Policy 6
Contingency Plan Policy and Procedure

1. Applications and Data Criticality Analysis

The Security Officer will be responsible for determining which electronic protected health information is considered "critical".

Criticality will be determined on both a long term and a short -term basis. Information is critical on a short- term basis if daily operations could not be continued without this information. Information is critical on a long-term basis if the practice would have liability exposure if the information was permanently lost or lost for a long -term period.

2. Data Backup and Disaster Recovery Plan

Data will be backed up based upon the schedule determined by the Security Officer, taking into account the criticality of the data stored on each information system.

The Security Officer will be responsible for investigating the various methods available to back up each system. To the extent that the Security Officer determines that back up requires the purchase of software, hardware, or the use of a third party vendor, the Security Officer will discuss options, including costs and benefits, with appropriate administrative personnel with decision-making authority.

In the event of a disaster that may impact the practice's systems containing electronic protected health information, the Security Officer will be responsible for overseeing the recovery of data. The process should be started immediately to decrease the likelihood of permanent losses. The Security Officer should compile a list of key individuals to contact in the event of a disaster situation (and prioritize).

3. Emergency Mode Operation plan

The data that is deemed to be most critical to daily operations will be restored first (to the extent that it does not impair the potential for recovery of information that is critical from a long term perspective).

Alternative procedures will be followed during the time period while systems are down.

4. Testing and Revision Procedures

The organization will test the contingency plan on a schedule determined by the Security Officer. Testing methods will be determined in a manner that will provide the least disruption to daily operations while still allowing the Security Officer and others to discover potential flaws in the plan.

Explanation of the Contingency Plan Standard and Instructions for Utilizing the Contingency Plan Policy

The Contingency Plan Standard requires covered entities to implement policies and procedures setting forth the way in which the covered entity will respond to emergencies or occurrences that could damage systems containing electronic protected health information. Examples of situations that a physician practice should plan for include fire, vandalism, system failure, and natural disasters.

The practice should make a list of any natural disasters that are reasonably likely to occur within its geographical area (e.g., tornado, flood, blizzard). Although each natural disaster does not require a separate policy, the practice should look at potential natural disasters and determine the types of damage that could result. For example, both a flood and a tornado could cause power outages and water damage or structural damage to electronic equipment.

The contingency plan standard has five implementation specifications. Policy 6 is a sample policy addressing all of these implementation specifications.

a. Data backup plan and disaster recovery plan

The first two required implementation specifications are the "Data backup plan" and the "Disaster recovery plan." These specifications require covered entities to develop policies and procedures for the creation and maintenance of a duplicate copy of all electronic protected health information that can be retrieved by the covered entity when necessary to restore any lost data.

Examples of ways in which data back up can be accomplished include:

- The use of a remote backup vendor (note that such vendors should be asked to sign a business associate agreement or provide assurances that they cannot access the information and are only acting as a conduit).
- The use of a system that copies all data on a daily basis and stores the information on electronic media that is physically removed from the practice on a daily basis.

b. Emergency mode operation plan

The third required implementation specification is "Emergency mode operation plan", which is the development of procedures designed to allow the practice to continue doing business and to continue to protect the security of electronic protected health information during and immediately after a crisis situation, such as after a natural disaster or during a power outage.

In an emergency situation, it will be likely that all systems will be down. As part of this plan, the practice should prioritize which systems should be recovered first, based upon the criticality of the information stored on each system.

The practice will also need to have alternative procedures in place when electronic systems are unavailable.

c. Testing and revision procedures

This specification involves the development and implementation of policies and procedures for testing backup and disaster recovery plans and revising these plans as necessary. For example, the backup system should be tested to see if it can be recovered if necessary.

d. Applications and data criticality analysis

The final addressable implementation specification is "Applications and data criticality analysis". This specification involves the assessment of a covered entity's data and applications to determine which would be considered "critical" when developing data backup and disaster recovery plans. As discussed in the emergency operation plan specification discussed above, the covered entity should look at what information is needed to continue day-to-day operations. In addition, the practice should look at the information that would be "critical" if lost or corrupted.

For example, an electronic patient medical record would most likely be considered "critical" data. On the other hand, information that is old and is being kept beyond the statutes of limitations for liability and beyond the time period specified by Medicare and other third party payor contracts might not be considered "critical".