

Special points of interest:

- HIPAA SECURITY
- HIPAA PORTABILITY-MEDICAID

Monthly Newsletter

HIPAA Security

In previous Newsletters we've addressed the implementation of the HIPAA Security requirements for small group health plans by April 20, 2006. The HIPAA Security requirements only apply to protected health information (PHI) in electronic form. Electronic media includes storage media such as hard drives, magnetic tapes or disks, and digital memory cards, and it also includes transmission media such as the Internet, extranets, leased lines, dial-up lines, private networks and the physical movement of electronic storage media. The security regulations require Plan Sponsors to implement safeguards to protect PHI in electronic form from unauthorized access, alteration, deletion or transmission.

The following are the 8th and 9th in a series of 9 articles prepared by The Clayton Group, a HIPAA consulting company, to assist in HIPAA Security compliance. These articles are designed to provide a process overview and are not meant to provide legal advice. You should seek your own legal counsel or consulting service for HIPAA Security compliance.

The below list of articles will address electronic data technologies, operational reengineering (policy and procedure development), strategic planning.

- Article #1—Getting Started
- Article #2 - *Completing Your Risk Analysis*
- Article #3 - *The Remediation Process (technical vs. policy)*
- Article #4 - *The Controversial Issues: Email and Encryption*
- Article #5 - *Sanctions*
- Article #6 - *Handling Security Incidents*
- Article #7 - *Training*

- Article #8 - *Ongoing Compliance & Evaluation*
- Article #9 - *Disaster Planning*

Source: The Clayton Group
www.theclaytongroup.org

Ongoing Compliance and Evaluation (No. 8 in series of 9 articles)

Now that the April 20th compliance date is here, the real work begins. Don't let all of your *hard work* go by the wayside because you don't *enforce compliance!* Make sure to perform ongoing evaluations of your compliance. CMS has published the following language in Frequently Asked Questions (FAQ)'s on this issue:

"Compliance is not a one-time goal, it must be maintained. Compliance with the evaluation standard at § 164.308(a)(8) will allow covered entities to maintain compliance. By performing a periodic technical and non-technical evaluation a covered entity will be able to address initial standards implementation and future environmental or operational changes affecting the security of electronic PHI."

Sample Language

Consider the following sample language (provided by The Clayton Group) for your Evaluation Policy Document:

1. [ENTITY] will perform a routine and periodic (every six months, once a year, once every two years) technical and non-technical (operational) review of all of [ENTITY]'s policies and procedures resulting from the initial risk analysis and general risk management program. This initial evaluation will take into consideration initial [ENTITY] enterprise status and its resulting early interpretation of the Administrative Simplification Security components. This will be [ENTITY]'S benchmark evaluation.

2. The same review will subsequently be undertaken periodically and whenever environmental or operational changes affecting the protected health information secured by [ENTITY] occur. The benchmark evaluation will be used as the beginning of the second review.

Now add your own procedures and remember...this is not a one-time goal. Make sure to implement a strong maintenance/auditing process to maintain your organizations HIPAA Security compliance today!

Disaster Planning (No. 9 in series of 9 articles)

Disaster Planning

The HIPAA Security compliance date for small group health plans was Thursday - April 20, 2006!

This is the last of a series of articles from The Clayton Group offering helpful tips to facilitate your HIPAA Security compliance efforts. The Security regulation includes 40+ implementation specifications; however only nine major topics have been covered via these articles. As a HIPAA covered entity, you are responsible to document your compliance efforts. One critical area of the regulation spills over into all of your proprietary business practices-disaster planning.

To assist with your HIPAA Security Contingency Planning The Clayton Group has provided the following draft language for your consideration in developing your policies.

Sample Language Describing the Policy "Purpose"

In accordance with the [ENTITY] goal of protecting the availability, integrity and confidentiality of electronic protected health information, the organization has developed policies and procedures for responding to an emergency or other unexpected negative event or occurrence that may damage computer systems containing electronic protected health information.

The next excerpt provides a sample of the initial "policy". Be sure your policy includes at a minimum the components listed in number 2 below:

1. In general the Contingency Plan provides a mechanism for [ENTITY] to accomplish the protection of the following assets in response to negative and unexpected occurrences while minimizing the total impact on business operations in response to the crisis:
 - a. Protect lives and personal safety
 - b. Protect sensitive data and allow for information safety and recovery
 - c. Protect equipment, limit damage and allow for recovery

- d. Protect the Facility, limit damage and allow for recovery
- e. Specifically, the Contingency Plan provides a mechanism to:

- **Avoid interruptions to critical functions** even while undergoing a loss of electricity, fire, vandalism, true disaster or other occurrence where systems and data are threatened.
- **Minimize impact on total business operations**, minimize interruptions to critical functions so that they occur only infrequently, are brief in duration and do not result in detrimental consequences.
- **Address complications and consequences of normal lost processing time**, operations degradation, lost equipment replacement processes, insurance funds, alternative processing sites, temporary office space, equipment, key personnel, telephones and other business basic equipment.

2. The Security and Privacy Officials, working with other key management personnel, are responsible to create, obtain management approval, implement and maintain a comprehensive Contingency Plan including the following components:

- a. **Data Back up Plan**- Provides for the creation and maintenance of an exact retrievable copy of all [ENTITY] electronic protected health information. It may also include maintenance and retrieval of paper files of protected health information.
- b. **Disaster Recovery Plan**- Defines procedures to restore any loss of data and equipment due to an emergency, power loss, fire, vandalism, natural disaster or other occurrences.
- c. **Emergency Mode Operation Plan**- Allows for continuation of critical business processes for protection and security of PHI even during emergency mode operations.
- d. **Testing and Revision** - Allows for routine testing of contingency plans as necessary in accordance with [ENTITY] system complexity, and other factors reviewed during the Risk Analysis and Risk Management Process.
- e. **Applications and Data Criticality** - Based upon system complexity and importance as a result of Risk Analysis and Risk Management, this process allows for the prioritization of system applications and related data in order to support resumption of normal business/systems processing.

The development of data back-up plans, disaster recovery plans, emergency mode operation plans, testing, revision, applications, and data criticality are core to the success of your organizations overall contingency plan. Each of these sub plans is truly unique to the organization and varies depending upon level of protected health information use, size, complexity of systems, location, physical, and technical considerations.

HIPAA PORTABILITY – LOSS OF MEDICAID COVERAGE

Recently we've received many inquiries regarding the **loss of Medicaid coverage** as a Special Enrollment right.

The following is an excerpt from a SPBA Update:

Loss of Medicaid – The final rule did not change the interim rule that omits the loss of Medicaid as a trigger for a special enrollment period. **Loss of Medicaid does not create a special enrollment period.** However, plans can always be more generous than the minimum required under HIPAA, provided the stop-loss carrier agrees. HHS (Health and Human Services) officials have noted that a change in the HIPAA statute is needed on this issue.

BAS will advise you of any change to the Special Enrollment rules.