HIPAA Compliance Reporter for Covered Entities – Liability Reduction by Automated, Cost Effective Support of Business Associates

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, greatly expands the legal right to sue under HIPAA, requires public notification of data breaches 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- Sections 164.308, 164.310, 164.312, and 164.316 of title 45, Code of Federal Regulations, shall apply to a business associate of a covered entity in the same manner that such sections apply to the covered entity. The additional requirements of this title that relate to security and that are made applicable with respect to covered entities shall also be applicable to such a business associate and shall be incorporated into the business associate agreement between the business associate and the covered entity."

The ARRA provides hospitals and other covered entities with both a threat and an opportunity. The expanded right to sue, public notification requirements and the increased penalties for breaches expand the risks to covered entities. At the same time, subsidies for automating medical records can reduce costs while increasing reimbursements.

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 small offices and business associates this simple and inexpensive program is ideal.

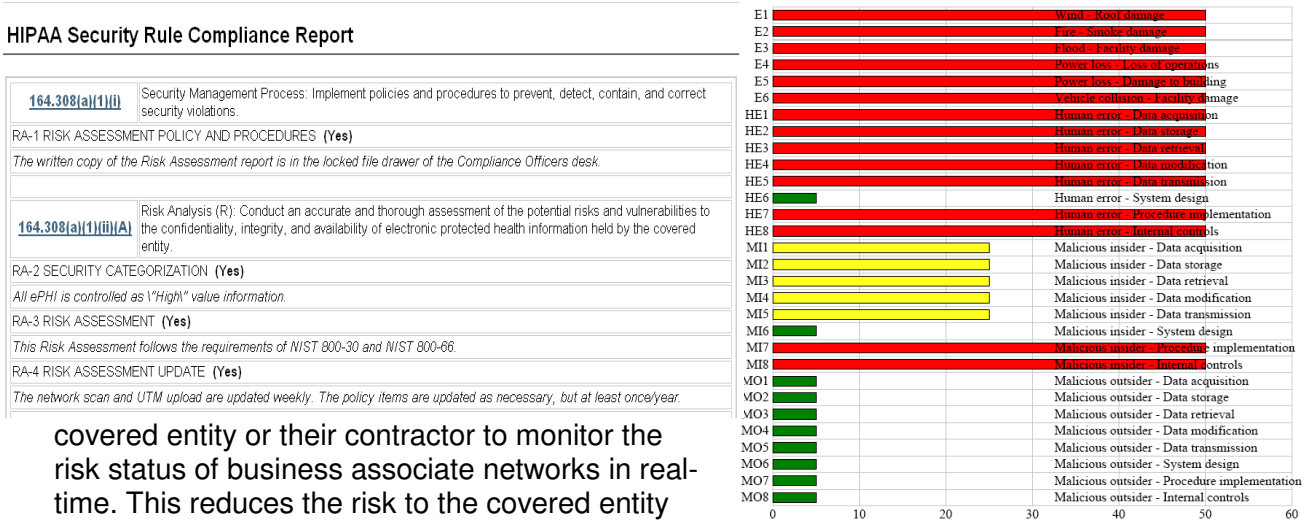
Directions for HIPAA security rule compliance are contained in the National Institute of Standards and Technology (NIST) "Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule (SP 800-66 REV 1)." Other guidance can be found on the CMS 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.

Implementation and Economics

To bring a covered entity and its business associates into compliance with the HIPAA security rule is a four 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.
2. Have the business associate acquire a copy of the HIPAA Compliance Reporter from ACR.
3. Have the business associate scan their workstations and create the Information Security Risk Assessment and the HIPAA Compliance Report. Have the business associate convey a copy of the reports to the covered entity. This information transfer may be done manually or electronically. 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. The Enterprise Console, shown below, allows the

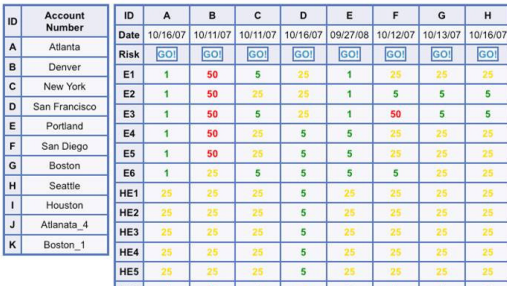


HIPAA Security Rule Compliance Report

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.	

covered entity or their contractor to monitor the risk status of business associate networks in real-time. This reduces the risk to the covered entity and provides technical support to the business associate. In the event that the covered entity or its contractor provides such risk management services to the business associate, a reasonable monitoring fee may be assessed.

4. Once the business associate networks have been secured, a similar process is done for the covered entity. Each department, if more than one, may be treated as a separate risk source. Funds from providing services to the business associates may be used to defray the costs of monitoring.



ID	Account Number
A	Atlanta
B	Denver
C	New York
D	San Francisco
E	Portland
F	San Diego
G	Boston
H	Seattle
I	Houston
J	Atlanata_4
K	Boston_1

ID	A	B	C	D	E	F	G	H
Date	10/16/07	10/11/07	10/11/07	10/16/07	09/27/08	10/12/07	10/13/07	10/16/07
Risk	GO!	GO!	GO!	GO!	GO!	GO!	GO!	GO!
E1	1	50	5	25	1	25	25	25
E2	1	50	25	25	1	5	5	5
E3	1	50	5	25	1	50	5	5
E4	1	50	25	5	5	25	25	25
E5	1	50	25	5	5	25	25	25
E6	1	25	5	5	5	5	25	25
HE1	25	25	25	5	25	25	25	25
HE2	25	25	25	5	25	25	25	25
HE3	25	25	25	5	25	25	25	25
HE4	25	25	25	5	25	25	25	25
HE5	25	25	25	5	25	25	25	25

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. At a time when cybercrime exceeds illegal drugs as a criminal enterprise, effective information security is now a mission critical item.

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