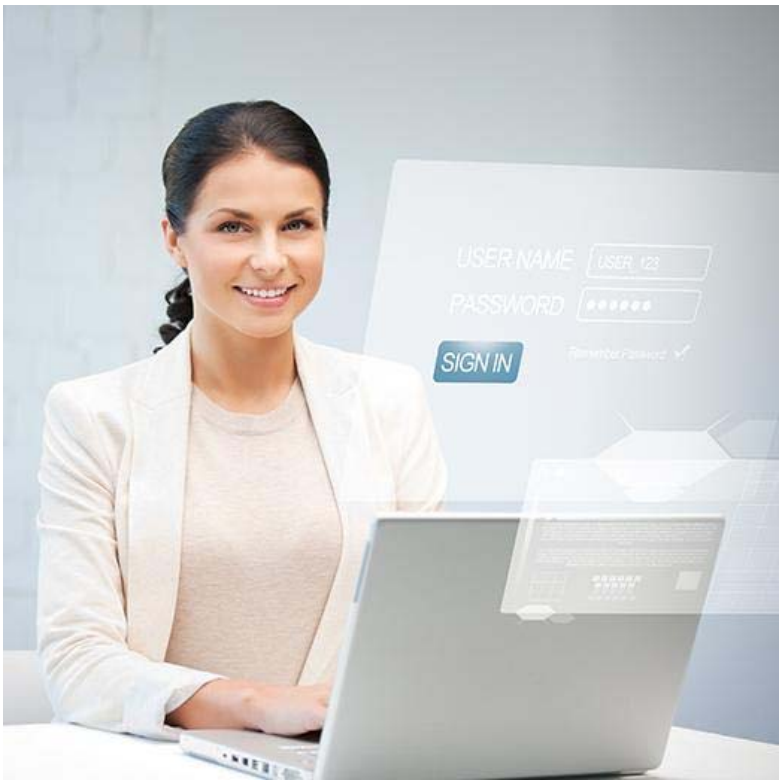
LEGAL MANAGEMENT
THE MAGAZINE OF THE ASSOCIATION OF LEGAL ADMINISTRATORS

Did the HIPAA Deadline Pass You By?

By Brian Ruthruff

Did you know that the Department of Health and Human Services (HHS) released its final Health Insurance Portability and Accountability Act (HIPAA) rule earlier this year? The rule significantly expands certain HIPAA obligations for healthcare-related businesses and, importantly for law firms, their business associates. HIPAA is the federal statute that governs the confidentiality and protection of a patient's protected health information, and law firms must care more about it now than ever.



Law firms are now required to comply and held accountable to HIPAA standards if the firm is working for healthcare organizations and hold PHI – protected health information. The fines can be as high as .5 million. The HIPAA act comprises several rules that must be followed. This article highlights the Security Rule and steps law firms can take to be in compliance with the rule.

The Security Rule specifies a minimum necessary standard – when you are using or disclosing PHI, requesting it or providing it, you need to make reasonable effort to limit access to the bare minimum necessary to accomplish the intended use.

Just as the healthcare organization needs to have a business associate agreement with the law firm, the firm needs to have business associate agreements with any of their business associates that handle PHI for the firm. For law firms, this could include document scanning or review services, eDiscovery and cloud storage vendors. Information technology vendors may not need business associate agreements as they could possibly be considered as an employee of the firm, with incidental contact with PHI. The rule requires physical safeguards and technical safeguards. Physical safeguards are required for workstations and electronic media, require policies and procedures regarding the transfer, removal, disposal, encryption and re-use of electronic media. Laptops and portable drives must be encrypted.

Technical safeguards include access controls, audit controls and integrity controls, as well as transmission security. Access controls would be similar to the ethical walls with which law firms are already familiar. The firm is required to limit PHI access to those individuals that require access. This would include categorizing data upon receipt at the firm as PHI.

In addition, this rule prohibits the use of shared accounts and passwords, sometimes common in firms today. Each user, including temporary or contract employees, must have their own account to access the firm's computer systems.

Audit controls are likely already in place at most firms today, as most common document management systems already include significant amounts of logging. If not then the logging and tracking of access to PHI must be implemented.

Integrity controls involve policies and procedures to ensure that electronic PHI is not improperly altered or destroyed. These controls are also likely built into many modern document management systems; the firm should review these systems for compliance. Transmission security covers data in motion between parties. In most cases, this will be accomplished via encryption of the data in transit. TLS encryption (Transport Layer Security) is commonly used with e-mail. TLS is incorporated into all major e-mail systems, but will likely need to be configured as required between parties exchanging PHI rather than the usual default of best effort use of TLS encryption.

If your firm is considered a business associate of an entity covered by HIPAA, it is critical to review the policies, procedures and information systems in use at your firm to ensure compliance with the HIPAA rules, starting with a gap analysis comparing current systems and practices to requirements that most IT consultants can perform. Failing to achieve compliance with HIPPA could result in government fines, embarrassment or loss of business for your firm.

ABOUT THE AUTHOR

Brian Ruthruff has been in the information technology field for more than 25 years. He has worked with law firms and technology extensively in his more than 10 years with Innovative Computing Systems (ICS). View Ruthruff's LinkedIn profile.

BRIAN RUTHRUFF
Regional Operations Manager at Innovative Computing Systems