

BENEFITS UPDATE

HIPAA Electronic Security Standards

Fall 2004

Just as Health Plan Sponsors thought they had mastered the HIPAA “Administrative Simplification” rules that first appeared in the form of the HIPAA privacy regulations, the Department of Health and Human Services has unleashed a new set of HIPAA rules — the electronic security standards.

When paired with the HIPAA privacy rules, the new electronic security standards will provide uniform standards for protecting Protected Health Information that is transmitted or maintained in electronic format.

Although the deadline for compliance with the new electronic security standards is not until April 21, 2005 for large health plans and April 21, 2006 for small health plans, it’s not too early to begin the compliance process.

Who must comply?

Covered Entities (health plans, healthcare clearing houses, and certain health care providers) must comply with the new standards. These are the same entities that were covered by the HIPAA privacy rules.

What health information is covered?

The new security standards will cover **Protected Health Information (“PHI”)** (as that term was defined in the privacy rules) that is maintained or transmitted using electronic media.

What is required?

A covered entity must implement the new security standards as required under the regulations. The regulations establish three broad categories of safeguard - Administrative, Physical, and Technical. Each category is further subdivided into “implementation specifications.” Each implementation specification is either “required” or “addressable.”

Administrative Safeguards include security policies and procedures to protect the PHI that is stored or transmitted electronically and to restrict employees’ access to the electronic PHI.

Physical Safeguards include procedures to protect the information systems, equipment, and buildings from natural or environmental hazard or unauthorized intrusion.

Technical Safeguards include the development of policies and technology to restrict access to the electronic PHI to those persons who have been granted access in accordance with the established Administrative safeguards.

Each of these broad categories is further divided into “implementation specifications” or specific measures that the covered entity is to take in order to implement the safeguard. If an implementation specification is “required,” the covered entity must implement that specification. If the implementation specification is “addressable,” the covered entity must either (1) implement the specification or (2) document why the implementation would be unreasonable or inappropriate and, if reasonable and appropriate, implement alternative measures.



2000 Equitable Building ♦ 10 S. Broadway ♦ St. Louis, Missouri ♦ 63102
12 Wolf Creek Drive ♦ Belleville (Swansea), Illinois ♦ 62226

Employee Benefits Practice Group

314-241-9090

© 2004 Greensfelder, Hemker & Gale, P.C.
All Rights Reserved

What steps should the covered entity take?

Although the compliance deadline is still several months away, you may wish to begin the lengthy compliance procedures well in advance of the deadline. The following are some of the preliminary steps which plan sponsors can take.

Alert the IS Department. Compliance with the new rules will require the active involvement of the covered entity's IS department as well as that of the department having control of the PHI. Plan Sponsors or Administrators should alert their IS departments to the upcoming compliance activities.

Appoint a Security Official. This individual will be responsible for the development and implementation of the policies and procedures required for compliance with the security standards.

Review and if necessary amend your Business Associate Contracts. With some exceptions, the Business Associates of the covered entity must agree to follow security standards for electronic storage or transmittal of PHI.

Review and if necessary amend the Health Plan document. The plan document must incorporate provisions requiring the plan sponsor to implement the security standards and ensure that the security procedures are followed.

Begin to conduct a thorough risk analysis. Each covered entity must conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic PHI held by the covered entity.

Develop written policies and procedures, train staff and impose sanctions for violations. As with the privacy rules, a covered entity has certain responsibilities which it must satisfy in compliance with these electronic safeguards. You must determine who has access to electronic PHI and train them with respect to security. In the event of breach, there must be appropriate sanctions.

Become familiar with the requirements imposed by the new regulations. We will be happy to assist you with understanding the new security rules. As the deadline for compliance approaches, we can also assist you with implementation of the specific standards and training your staff.

These new rules apply to PHI that is maintained or transmitted in electronic format. Paper records are not covered by these rules, and covered entities should be aware that in the future the Department of Health and Human Services may also issue rules about security of paper records.

We will be happy to assist you to comply with the new rules. Please call Theresa Brennan, Dan Schwartz, Toni Landreth or Doug Neville with any questions.

For further information please contact :

**Theresa A. Brennan, Toni S. Landreth
Douglas S. Neville, and Daniel J. Schwartz**