HIPAA Compliance Reporter for Business Associates of Covered Entities

Liability Reduction by Automated Risk Management

On February 17, 2009 President Obama signed the American Recovery and Reinvestment Act of 2009 (ARRA). This bill authorizes over $700 billion in new spending, increases penalties for release of protected health information, requires public notification of data breaches, greatly expands the legal right to sue under HIPAA and makes business associates of covered entities directly responsible for full compliance with the HIPAA security rule.

Quoting from section 13401 of the ARRA, "(a) Application of Security Provisions…shall apply to a business associate of a covered entity in the same manner that such sections apply to the covered entity…and shall be incorporated into the business associate agreement between the business associate and the covered entity."

The ARRA provides business associates of covered entities with both a threat and an opportunity. The expanded right to sue and the increased penalties for information release expand the risks to anyone handling health information. At the same time, business associates will be eligible for grants up to $40,000 to install automated data systems.

Automating Information Security – NIST 800-66 and the DHS SCAP Program

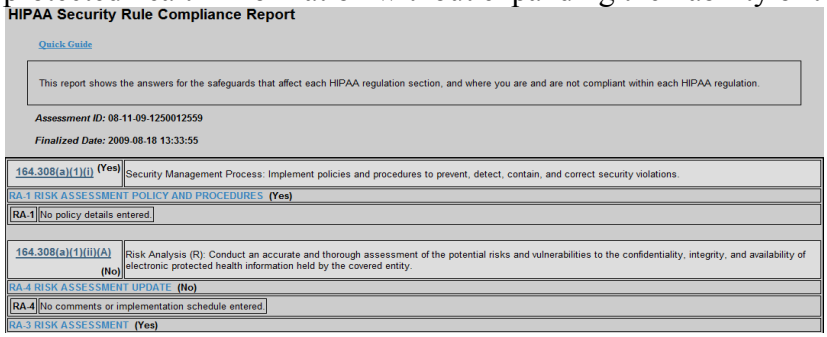
Within the last year powerful new tools have been developed for information security under the DHS Security Content Automation Protocol (SCAP) program. SCAP validated network scanners are available from a dozen vendors, with more programs in the process of validation. Most of these are sized to deal with larger networks from 150 to 15000 workstations. However the Secutor program from ThreatGuard has a version small enough to fit on a thumb drive and be used a scan a single workstation at a time. For most business associates this simple and inexpensive scanner is ideal. Directions for HIPAA security rule compliance are contained in the the National Institute of Standards and Technology (NIST) "Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule (SP 800-66 REV 1)." Other guidance can be found on the CMS webpage, but the 800-66 protocol is readily implemented and allows significant automation of the risk management process.

A special benefit of 800-66 compliance is that it removes the requirement for public notification of data breaches. Page 10 of the HHS guidance document on ARRA states that compliance with 800-66 safeguards will "create the functional equivalent of a safe harbor, and thus, result in covered entities and business associates not being required to provide the notification otherwise required…" Following the signing of the ARRA, ThreatGuard and ACR teamed up to produce the HIPAA Compliance Reporter. This inexpensive program combines the Secutor thumb drive scanner with an online version of the NIST 800-66 protocol. A full program can be setup in a few hours, although reaching acceptable levels of compliance can be expected to take months or years, based on ACR experience in securing banks to similar levels of information security.

Implementation

Bringing a business associate of a covered entity into compliance with the HIPAA security rule is a three step process.

1. Update the business associate contract. As noted in the ARRA, security rule compliance "shall be incorporated into the business associate agreement between the business associate and the covered entity." NIST 800-66, p48 notes that it is appropriate for covered entities to request network risk assessments from their business associates. Business associates should work with their covered entities to streamline the contracting process.
2. Acquire a copy of the HIPAA Compliance Reporter from ACR.
3. Scan business associate workstations and create the Information Security Risk Assessment and the HIPAA Compliance Report. Risk Assessment summaries use an easily understood red/yellow/green report format. The HIPAA Compliance Report is a clause by clause review of the Security Rule with the current status of the business associate network. Convey a copy of the Risk Assessment and Compliance Report to the covered entities with which the business associate has contracts. These reports will prove the fitness of the business associate to handle protected health information without expanding the liability of the covered entity.


HIPAA Security Rule Compliance Report

Quick Guide

This report shows the answers for the safeguards that affect each HIPAA regulation section, and where you are and are not compliant within each HIPAA regulation.

Assessment ID: 08-11-09-1250012559

Finalized Date: 2009-08-18 13:33:55

164.308(a)(1)(i) (Yes) Security Management Process: Implement policies and procedures to prevent, detect, contain, and correct security violations.

RA-1 RISK ASSESSMENT POLICY AND PROCEDURES (Yes)

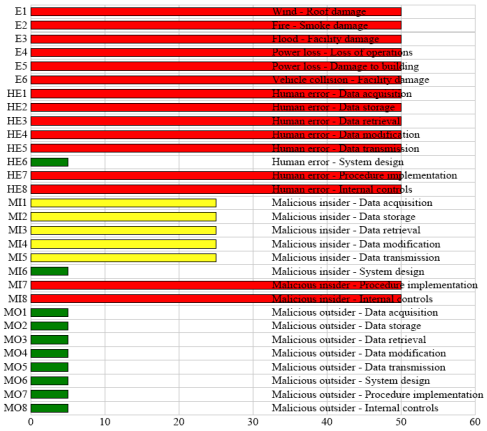
RA-1 No policy details entered.

164.308(a)(1)(ii)(A) (No) Risk Analysis (R): Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.

RA-4 RISK ASSESSMENT UPDATE (No)

RA-4 No comments or implementation schedule entered.

RA-3 RISK ASSESSMENT (Yes)



Cost Effective HIPAA Security Rule Compliance

The combination of SCAP scanning, developed under the sponsorship of the US Department of Homeland Security, and automation of the NIST 800-66 compliance process allows covered entities and their business associates to secure private health information to the levels envisioned by the creators of HIPAA.

For more information, please contact Info@acr2solutions.com or call (678)261-8181.