Management Performance Associates

HIPAA Security Risk Analysis

MPA's HIPAA Security Risk Analysis includes the following:

Objectives

- Determine the strengths and weaknesses of HIPAA Security practices, policies and procedures
- Develop an action plan that prioritizes addressable security practices

Scope of Work

Covered entities must identify where ePHI is stored, received, maintained and transmitted. This is addressed by completing a Security Risk Analysis. MPA's HIPAA Security Risk Analysis will assess the current status of HIPAA security by:

1. Developing a PHI inventory
2. Reviewing documentation of compliance with each HIPAA Security safeguard
3. Reviewing existing HIPAA Security policies and procedures and recommending updates

A list of the security safeguards we will review is on page 5. *Note: MPA's HIPAA Security Risk Analysis is very thorough, as we address each and every HIPAA Security Safeguard, and create an ePHI inventory. We cover all of this material because it is required by the HIPAA Security Rule.*

1. Developing a PHI inventory

Working with you and your IT support, MPA will develop an inventory of all ePHI stored, received, maintained and transmitted by your organization. We will identify and document reasonably anticipated threats and vulnerabilities to ePHI; determine the probability of those threats and vulnerabilities; determine the potential impact of all threats and vulnerabilities; and determine the risk level of these threats and vulnerabilities.

2. Reviewing documentation of compliance with each HIPAA Security safeguard

MPA will work with your Privacy Officer, Security Officer, IT Support and/or Compliance Officer to:

- Identify whether each HIPAA Security Safeguard has been addressed with a procedure
- Determine whether such procedures are documented

- Identify if additional measures are needed to implement safeguards
- Develop an action plan to mitigate risk

3. Reviewing existing HIPAA Security policies and procedures and recommending updates

MPA will review your security policies to determine whether they align with the findings of the HIPAA Security safeguard review (step 2).

Method

Within two weeks of engagement, MPA will provide a HIPAA Program Review Tool that includes:

- Requests for documents (e.g. policies and procedures, audit tools and results, etc.)
- Anonymous HIPAA survey for you to disseminate to your employees
- Customer questions. These questions are designed to obtain information not revealed in the document review. Answers to questions can be provided by Customer in writing; or, Customer and MPA can complete the questions via discussion.

Results

MPA will review the above materials and prepare an Assessment Report, which will include:

- Findings regarding the successes and challenges of the HIPAA Security program
- An action plan with specific recommendations for improving the HIPAA Security program. The action plan can be implemented directly by Customer; or, if requested, with the assistance of additional services or products offered by MPA.
- Risk levels for each area of HIPAA compliance, to help you prioritize your next steps.

Note: The HIPAA review will address a number of areas that require input from you and your IT support. MPA does not provide services to address the IT or technical aspects of the HIPAA Security Risk Analysis. For example, vulnerability scans, penetration tests, or assessment of operating system patch updates. MPA will work with your IT personnel; or MPA can recommend an IT contractor which is also a HIPAA expert to provide a technical evaluation.

Advantages of working with MPA

A team of experts.

Margaret Scavotto, JD, CHC is a nationally recognized compliance expert and speaker, who was trained in health care regulation at Lashly & Baer.

Scott Gima, RN, MHA has over 20 years' experience managing healthcare providers developing quality assurance programs from the clinical perspective, and working with healthcare boards.

Michael Scavotto, MHA has over 40 years' experience as a healthcare executive and hospital physician venture specialist, who has served as a hospital CEO and positioned dozens of healthcare providers for success.

An operational perspective.

MPA's 20+ years of experience managing healthcare providers yields compliance approaches that fit your operational needs. Simply put, MPA understands how compliance requirements are implemented in the daily workings of a nursing home.

Customized approaches to auditing.

MPA evaluates your organization's risks and helps you create an auditing approach tailored to your risks, maximizing your resources.

Flexible service offerings.

Select the amount of compliance support you need: MPA can help you with the entire compliance puzzle, or simply provide the missing piece.

Competitive pricing.

Our clients choose MPA for a competitive price that does not compromise on quality or scope.

Clinical involvement.

Scott Gima, RN brings an operational management and a clinical perspective to our compliance approach, which helps integrate compliance seamlessly with quality care.

Quality and process improvement.

MPA believes compliance is a form of quality and process improvement, and focuses on strengthening both core functions.

HIPAA expertise.

Margaret Scavotto had extensive experience with HIPAA when practicing law at Lashly & Baer, and has continued this skill at MPA. Scott Gima has a wealth of knowledge and expertise on HIPAA Security. Scavotto and Scott Gima provide comprehensive assistance with HIPAA privacy, security and social media use.

A focus on culture and training.

MPA strongly believes a successful compliance program needs ongoing training, and a culture of compliance to support it, and our compliance program effectiveness review evaluates both.

Comprehensive library of compliance tools.

MPA has a comprehensive library of compliance tools at our fingertips. We have spent more than seven years developing practical compliance tools and we have not found a library that is more extensive or user friendly.

EXHIBIT A

HIPAA Program Effectiveness Review Items

Section	Standards	CFR & Specification	Implementation Specifications Description	Required (R) or Addressable (A)	
				(B)	(A)
Administrative Safeguards					
1.0	**Security Management Process**	**164.308(a)(1)**			
1.1		Risk Analysis	Assess potential risks and vulnerabilities with confidentiality, integrity and availability of ePHI	(R)	
1.2		Risk Management	Security measures to minimize ePHI breaches	(R)	
1.3		Sanction Policy	Sanctions/disciplinary action for employees who violate privacy and security policies	(R)	
2.0	Assigned Security Responsibility	164.308(a)(2) Security Officer	Appoint Security Officer – handles privacy policies and procedures	(R)	
3.0	Workforce Security	164.308(a)(3)			
3.1		Authorization and/or Supervision	Procedures for supervision and oversight of employees working with ePHI		(A)
3.2		Workforce Clearance	Procedures that address employee's access to ePHI based on their job responsibilities and minimum necessary requirement		(A)

Section	**Standards**	**CFR & Specification**	**Implementation Specifications Description**	**Required (R) or Addressable (A)**	
				(B)	**(A)**
3.3		Termination Procedures	Procedures to terminate employee access to ePHI after separation from organization		(A)
4.0	Information Access Management	164.308(a)(4)(i)			
4.1		Isolating Health care clearing house functions	Policies and procedures for clearinghouses' protection of its' ePHI	(R)	
4.2		Access Authorization	Policies and procedures for ePHI access through workstations, processes or programs	(R)	
4.3		Access Establishment & Modification	Policies and procedures that are based on access authorization policies. This specification addresses the establishment, documentation and modification of a user's right to access ePHI.	(R)	
5.0	Security Awareness and Training	164.308(a)(5)			
5.1		Security Reminders	Policies and procedures to provide periodic security updates to the workforce		(A)
5.2		Protection from Malicious Software	Policies and procedures for awareness training to guard against malicious software that can access and compromise ePHI		(A)

Section	Standards	CFR & Specification	Implementation Specifications Description	Required (R) or Addressable (A)	
				(B)	**(A)**
5.3		Log-in Monitoring	Policies and procedures to monitor log-in attempts and periodic review of logs to identify unauthorized access to ePHI		(A)
5.4		Password Management	Policies and procedures for creating, changing and safeguarding passwords		(A)
6.0	Security Incident Procedures	164.308(a)(6) Response and Reporting	Policies and Procedures to identify, mitigate and document security breaches or incidents and the effects or impact on ePHI	(R)	
7.0	Contingency Plan	164.308(a)(7)			
7.1		Data Backup Plan	Policies and Procedures and methods to backup ePHI and to obtain copies of ePHI or restoration procedures in the event of a breach or incident that compromises the integrity of the ePHI data	(R)	
7.2		Disaster Recovery Plan	Development and updating of plans to restore data while minimizing disruption to operations	(R)	
7.3		Emergency Mode Operation Plan	Policies and procedures to ensure continuation of critical business operations while protecting ePHI in emergency conditions	(R)	
7.4		Testing and Revision Procedures	Policies and procedures for periodic testing and revising of all phases of the contingency plan		(A)
7.5		Applications and Data Criticality Analysis	Analysis and review of software applications, data and IT systems (that support apps and data) that are important or required for critical		(A)

Section	Standards	CFR & Specification	Implementation Specifications Description	Required (R) or Addressable (A)	
				(B)	(A)
			operations. This determines the order of applications and data restoration		
8.0	Evaluation	164.308(a)(8)	Periodic assessment of technical and non-technical elements of ePHI security. This needs to be done in response to changes in the cybersecurity environment or operational changes	(R)	
9.0	Business Associate Contracts and Other Arrangements	164.308(b)(1) Written Contract or Other Arrangement	Develop and implement Business Associates agreements with vendors requiring their compliance with all BA HIPAA requirements	(R)	
Physical Safeguards					
10.0	Facility Access Controls	164.310(a)(1)			
10.1		Contingency Operations	Policies and procedures that allow access to facility or organization and data restoration in emergency situations		(A)
10.2		Facility Security Plan	Policies and procedures to protect facility and its equipment from unauthorized access, tampering or theft		(A)
10.3		Access Control and Validation Procedures	Policies and procedures to control validate person's physical access to facility or areas of the facility based on their role/function and control access to software programs for testing and revision (vendor access to areas of systems that contain ePHI).		(A)
10.4		Maintenance Records	Policies and procedures to document repairs and changes to the parts of a		(A)

Section	Standards	CFR & Specification	Implementation Specifications Description	Required (R) or Addressable (A)	
				(B)	**(A)**
			facility dealing with physical security related to protecting ePHI.		
11.0	Workstation Use	164.310(b)	Policies and procedures that specify workstation functions, how the functions are to be performed and the physical surroundings around the workstations to protect ePHI	(R)	
12.0	Workstation Security	164.310(c)	Policies and procedures to restrict access to all workstations to authorized user(s)	(R)	
13.0	Device and Media Controls	164.310(d)(1)			
13.1		Disposal	Policies and procedures for permanent removal of ePHI data that is stored or resides on electronic media or hardware.	(R)	
13.2		Media Re-use	Policies and procedures for permanent removal of ePHI data that is stored or resides on electronic media or hardware before the hardware or media is reused or reissued.	(R)	
13.3		Accountability	Policies and procedures for documenting the permanent removal of ePHI from hardware or electronic media		(A)
13.4		Data Backup and Storage	Creating validated copies of ePHI when it is necessary to move ePHI data between electronic media or hardware. Copies must be exact, retrievable and properly protected.		(A)
Technical Safeguards					

Section	Standards	CFR & Specification	Implementation Specifications Description	Required (R) or Addressable (A)	
				(B)	(A)
14.0	Access Control	164.312(a)(1)			
14.1		Unique User Identification	Each workforce member is assigned a user ID specific to each person	(R)	
14.2		Emergency Access Procedure	Procedures for timely access to ePHI when there is loss of data and/or systems during an emergency.	(R)	
14.3		Automatic Logoff	Specifying timed logoff's that automatically lock workstations. Timeout periods are based on proximity to unauthorized physical access (high-traffic areas)		(A)
14.4		Encryption and Decryption	Based on a risk analysis, determine the need for encryption/decryption of ePHI data that resides or is stored on workstations and electronic media. This includes ePHI data at rest and in motion.		(A)
15.0	Audit Controls	164.312(b)	Develop mechanisms to capture and review activity in systems, programs and applications that contain ePHI. Audit controls all the monitoring of workforce activities and actions, mitigating security incidents, policy enforcement and/or network troubleshooting.	(R)	
16.0	Integrity	164.312(c)(1) Mechanism to Authenticate Electronic Protected Health Information	Policies and procedures to ensure ePHI data is accurate and dependable for access or retrieval by preventing improper alteration or destruction of ePHI data.		(A)

Section	Standards	CFR & Specification	Implementation Specifications Description	Required (R) or Addressable (A)	
				(B)	**(A)**
17.0	Person or Entity Authentication	164.312(d) Verifying user is the correct user	Workforce members do not allow others to use their ID/passwords. Verify receiver of ePHI before it is sent. Determination of the need for multi-factor user authentication in addition of ID/passwords	(R)	
18.0	Transmission Security	164.312(e)(1)			
18.1		Integrity Controls	Security measures to protect the integrity of electronically transmitted ePHI		(A)
18.2		Encryption	Determine the need for encrypting the transmission of ePHI.		(A)
Organizational Requirements					
19.0	Business Associate Contracts or Other Arrangements	164.314(a)(1)			
19.1		Business Associate Contracts	BAAs will ensure that a BA or its subcontractor that creates, maintains or transmits ePHI will agree to protect ePHI and report any security incidents to the BA.	(R)	
19.2		Other Arrangements	The BA must abide by 19.1 for any other arrangements with vendors that create, maintain or transmit ePHI.	(R)	
20.0	Requirements for Group Health Plans	164.314(b)(1) Implementation Specifications	Group health plans and/or its plan sponsor must safeguard its ePHI.	(R)	

Section	Standards	CFR & Specification	Implementation Specifications Description	Required (R) or Addressable (A)	
				(B)	(A)
Policies and Procedures and Documentation Requirements					
21.0	Policies and Procedures	164.316(a) Policy documentation	All required and necessary HIPAA policies and procedures must be documented. Other required communication, action, activity or designation must also be documented.	(R)	
22.0	Documentation	164.316(b)(1)			
22.1		Time Limit	Retain documentation for 6 years	(R)	
22.2		Availability	Documentation must be made available	(R)	
22.3		Updates	Periodic documentation review is required as needed in response to changes in environment or operations that affect ePHI security	(R)	