responsibilities
- Related Forms, Plans, and Documents
- Related Policies
- And Relevant Regulations, Standards, and Criteria

POLICY

Contingency plans, policies, and procedures are designed to guide Organization through emergencies and disasters that could affect the business.

During emergencies or disasters, systems and physical assets containing PHI and ePHI may be damaged or disrupted in some way. Organization's contingency plans will make sure that we are prepared for an emergency.

Your contingency plan must include all of the following components.

Data Backup Plan

Organization will create a data backup plan or procedure, which describes the process for backing up information systems and data. Backup frequency for each system is determined by the criticality of the system and impact of data loss, as defined in each system's risk analysis.

Disaster Recovery Plan

Organization will adopt and follow a Disaster Recovery Plan, which describes how the business will recover from an emergency or disaster event. This written plan makes sure that Organization can recover from the loss of data or disruption due to an emergency or disaster such as fire, vandalism, terrorism, system failure, or natural disaster affecting systems containing sensitive or protected information, including ePHI.

Emergency Mode Operating Plan

Organization will adopt and follow a written Emergency Mode Operating Plan, also known as a Business Continuity Plan, which directs how Organization and its employees should operate in an emergency scenario. The plan will cover how PHI and ePHI will be secured and handled while Organization remains in emergency mode.

PROCEDURES

Organization's Contingency Plan Policy will be reviewed and updated at least annually, or when significant changes occur.

Data Backup Plan

Organization uses a backup tool to manage digital backups where feasible.

Organization will create and maintain retrievable exact copies of ePHI and other data necessary for operations. Backups are sufficient to restore information systems to a recent and operational state. Organization will hold these backups offsite in a secure location, or with a HIPAA-compliant cloud vendor.

Organization will implement backups and replication for all cloud storage (Google, Microsoft 365, Dropbox, etc.) and cloud services (AWS, GCP, Azure, etc.) used.

Organization performs backups of systems and data containing sensitive and protected information at least daily, or continuously when possible.

Organization secures any backup media in a safe location separate from the system that created the backup. We track backup locations, activity, and files. You may use The Guard's asset module to assist with this control activity.

All backups are secured and encrypted, with any exceptions documented.

Disaster Recovery Plan

Organization will develop, adopt, and follow the disaster recovery plan consisting of the following components:

- **A communication plan** that includes:
    - Who should be notified of a disaster
    - Employee contact information
- **Data backups** and where they are stored
- **Role descriptions** that cover:
    - Who is responsible for assessing damage
    - Who is responsible for system recovery
    - Who is responsible for other key roles in the recovery process
- **A detailed asset inventory,** or a way to access it, that includes details about:
    - Computers
    - Workstations
    - Devices
    - Hardware
    - Printers
    - Scanners
    - Other **Organization** assets
- **An equipment plan** for protecting:
    - Desktop and laptop computers
    - Devices
    - Printers
    - Other equipment that can be damaged in a disaster
- **A data restoration priority plan** that lists systems in the order they should be restored in, if feasible
- **A vendor communication plan** that includes:
    - A list of vendors that need to be contacted
    - Vendor contact information
    - Vendor communication prioritization (e.g., who should be contacted first)

- **A plan for document storage, access, training, and review** that includes:
    - Where the plan will be stored on-site
    - Where the plan will be stored off-site
    - Where employees can find the plan
    - How employees are trained on the plan and how often
    - When the plan is reviewed and updated

Emergency Mode Operating Plan (Business Continuity Plan)

Organization will adopt and follow a written business continuity plan, also known as an Emergency Mode Operating Plan that includes:

- **Definitions of critical business processes** that need to operate during an emergency for the security of ePHI and other sensitive information
- **Designating who should be responsible** for recovering and/or continuing critical business process operations
- **Steps for recovering and operating** critical business processes
- **Testing the plan** for continued effectiveness and opportunities for improvement

We will test the Emergency Mode Operating Plan at least annually. Changes to the plan require approval from the Security Officer.

Periodic Testing and Revision of Contingency Plan

The data backup plan, disaster recovery plan, and business continuity plans will undergo periodic testing and revision.

- Each plan will be tested no less than annually.
- Each plan will be tested whenever changes are made to the plan. Testing will include workforce members, to ensure they understand their roles and responsibilities. If testing reveals that the Contingency Plan will be ineffective in the event of an emergency or other occurrence, the Security Official will revise the plan accordingly.
- Backup plan testing will include backup media testing. **Organization** will ensure that backup media will be tested periodically for accessibility and integrity. If there are readability issues, backup media will be replaced to ensure sufficient backup data is available to enable the restoration of the system to a recent, operable, and accurate state. Backup recovery testing will occur at least quarterly.

ROLES AND RESPONSIBILITIES

Security Official: Responsible for establishing, reviewing, and approving changes to the Contingency Plan Policy.

FORMS/PLANS/DOCUMENTS

Contingency Plan Annual Test

System-Specific Disaster Recovery Plan

Emergency Mode Operating Plan

RELATED POLICY

Data Security Policy - Security Management

Data Security Policy - Access Control

Data Security Policy - Device and Media Control

RELEVANT HIPAA REGULATIONS:

- §164.308(a)(7)(i) *Contingency plan*
- §164.308(a)(7)(ii)(A) *Data backup plan*
- §164.308(a)(7)(ii)(B) *Disaster recovery plan*
- §164.308(a)(7)(ii)(C) *Emergency mode operation plan*
- §164.308(a)(7)(ii)(D) *Testing and revision procedures*
- §164.308(a)(7)(ii)(E) *Applications and data criticality analysis*
- §164.310(a)(2)(i) *Contingency operations*

RELEVANT SOC 2 CRITERIA

- CC 7.3.1 *Responds to Security Incidents*
- CC 7.4.5 *Restores Operations*
- CC 7.5.1 *Restores the Affected Environment*
- CC 7.5.2 *Communicates Information About the Event*
- CC 7.5.3 *Determines Root Cause of the Event*
- CC 7.5.4 *Implements Changes to Prevent and Detect Recurrences*
- CC 7.5.5 Improves Response and Recovery Procedures
- CC 7.5.6 Implements Incident Recovery Plan Testing