HIPAA Security Policy #7

Administrative Safeguards
Contingency Plan

Statement of Policy

The Company is a *Business Associate* under the Health Insurance Portability and Accountability Act (HIPAA) Security Regulations. As such, The Company is required to safeguard electronic protected health information (ePHI) in accordance with the HIPAA Security Rule Regulations as well as The Health Information Technology for Economic and Clinical Health Act (the "HITECH Act"). These policies reflect The Company's commitment to complying with such Regulations. The Company will comply with the *Covered Entity's* documented HIPAA policies and procedures unless specifically stated in the below policy.

Purpose of Policy

The purpose of the policy is to plan for operational contingencies in the event of a disaster or emergency and to ensure that ePHI is protected during the disaster or emergency.

Policy

7 Contingency Plan

TYPE: Standard
REFERENCE: 45 CFR 164.308(a)(7)(i)
SECURITY REGULATION STANDARDS LANGUAGE:
"Establish 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."

1. The Company must develop or follow a covered entity's documented procedure to respond in the event an emergency, disaster or other occurrence (i.e., fire, vandalism, system failure and natural disaster) when any system that contains ePHI is affected, including:

    i. Data Backup Plan

    ii. Disaster Recovery Planning

    iii. Emergency mode operation plan

    iv. Testing and Revision Procedures

7.1 Data Backup Plan

IMPLEMENTATION TYPE: Required
REFERENCE: 45 CFR 164.308(a)(7)(ii)(A)
SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:
"Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information."

1. The Company shall establish and implement or follow a covered entity's Data Backup Plan pursuant to which it would create and maintain retrievable exact copies of all ePHI that is stored on all The Company computer systems.

2. The Data Backup Plan will apply to all systems that contain ePHI that The Company has operational control of and are not covered under the covered entity's Data Backup Plan.

3. The Data Backup Plan shall apply to all files, records, images, voice or video files that may contain ePHI.

4. The Data Backup Plan shall require that all media used for backing up ePHI be stored in a physically secure environment, such as a secure, off-site storage facility or, if backup media remains on site, in a physically secure location, different from the location of the computer systems it backed up.

5. If an off-site storage facility or backup service is used, a written contract or Business Associate Agreement shall be used to ensure that the Business Associate or Contractor will safeguard the ePHI in an appropriate manner.

6. Data backup procedures outlined in the Data Backup Plan shall be tested on a periodic basis to ensure that exact copies of ePHI can be retrieved and made available.

Procedure

1. The Company will develop and implement or follow a covered entity's procedure to ensure that daily backups and exact and retrievable copies are made of all systems that contain ePHI.

2. The Data Backup Plan will apply to all systems that contain ePHI that The Company has operational control of and are not covered under the covered entity's Data Backup Plan.

3. The Company will develop a list of systems that contain ePHI or that contain critical information and ensure that each of the systems are included in the daily backup.

4. The Company will ensure that periodic tests are performed to ensure the daily backups are valid, contain retrievable information and can be restored in the event of a disaster or emergency.

5. The Company will develop and implement a procedure to define restoration steps in the event data needs to be restored from backup.

6. The Company will ensure that any media used for the daily backup will be stored in a physically secure environment, such as a secure, off-site storage facility or, if backup media remains on site, in a physically secure location, different from the location of the computer systems it backed up.

7. Data encryption should be used to safeguard any ePHI on the daily backups.

7.2 Disaster Recovery Plan

IMPLEMENTATION TYPE: Required
REFERENCE: 45 CFR 164.308(a)(7)(ii)(B)

SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:
"Establish procedures to restore any loss of data."

1. To ensure that The Company can recover from the loss of data due to an emergency or disaster such as fire, vandalism, terrorism, system failure, or natural disaster effecting systems containing ePHI, The Company shall establish and implement or follow a covered entity's Disaster Recovery Plan pursuant to which it can restore or recover any loss of ePHI and the systems needed to make that ePHI available in a timely manner.

2. The Disaster Recovery Plan will apply to all systems that contain ePHI that The Company has operational control of and are e not covered under the covered entity's Disaster Recovery Plan.

3. The Disaster Recovery Plan should include training and security reminders to all workforce members.

Procedure

1. The Disaster Recovery Plan should include procedures to restore ePHI from data backups in the case of a disaster causing data loss.

2. The Disaster Recovery Plan should include procedures to log system outages, failures, and data loss to critical systems, and procedures to train the appropriate personnel to implement the disaster recovery plan.

3. The Disaster Recovery Plan shall be documented and easily available to the necessary personnel at all times.

7.3 Emergency Mode Operation Plan

IMPLEMENTATION TYPE: Required
REFERENCE: 45 CFR 164.308(a)(7)(ii)(C)
SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:
"Establish procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode."

1. The Company shall establish and implement (as needed) or follow a covered entity's procedures to enable continuation of critical business processes for protection of the security of ePHI while operating in emergency mode.

2. The Emergency Mode Operation Plan will apply to all systems / processes that The Company has operational control of and are not covered under the covered entity's Emergency Mode Operation Plan.

Procedure

1. The Company will define or follow a covered entity's definition of what constitutes and triggers an Emergency that would require an Emergency Mode Operation Plan.

2. The Emergency Mode Operation Plan will apply to all systems / processes that The Company has operational control of and are not covered under the covered entity's Emergency Mode Operation Plan.

3. The Emergency Mode Operation Plan shall include detailed steps on how workforce members will react to emergencies that impact the confidentiality, integrity, and availability of ePHI.

4. The Emergency Mode Operation Plan shall include steps that outline security processes and controls to ensure the confidentiality, integrity, and availability of ePHI.

5. The Emergency Mode Operation Plan shall be documented and easily available to the necessary personnel at all times.

6. The Emergency Mode Operation Plan should include training and security reminders to all workforce members.

7.4 Testing and Revision Procedures

IMPLEMENTATION TYPE: Addressable
REFERENCE: 45 CFR 164.308(a)(7)(ii)(D)
SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:
"Implement procedures for periodic testing and revision of contingency plans."

1. The Contingency procedures outlined in the Disaster Recovery and Emergency Operations Plans (Contingency Plan) shall be tested on a periodic basis.

2. Any necessary revisions or updates to the Contingency Plans shall be made.

Procedure

1. Testing of Contingency Plan should be performed at least annually.

2. Any necessary revisions that are identified during the Contingency Plan testing will be made to the Contingency Plans.

7.5 Application and Data Criticality Analysis

IMPLEMENTATION TYPE: Addressable
REFERENCE: 45 CFR 164.308(a)(7)(ii)(E)
SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:
"Assess the relative criticality of specific applications and data in support of other contingency plan components.

1. The Company shall assess or follow a covered entity's assessment of the relative criticality of specific applications and data for purposes of developing its Data Backup Plan, its Disaster Recovery Plan and its Emergency Mode Operation Plan.

2. The Application and Data Criticality Analysis will apply to all systems / processes that The Company has operational control of and are not covered under the covered entity's Application and Data Criticality Analysis.

3. The assessment of data and application criticality should be conducted periodically and at least annually to ensure that appropriate procedures are in place for data and applications at each level of risk.

Procedure

1. The Company will, at least annually, identify the relative criticality of each system that may or may not contain ePHI in relation to patient care.

2. The list of critical systems will be used to prioritize which systems to concentrate on when implementing the Contingency Plan.

Creation Date:
Effective Date:
Last Revision Date: