ARRA Subsidies and Mandatory HIPAA Compliance for Business Associates of Covered Entities
November 23, 2009

ARRA Subsidies

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.

More than $19 billion of the ARRA is reserved for hospitals and medical practices that make "meaningful use" of "certified" Electronic Medical Record (EMR) systems. Hospitals that meet the meaningful use standard are eligible for subsidies of more than $2.5 million each, beginning in October of 2010. However, hospitals that do not meet "meaningful use" do not qualify for the subsidy, and may be subject to penalties.

Qualifying for Subsidies

The standards for "meaningful use", issued by HHS on June 15, 2009, include a number of transaction standards, including

Computerized Physician Order Entry (CPOE)
Patient access to electronic clinical information
Electronic storage of clinical information
Electronic data exchange between multiple care providers
Immunization history and recommendations
Generate and transmit permissible prescriptions electronically (eRx)"

At the same time, hospitals must achieve "Full compliance with HIPAA Privacy and Security Rules" (page 7). This is internally consistent, since electronic prescribing and EMR systems that are not secure put patient privacy at significant risk. HHS reports that in 2008, over 5,000,000 patient records were stolen (Federal Register, Vol. 74, No. 162, Monday, August 24, 2009, page 42762).

HIPAA Security Rule compliance is emphasized in the meaningful use guidelines. Page 7 notes that "An entity under investigation for a HIPAA privacy or security violation cannot achieve meaningful use until the entity is cleared by the investigating authority".

Business Associate Requirements

In order for hospitals to meet meaningful use requirements, and qualify for million dollar subsidies, they and all of their business associates must comply with the HIPAA Security Rule. For purposes of the HIPAA Security Rule, a "business associate" is any organization that received electronically Protected Health Information (ePHI). 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."

Directions for HIPAA Security Rule Compliance

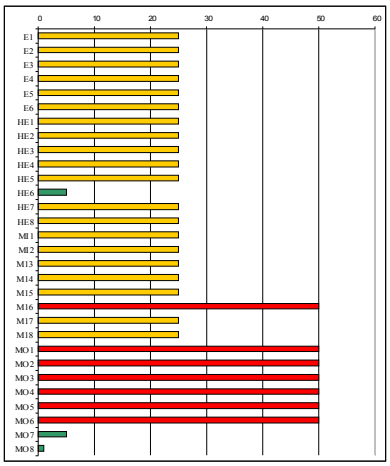
Directions for HIPAA security rule compliance are contained in the National Institute of Standards and Technology (NIST) "Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule (SP 800-66 REV 1) On page 48 of NIST 800-66 it is stated that "it is appropriate for covered entities to request network risk assessments from their business associates."

Procedure for HIPAA Security Rule Compliance

HIPAA Security Rule compliance for covered entities and business associates as defined by NIST 800-66 involves several basic steps:

1. Scan the computer network using an SCAP validated vulnerability scanner.
2. Conduct a risk assessment using the NIST 800-30 protocol.
3. Implement safeguards to protect against the risks identified during the risk assessment and vulnerability scan. This will generally include use of access control and intrusion detection/prevention (IPS) for data in motion and encryption for data at rest.

The NIST risk assessment procedure provides a quantitative scoring of network risks. Software is available to automate this process and provide NIST compliant risk assessment reports to hospitals and other covered entities who wish to qualify for ARRA subsidies. Excerpts from a typical risk assessment report are shown below.



HIPAA Security Rule Compliance Report

164.308(a)(1)(i)	Security Management Process: Implement policies and procedures to prevent, detect, contain, and correct security violations.
RA-1 RISK ASSESSMENT POLICY AND PROCEDURES **(Yes)**	
The written copy of the Risk Assessment report is in the locked file drawer of the Compliance Officers desk.	
164.308(a)(1)(ii)(A)	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-2 SECURITY CATEGORIZATION **(Yes)**	
All ePHI is controlled as \"High\" value information.	
RA-3 RISK ASSESSMENT **(Yes)**	
This Risk Assessment follows the requirements of NIST 800-30 and NIST 800-66.	
RA-4 RISK ASSESSMENT UPDATE **(Yes)**	
The network scan and UTM upload are updated weekly. The policy items are updated as necessary, but at least once/year.	

Summary

Hospitals that qualify for "meaningful use" of "certified" EMR systems can receive subsidies in excess of $2.5 million, starting in October of 2010. However, hospitals who do not comply with the HIPAA Security Rule are not eligible for the subsidy. This includes hospitals with business associates that are not compliant with the HIPAA Security Rule.

HIPAA Security Rule compliance is likely to be a **significant competitive advantage** for organizations that supply goods and services to hospitals and clinics. Hospitals with non-compliant business associates may work with the associates to achieve compliance, decide to decline multi-million dollar ARRA subsidies, or seek out suppliers that are HIPAA Security Rule compliant.