



HIPAA Security

Background on HIPAA

In April 2004, certain organizations (called "covered entities") were first required to comply with the **HIPAA Privacy** rules through a number of administrative safeguards designed to protect individuals' protected health information (PHI). Some of the required steps involved implementing business associate agreements with vendors, appointing privacy officers and completing authorization forms prior to accessing the PHI of an individual. Now, organizations (including many employers) are being asked to begin complying with the HIPAA Security standards. Much like HIPAA Privacy, the Security standards are designed to ensure that your employees' PHI is kept private and confidential. The specific focus of **HIPAA Security** is on PHI that is transmitted electronically, or *ePHI*. **The bottom line is that health plans now need to make sure that any ePHI they are storing on their systems or sending outside of their organization is protected from unauthorized access.**

Who must comply with HIPAA Security?

Since various entities including healthcare providers, insurance companies and health plan sponsors (who are typically employers) have access to an employee's ePHI, all are considered "covered entities" under HIPAA Security and must comply with its safeguards to protect that confidential data. Additionally, any business associates of a covered entity who may handle ePHI, such as RSI, must also be in compliance with HIPAA Security. Employer-sponsored health plans are covered by the scope of HIPAA Security unless they do not receive, transmit or house any electronic PHI. An employer that does not receive, store or transmit any ePHI would have no data to safeguard and would not be covered by the scope of HIPAA Security.

What is HIPAA Security?

The HIPAA security standards are designed to protect **electronic** protected health information or ePHI. In practical terms, this means that employers who offer employee health plans must safeguard the protected health information of their employees while it is being electronically stored or transmitted to another party. HIPAA Security's main objective is to prevent unlawful access to members' ePHI. In a nutshell, the HIPAA Security guidelines require covered entities to:

- **Assess** potential risks to ePHI
- **Develop** and **maintain** security measures to protect ePHI
- **Document** the security measures it has taken

When is the deadline?

The compliance date for "small health plans" is **April 20, 2006**. HIPAA defines small health plans as having less than \$5 million in annual premiums or claims during the prior fiscal year- this would roughly translate into about 1000 or fewer employees. The compliance date for *large* health plans was April 20, 2005. Since a group would have needed over \$5 million in premiums or claims during the fiscal

year prior to April 2005 to be a "large health plan", RSI is considering all of their clients to be small health plans.

What must I do to comply with the HIPAA requirements?

While we want you to be aware of your possible obligations under HIPAA Security, we don't want to overwhelm our clients with volumes of HIPAA Security detail. We would like to help you focus on the most basic and easily remedied aspects of HIPAA Security that can be addressed as a first step. While there are technically 18 security standards under HIPAA, they fall into three basic categories:

- **Administrative Safeguards** - involves evaluating the policies and procedures that spell out an organization's security measures, which can include the training of the workforce, the procedures for granting employees access to ePHI and policies for reporting security incidents.
- **Physical safeguards** - involves the measures in place to protect the building and equipment from environmental hazards and unauthorized access. These safeguards focus on the physical barriers such as door locks and access control policies.
- **Technical Safeguards** - involves the technology in place and the policies governing the use of that technology. These safeguards are focused on the computer-oriented safety controls such as the use of user names and passwords by employees, firewall protection and data encryption capabilities.

What is my first step?

If your organization determines that it does receive, store or transmit ePHI, the first step you can take is to evaluate how well that data is protected and establish areas of improvement that may be required. For example, at RSI, we are encouraging clients who are transmitting ePHI to do so using email attachments that are password-protected, rather than to include ePHI in the body of the email itself. While there are additional levels of protection that need to be addressed, beginning to develop some measures for protecting the data you transmit will bring you one step closer to avoiding any breaches in HIPAA Security.

Where do I go from here?

RSI can work with you to complete a HIPAA Audit, which will guide you through the development of a risk analysis and the creation of a HIPAA Security Policy for your organization. The audit process will assess your company's preparedness for HIPAA Security and will highlight any areas of concern that should be addressed. For more information on the HIPAA Audit service, please contact Diane Allen, RSI Human Resources Consultant at 800-394-6111, ext. 4395.

March 16, 2006

[BACK](#)