Kim Stanger

Partner
208.383.3913
Boise
kcstanger@hollandhart.com

HIPAA Compliance: Security Rule Enforcement on the Rise

HIPAA Compliance: Security Rule Enforcement on the Rise

Insight — 7/11/2012

Most healthcare providers are acutely aware of and generally comply with the HIPAA Privacy Rule; however, they and their business associates may be less familiar with and likely fail to satisfy HIPAA Security Rule requirements. The Privacy Rule generally prohibits covered entities from using or disclosing a patient's protected health information ("PHI") without authorization. (45 C.F.R. § 164.500 et seq.). In contrast, the Security Rule applies to electronic health information ("e-PHI"). It requires covered entities and their business associates to implement specific administrative, technical, and physical safeguards to protect the integrity, availability, and confidentiality of e-PHI, e.g., by ensuring that computers and other electronic devices satisfy regulatory standards pertaining to passwords, firewalls, backups, transmission security, etc. (45 C.F.R. § 164.300 *et seq*.).

In the past, the Office of Civil Rights ("OCR") seemed not to actively enforce the Security Rule, but that is changing:

- In March, Blue Cross Blue Shield of Tennessee ("BCBS") agreed to pay $1.5 million for security rule violations arising out of the theft of unencrypted laptops. Among other things, BCBS failed to conduct the required security assessment and implement access controls required by the Security Rule.
- In April, a Phoenix cardiology group agreed to pay $100,000 for, among other things, failing to designate a security officer, conduct the required security assessment, implement safeguards required by the Security Rule, or execute business associate agreements with vendors who stored or accessed e-PHI.
- In June, the Alaska Department of Health and Social Services ("DHSS") agreed to pay $1.7 million after a USB hard drive was stolen. The OCR's investigation showed that DHSS did not have adequate policies and procedures in place to safeguard ePHI, and had not completed the required risk analysis, implemented sufficient risk management measures, completed security training for its workforce members, implemented device and media controls, or addressed device and media encryption as required by the Security Rule.

These actions sound a wake up call to all providers and business associates—large, small, or public—who have ignored or become lax with Security Rule compliance. As OCR Director Rodriguez stated, "We hope that health care providers pay careful attention to [these] resolution agreement[s] and understand that the HIPAA Privacy and Security Rules

have been in place for many years, and OCR expects full compliance no matter the size of a covered entity." The OCR is now required to impose mandatory penalties of $10,000 to $50,000 per violation if a provider is determined to have acted with willful neglect. Based on the recent cases, failing to implement safeguards required by the Security Rule may evidence willful neglect.

If they have not done so recently, providers and their business associates should review their Security Rule compliance. Among other things, they should conduct a security assessment to determine their system vulnerabilities, and implement the safeguards specified in the Security Rule regulations. To obtain a checklist for Security Rule compliance, please click here. In addition, the OCR has published several tools to help entities comply:

- The OCR's recently published HIPAA Audit Protocol is a good roadmap for compliance; it is available at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/protocol.html.
- The OCR's Final Guidance on Risk Analysis is available at: http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalintro.html.
- The OCR's series of technical guides for implementing the security rule is available at: http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityruleguidance.html.

Putting in place the required policies and practices and documenting appropriate training will go a long way to avoiding Security Rule penalties. More importantly, they will help providers avoid potentially devastating consequences of a security failure, system crash, or the loss of electronic data which the Security Rule is designed to protect. In that regard, Security Rule compliance is not just a regulatory mandate; it is a prudent business practice.

For questions regarding this update, please contact
Kim C. Stanger
Holland & Hart, U.S. Bank Plaza, 101 S. Capitol Boulevard, Suite 1400, Boise, ID 83702-7714
email: kcstanger@hollandhart.com, phone: 208-383-3913