Meaningful Use Requirement for HIPAA Security Risk Assessment

Mary Sirois, MBA, PT, CPHIMSS
Kenneth Clarke, FHIMSS

The Health Information Technology for Economic and Clinical Health Act (HITECH), set forth by Title XIII of the American Reinvestment and Recovery Act of 2009 (ARRA), not only defined requirements for meaningful use of electronic health records but also set forth numerous modifications and enhancements to the Health Information Portability and Accountability (HIPAA) information security and privacy standards.

The HITECH Act requires covered entities to conduct a risk assessment (CFR §164.308(a)(1)(ii)(A)) to determine security risks and implement measures "to sufficiently reduce those risks and vulnerabilities to a reasonable and appropriate level." The meaningful use requirements state that eligible hospitals (EH) and eligible professionals (EP) must "Conduct or review a security risk analysis per 45 CFR 164.308(a)(1) of the certified electronic health record (EHR) technology, and implement security updates and correct identified security deficiencies as part of its risk management process". The meaningful use attestation requirement states that a risk analysis and gaps are addressed as part of the EH's and EP's risk management process; it does not state that any gaps must be resolved prior to meaningful use compliance attestation. While EH and EPs may have certified EHR(s) in place to meet the requirements of the HIPAA security rule for applications, the rule goes well-beyond vendor compliance to address EH's organizational policies, procedures and practices that ensure information security.

The MU attestation requirement does not state that any gaps must be resolved prior to meaningful use attestation.

The added availability and use of EHRs in the patient care process and across the continuum of care poses significant increased risks related to information security and privacy. Now more than ever, EHs and EPs must ensure prudent steps are taken to ensure the security and privacy of electronic patient health information (ePHI). Beyond the requirement to conduct an information security risk assessment, section 13402(e)(4) of the HITECH Act, the Secretary must post a list of breaches of unsecured protected health information affecting 500 or more individuals, therefore covered entities, including business associates, must have a process in place to monitor for such breaches and respond accordingly. Additionally, the HITECH amendments to the HIPAA Security and Privacy rules raised the maximum penalty from $250,000 to $1.5M and now also allow for criminal penalties. The Office of Civil Rights (OCR) is responsible for enforcing both the HIPAA Privacy and Security Rules.

Risk Assessment Requirements

The table below outlines the various assessment areas that should be considered as part of an comprehensive information security risk assessment process.

HIPAA Requirement	**Description**
ADMINISTRATIVE SAFEGUARDS	
Security Management Process (§ 164.308(a)(1))	Implement policies and procedures to prevent, detect, contain, and correct security violations.
Assigned Security Responsibility (§ 164.308(a)(2))	Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity.
Workforce Security (§ 64.308(a)(3))	Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, and to prevent those workforce members who do not have access from obtaining access to electronic protected health information.
Information Access Management (§ 164.308(a)(4))	Implement policies and procedures for authorizing access to electronic protected health information.
Security Awareness and Training (§ 164.308(a)(5))	Implement a security awareness and training program for all members of its workforce (including management).
Security Incident Procedures (§ 164.308(a)(6))	Implement policies and procedures to address security incidents.

HIPAA Requirement	**Description**
Contingency Plan (§ 164.308(a)(7))	Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.
Evaluation (§ 164.308(a)(8))	Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information.
Business Associate Contracts and Other Arrangements (§ 164.308(b)(1))	A covered entity may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with § 164.314(a), that the business associate will appropriately safeguard the information.
PHYSICIAL SAFEGUARDS	
Facility Access Controls (§ 164.310(a)(1))	Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.
Workstation Use (§ 164.310(b))	Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.

HIPAA Requirement	**Description**
Workstation Security (§ 164.310(c))	Implement physical safeguards for all workstations that access electronic protected health information and limit access to authorized users.
Device and Media Controls (§ 164.310(d)(1))	Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.
TECHNICAL SAFEGUARDS	
Access Control (§ 164.312(a)(1))	Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in Business Associate Agreements.
Audit Controls (§ 164.312(b))	Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.
Integrity (§ 164.312(c)(1))	Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.
Person or Entity Authentication (§ 164.312(d))	Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.
Transmission Security (§ 164.312(e)(1))	Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.

HIPAA Requirement	Description
ORGANIZATIONAL SAFEGUARDS	
Business Associate Contracts or Other Arrangements (§ 164.314(a)(1))	(i) The contract or other arrangement between the covered entity and its business associate required by § 164.308(b) must meet the requirements of paragraph (a)(2)(i) or (a)(2)(ii) of this section, as applicable. (ii) A covered entity is not in compliance with the standards in § 164.502(e) and paragraph (a) of this section if the covered entity knew of a pattern of an activity or practice of the business associate that constituted a material breach or violation of the business associate's obligation under the contract or other arrangement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful—(A) Terminated the contract or arrangement, if feasible; or (B) If termination is not feasible, reported the problem to the Secretary.
DOCUMENTATION SAFEGUARDS	
Policies and Procedures (§ 164.316(a))	Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart. A covered entity may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart.
Documentation (§ 164.316(b)(1))	(i) Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and (ii) if an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment.

Each of the requirement areas have a number of specifications that could be considered “required”, “addressable” and “optional”. The “optional” items are those items that DIVURGENT recommends be included in addition to the HIPAA defined “required” and “addressable” items because they exemplify industry best practices.

The **required** aspects as defined in the Security Rule must be complied with. The **addressable** standards must be documented as being analyzed and accepted or replaced or not required with the reason for rejection.

An example of is as follows for the first Administrative Safeguards standards, Security Management Process:

1. Identify Relevant Information Systems (Optional)
2. Conduct Risk Assessment (Required)
3. Implement a Risk Management Program (Required)
4. Acquire IT Systems and Services (Optional)
5. Create and Deploy Policies and Procedures (Optional)
6. Develop and Implement a Sanction Policy (Required)
7. Develop and Deploy the Information System Activity Review Process (Required)
8. Develop Appropriate Standard Operating Procedures (Optional)
9. Implement the Information System Activity Review and Audit Process (Optional)

Threats and Vulnerabilities

In addition to a review of policies and procedures, a complete HIPAA information security assessment should address threats and vulnerabilities of the mission critical systems containing ePHI. Some of these would include:

Threats	Vulnerabilities
Loss of Network	Hardware/Server Failure
Loss of Power	Data Corruption
Loss of Climate Control	Application Failure
Vandalism	Disgruntled IT Employee
Flooding	Disgruntled non-IT Employee
Fire	Unencrypted Backup Files
Natural Disaster	Change Control
	Inappropriate Access by Employee or Contractor

It is imperative to remember that, as stated by CMS, "any provider attesting to receive an EHR incentive payment for either the Medicare EHR Incentive Program or the Medicaid EHR Incentive Program potentially may be subject to an audit." Furthermore, CMS states that "All providers attesting to receive an EHR incentive payment for either Medicare or Medicaid EHR Incentive Programs should retain ALL relevant supporting documentation. Documentation to support the attestation should be retained for six years post-attestation. Documentation to support payment calculations (such as cost report data) should continue to follow the current documentation retention processes."
(https://www.cms.gov/EHRIncentivePrograms/32_Attestation.asp)

As previously stated, eligible hospitals and eligible professionals must conduct a HIPAA security risk assessment as part of their meaningful use readiness activities. DIVURGENT strongly recommends a thorough and well-documented assessment process. Any deficiencies found during the assessment should then be managed and documented in a formal, ongoing information security management process.

About the Authors

Mary Staley-Sirois, MBA, PT, CPHIMSS is Principal of Clinical Transformation at DIVURGENT. Ms. Sirois has nearly 20 years of healthcare operational and strategic planning experience across a wide spectrum of providers and academic environments. As a physical therapist by clinical background, she has worked with large and small healthcare systems on the planning necessary for clinical transformation as a result of an EHR deployment, organization governance and change management, medical and clinical staff collaboration on best practice and evidence-based processes, regulatory compliance readiness and issue resolution, organizational budget development and related benefits realization projection, and detailed project planning. Ms. Sirois' work is focused on leveraging the skills and team of the healthcare organization in the deployment of strategic initiatives - from product development, to operational management, to transformation of clinical process and practice, to EHR adoption. Ms. Sirois is well-published on HIPAA compliance and is a public speaker in healthcare operations and regulatory compliance. In addition to her work in the healthcare provider market, Ms. Sirois works closely with international organizations for the development of operational and educational programs to improve healthcare in developing countries.

Kenneth Clarke, FHIMSS, is an independent consultant with over 30 years of healthcare operational and IT experience across a broad spectrum of healthcare providers and environments. Mr. Clarke has worked with hospitals ranging from critical access hospitals to academic medical centers to large IDNs. Consulting projects included strategic planning, system selection, contract negotiations, clinical EMR governance, IT assessments, budget and total cost of ownership development, project management, and IT organization review and development. Mr. Clarke was also a CIO for a multi-hospital IDN with a multi-specialty physician practice. While there, he successfully implemented an Ambulatory EMR used by 115 providers and led a wide variety of clinical, financial and technology projects. Mr. Clarke is familiar with healthcare regulations, issues, vendors, and technology. He has published a number of articles on contract negotiations and has presented at local and national HIMSS meetings.

About DIVURGENT

Founded by a team of consulting veterans, DIVURGENT is a national health care consulting firm focused solely on the business of hospitals and other healthcare providers. DIVURGENT provides advisory, interim management, revenue cycle management, project management, and modeling and simulation services to help improve patients' lives.

We are committed to:

Providing Thought Leadership

Providing Exceptional Value for our Services

Facilitating Knowledge Transfer

Ensuring Client Satisfaction

DIVURGENT

6119 Greenville Avenue
Suite 144
Dallas, TX 75206

4445 Corporation Lane
Suite 229
Virginia Beach, VA 23462

(877) 254-9794

info@DIVURGENT.com

www.DIVURGENT.com