An Exec Brief

HIPAA Compliance Readiness

ecfirst | HIPAA™ Academy

Ali Pabrai
Global Cyber Defense Thought Leader

Table of Contents

Methodology for Healthcare Information Security

Figure 1: HIPAA Compliance Life Cycle.

Figure 1 describes the seven-step methodology for a credible HIPAA compliance program. The seven steps establish a life-cycle approach for continual HIPAA compliance. From clearly establishing responsibility in Step 1, to an actively monitored risk management program, organizations must ensure an evidence-based program for an effective HIPAA compliance program.

Most organizations, be they covered entities or business associates, are impacted by more than one regulation. Your organization may be impacted by not just HIPAA, but other mandates such as PCI DSS, NIST, or state regulations such as CCPA or global standards such as GDPR. Hence the recommendation that all organizations directly or indirectly impacted by the HIPAA mandate go beyond the compliance requirements to address not just ePHI, but all vital enterprise assets and sensitive information.

1 Assigned Responsibility

Objective: Assigned Responsibility includes the following activities:

1. Develop a specific job description.
2. Assign responsibility for the organization's Information Security Officer (ISO).
3. Communicate ISO role to organization.
4. Establish priority and budget.

The organization must clearly establish job responsibilities and associated authority to address this requirement. Next, identify who in the organization will be responsible for coordinating all activities and initiatives to enable compliance with HIPAA. This individual will also be responsible for leading or coordinating the development of all security policies and procedures and coordinating the deployment of appropriate security technologies. The ISO will identify key team members to assist with security activities.

Smaller organizations may assign this responsibility to the Compliance or Privacy Officer. The individual identified must be very familiar with HIPAA as well as have a broad understanding of security policies and technologies. Once the individual has been identified, next determine the team that will be working together to assist with HIPAA priorities.

The core team responsible for implementing HIPAA requirements must next acquire the necessary knowledge so that there is consistent and intimate knowledge of this area. Training in HIPAA requirements and corresponding certifications such as the Certified HIPAA Professional, CHP™, Certified HIPAA Security Specialist, CHSS™, and the Certified Security Compliance Specialist, CSCS™, provides an excellent knowledge base for the Security Officer and their team.

Finally, the individual responsible must determine an initial budget for the next critical step, risk analysis. Based on compliance and cybersecurity priorities, a budget is developed for the fiscal period.

Assign Security Responsibility is a HIPAA Security Rule Standard defined within the Administrative Safeguards section (164.308 (a) (2)).

2 Risk Analysis

Objective: Risk Analysis includes the following activities:

1. Conduct a technical cybersecurity vulnerability assessment and penetration testing.
2. Perform a Business Impact Analysis (BIA) and identify contingency plan requirements.
3. Actively ensure information system activity review and assessment of audit controls across systems and applications.

As part of the vulnerability assessment initiative, the organization must create an inventory of all vital enterprise assets, systems and communications. Asset management is addressed in this step. Consider all assets, including IoT, biomed as well as systems and applications in the cloud. This provides the basis for a comprehensive risk analysis and an information system activity review.

A risk analysis identifies areas that need to be addressed for HIPAA security compliance as well as all gaps that may be exploited by unauthorized parties be, they insiders or external hackers. Organizations must conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of ePHI. As part of the risk analysis process, organizations must:

1. Identify critical assets and the threats to those assets.
2. Identify the vulnerabilities that expose those threats.

The Risk Analysis team must create a pre-assessment checklist to document information about all critical systems and applications that process or store electronic PHI. The Risk Analysis team then specifically identifies:

- Key information technology systems and components for each critical asset.
- Key systems and components for technology weaknesses/vulnerabilities that may be exploited.

Vulnerability tools such as scanning software, checklists and scripts may be used to identify weaknesses in the security of systems and networks.

The analysis team identifies the impact of threats to critical assets to define risks, develop criteria to evaluate those risks, and evaluate the risk impact based on the criteria developed.

The objective of an information system activity review is to review records such as audit logs, access reports, and security incident tracking reports. This is an important activity. It enables the organization to review the type of information that is currently being logged or recorded and determine if there is a need to record additional information and/or identify additional systems that need to be monitored. In the event of an incident, complaint, or audit, the organization must be able to definitively prove who did what to what data, when?

The team must also perform a BIA exercise to identify requirements for contingency planning and disaster recovery.

Risk Analysis is a HIPAA Security Rule implementation specification defined within the Security Management Process Standard in the Administrative Safeguards section (164.308 (a) (1)) that is required, not addressable.

3 Policy and Procedure

Objective: Policy and Procedure includes the following activities:

1. Develop information security plan documents such as Cybersecurity, Contingency, and Incident Response Management.
2. Build a library of comprehensive cybersecurity policies.
3. Create procedure documents.

Organizations must develop a security strategy and risk mitigation plans appropriate for the organization's mission and priorities. Organizations must implement reasonable and appropriate policies and procedures to comply with HIPAA requirements. All organizations must maintain the policies and procedures implemented in written (which may be electronic) form.

The security strategy provides the framework and blueprint for a credible cyber defense. The cybersecurity strategy must provide the basis for a comprehensive and scalable solution that is based on core business objectives, legislative requirements, and threats to the enterprise.

Figure 2 describes the typical policies that an organization may develop to address HIPAA mandates.

#	Policy Name	Policy Description
	Information Security Policies	
1	**Information Security Strategy Policy** HIPAA Reference § 164.308 (a)(1)(i)	The purpose is to provide reasonable and appropriate safeguards to ensure the confidentiality, integrity, and availability of information assets by protecting those assets from unauthorized access, modification, destruction, or disclosure.
2	***Security Management Process Policy*** HIPAA Reference § 164.308 (a)(1)(i) STD	The purpose is to implement policies and procedures to prevent, detect, contain, and correct security violations.
3	**Risk Analysis Policy** HIPAA Reference § 164.308 (a)(1)(ii)(A) SPEC	The purpose is to conduct an accurate and thorough assessment of the risks and vulnerabilities to the confidentiality, integrity, and availability of sensitive information held by the organization.
4	**Risk Management Policy** HIPAA Reference § 164.308 (a)(1)(ii)(B) SPEC	The purpose is to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with impacted regulations.
5	**Sanction Policy** HIPAA Reference § 164.308 (a)(1)(ii)(C) SPEC	The purpose is to apply appropriate sanctions against workforce members who fail to comply with the security policies or procedures of the organization.
6	**Information System Activity Review Policy** HIPAA Reference § 164.308 (a)(1)(ii)(D) SPEC	The purpose is to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.
7	***Assigned Security Responsibility Policy*** HIPAA Reference *§ 164.308 (a)(2) STD*	The purpose of this policy is to identify the security official who is responsible for the development and implementation of policies and procedures required by regulatory mandates 164.308(a)(2).
8	***Workforce Security Policy*** HIPAA Reference *§ 164.308 (a)(3)*(i) STD	The purpose is to implement policies and procedures to ensure that all members of the workforce have appropriate access to sensitive information and to prevent those workforce members who should not have access from obtaining access to sensitive information.

#	Policy Name	Policy Description
	Information Security Policies	
9	**Authorization and/or Supervision Policy** HIPAA Reference § 164.308 (a)(3)(ii)(A) SPEC	The purpose is to implement procedures for the authorization and/or supervision of workforce members who work with sensitive information or in locations where it might be accessed.
10	**Workforce Clearance Policy** HIPAA Reference § 164.308 (a)(3)(ii)(B) SPEC	The purpose is to implement procedures to determine the access of a workforce member to sensitive information is appropriate.
11	**Termination Policy** HIPAA Reference § 164.308 (a)(3)(ii)(C) SPEC	The purpose is to implement procedures for quickly, securely, and completely terminating access to sensitive information when the employment of a workforce member or other arrangement ends.
12	***Information Access Management Policy*** HIPAA Reference § 164.308 (a)(4)(i) STD	The purpose is to implement policies and procedures for authorizing access to sensitive information.
13	**Access Authorization Policy** HIPAA Reference § 164.308 (a)(4)(ii)(B) SPEC	The purpose is to implement policies and procedures for granting access to sensitive information, for example, authorization required to access a workstation, transaction, program, process, or other mechanism.
14	**Access Establishment and Modification Policy** HIPAA Reference § 164.308 (a)(4)(ii)(C) SPEC	The purpose is to implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.
15	***Security Awareness and Training Policy*** HIPAA Reference *§ 164.308 (a)(5)*(i) STD	The purpose is to implement a security awareness and training program for all members of the organization's workforce, including management.
16	**Security Reminders Policy** HIPAA Reference § 164.308 (a)(5)(ii)(A) SPEC	The purpose is to implement and ensure that periodic security reminders are distributed to all members of the workforce.

#	Policy Name	Policy Description
	Information Security Policies	
17	**Protection from Malicious Software Policy** HIPAA Reference § 164.308 (a)(5)(ii)(B) SPEC	The purpose is to implement procedures for guarding against, detecting, and reporting malicious software.
18	**Patch Management Policy** HIPAA Reference § 164.308 (a)(1)(ii)(B) SPEC	The purpose is to ensure the security of organization member data by installing security patches in timely fashion.
19	**Log-in Monitoring Policy** HIPAA Reference § 164.308 (a)(5)(ii)(C) SPEC	The purpose is to implement procedures for monitoring log-in attempts and reporting discrepancies.
20	**Password Management Policy** HIPAA Reference § 164.308 (a)(5)(ii)(D) SPEC	The purpose is to implement procedures for creating, changing and safeguarding passwords.
21	***Security Incident Policy*** HIPAA Reference § 164.308 (a)(6)(i) STD	The purpose is to thoroughly address security incidents.
22	**Response and Reporting Policy** HIPAA Reference § 164.308 (a)(6)(ii) SPEC	The purpose is to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the organization, and document security incidents and their outcomes.
23	***Contingency Plan Policy*** HIPAA Reference § 164.308 (a)(7)(i) STD	The purpose is to 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 sensitive information.
24	**Data Backup Plan Policy** HIPAA Reference § 164.308 (a)(7)(ii)(A) SPEC	The purpose is to establish and implement procedures to create and maintain retrievable exact copies of sensitive information in the event of equipment failure or damage.

#	Policy Name	Policy Description
	Information Security Policies	
25	**Emergency Mode Operation Plan Policy** HIPAA Reference § 164.308 (a)(7)(ii)(C) SPEC	The purpose is to establish and implement as needed procedures to enable continuation of critical business processes for protection of the security of sensitive information while operating in an emergency mode.
26	**Testing and Revision Policy** HIPAA Reference § 164.308 (a)(7)(ii)(D) SPEC	The purpose is to implement procedures for periodic testing and revision of contingency plans.
27	**Applications and Data Criticality Analysis Policy** HIPAA Reference § 164.308 (a)(7)(ii)(E) SPEC	The purpose is to assess the relative criticality of specific applications and data in support of other contingency plan components.
28	***Evaluation Policy*** HIPAA Reference *§ 164.308 (a)(8) STD*	The purpose is to perform a technical and non-technical evaluation that establishes the extent to which the organization's security policies and procedures meet the requirements of impacted regulations.
29	***Business Associate Agreement and Other Arrangements Policy*** HIPAA Reference *§ 164.308 (b)(1) STD*	The purpose is to obtain satisfactory assurances that the business associate will appropriately safeguard all sensitive information in accordance with applicable regulations.
30	***Facility Access Controls Policy*** HIPAA Reference § 164.310 (a)(1) STD	The purpose is to implement policies and procedures to limit physical access to the organization's electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.
31	**Contingency Operations Policy** HIPAA Reference § 164.310 (a)(2)(i) SPEC	The purpose is to establish and implement as needed procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.

#	Policy Name	Policy Description
	Information Security Policies	
32	**Facility Security Plan Policy** HIPAA Reference § 164.310 (a)(2)(ii) SPEC	The purpose is to implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.
33	**Access Control and Validation Policy** HIPAA Reference § 164.310 (a)(2)(iii) SPEC	The purpose is to implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control access to software programs for testing and revision. To ensure that employees are able to access the information that is appropriate and required in their positions and that all other office and patient information remains confidential.
34	**Maintenance Records Policy** HIPAA Reference § 164.310 (a)(2)(iv) SPEC	The purpose is to implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).
35	***Workstation Use Policy*** HIPAA Reference *§ 164.310 (b) STD*	The purpose is to 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 sensitive information.
36	***Workstation Security Policy*** HIPAA Reference *§ 164.310 (c) STD*	The purpose is to implement physical safeguards for all workstations that access sensitive information and to restrict access to authorized users.
37	***Device and Media Controls Policy*** HIPAA Reference § 164.310 (d)(1) STD	The purpose is to implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain sensitive information into and out of a facility, and the movement of these items within a facility.
38	**Disposal Policy** HIPAA Reference § 164.310 (d)(2)(i) SPEC	The purpose is to implement policies and procedures to address the final disposition of sensitive information and/or the hardware or electronic media on which it is stored.

#	Policy Name	Policy Description
	Information Security Policies	
39	**Media Re-Use Policy** HIPAA Reference § 164.310 (d)(2)(ii) SPEC	The purpose is to implement procedures for removal of sensitive information from electronic media before the media are made available for re-use.
40	**Accountability Policy** HIPAA Reference § 164.310 (d)(2)(iii) SPEC	The purpose is to maintain a record of the movements of hardware and electronic media and any person responsible therefore.
41	**Data Backup and Storage Policy** HIPAA Reference § 164.310 (d)(2)(iv) SPEC	The purpose is to create a retrievable, exact copy of sensitive information, when needed, prior to the movement of equipment.
42	***Access Control Policy*** HIPAA Reference § 164.312 (a)(1) STD	The purpose is to implement technical policies and procedures for electronic information systems that maintain sensitive information to allow access only to those persons or software programs that have been granted access rights as specified by regulation or business process.
43	**Unique User Identification Policy** HIPAA Reference § 164.312 (a)(2)(i) SPEC	The purpose is to assign a unique name and/or number for identifying and tracking user identity.
44	**Emergency Access Policy** HIPAA Reference § 164.312 (a)(2)(ii) SPEC	The purpose is to establish and implement as necessary authorized access sensitive information during an emergency.
45	**Automatic Logoff Policy** HIPAA Reference § 164.312 (a)(2)(iii) SPEC	The purpose is to implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.
46	**Encryption and Decryption Policy** HIPAA Reference § 164.312 (a)(2)(iv) SPEC	The purpose is to implement a mechanism to encrypt and decrypt sensitive information. The Encryption Policy is intended to assist employees of the organization in making a decision about the use of encryption technologies as a method of protecting data stored on systems that process sensitive information.
47	***Audit Controls Policy*** HIPAA Reference *§ 164.312 (b) STD*	The purpose is to implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use sensitive information.
48	***Integrity Policy*** HIPAA Reference *§ 164.312 (c)(1) STD*	The purpose is to implement policies and procedures to protect sensitive information from improper alteration or destruction.
49	**Mechanism to Authenticate Sensitive Information Policy** HIPAA Reference § 164.312 (c)(2) SPEC	The purpose is to implement electronic mechanisms to corroborate that sensitive information has not been altered or destroyed in any unauthorized manner.
50	***Person or Entity Authentication Policy*** HIPAA Reference *§ 164.312 (d) STD*	The purpose is to implement procedures to verify that the person or entity seeking access to sensitive information is the one claimed.
51	***Transmission Security Policy*** HIPAA Reference *§ 164.312 (e)(1) STD*	The purpose is to implement technical security measures to guard against unauthorized access to sensitive information that is being transmitted over an electronic communications network.
52	**Integrity Controls Policy** HIPAA Reference § 164.312 (e)(2)(i) SPEC	The purpose is to implement security measures to ensure that electronically transmitted sensitive information is not improperly modified without detection until disposed of.
53	**Encryption Policy** HIPAA Reference § 164.312 (e)(2)(ii) SPEC	The purpose is to implement a mechanism to encrypt sensitive information in transit whenever deemed appropriate.
54	***Policies and Procedures Standard Policy*** HIPAA Reference *§ 164.316 (a) STD*	The purpose is to implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications and other requirements of impacted regulations.

#	Policy Name	Policy Description
	Information Security Policies	
55	***Documentation Standard Policy*** HIPAA Reference *§ 164.316 (b)(1) STD*	The purpose is to maintain the policies and procedures implemented to comply with the impacted regulation in written (or electronic) form and if an action, activity or assessment is required to maintain a written (which may be electronic) record of that action, activity or assessment.
56	**Information Classification Policy** HIPAA Reference § 164.308 (a)(1)(ii)(B) SPEC	The purpose is to address information classification categories, acceptable access and use of information such as ePHI and other sensitive information.
57	**Network Security Policy** HIPAA Reference § 164.312 (e)(1) STD	The purpose is to establish standards for secure communication devices and data on equipment that is owned and/or operated by the organization. By securing the organization's network and infrastructure, the organization will minimize unauthorized access to the organization's proprietary information and technology.
58	**Email Security Policy** HIPAA Reference § 164.312 (e)(1) STD	The purpose is to protect the confidentiality and integrity of sensitive information that may be sent or received via email.
59	**Remote Access Policy** HIPAA Reference § 164.312 (e)(1) STD	The purpose is to implement security measures sufficient to reduce risks and vulnerabilities of remote access connections to the organization's enterprise infrastructure to a reasonable and appropriate level.
60	**VPN Policy** HIPAA Reference § 164.312 (e)(1) STD	The purpose is to implement security measures sufficient to reduce the risks and vulnerabilities of the organization's VPN infrastructure to a reasonable and appropriate level.
61	**Wireless Security Policy** HIPAA Reference § 164.312 (e)(1) STD	The purpose is to implement security measures sufficient to reduce risks and vulnerabilities of the organization's wireless infrastructure to a reasonable and appropriate level.
62	**Wireless IP Phone Policy** HIPAA Reference § 164.312 (e)(1) STD	The purpose is to implement security measures sufficient to reduce risks and vulnerabilities of the organization's wireless IP phones to a reasonable and appropriate level.

#	Policy Name	Policy Description
	Information Security Policies	
63	**Bring Your Own Device (BYOD) Policy** HIPAA Reference § 164.310 (d)(1) STD	The purpose is to address the rights and obligations of both owners of a device used for the company's work and the organization's rights and obligations to protect and own its data on these devices.
64	**Biomedical Device Security Policy** HIPAA Reference § 164.310 (d)(1) STD	The purpose is to provide reasonable and appropriate safeguards to ensure the Confidentiality, Integrity, and Availability (CIA) of biomedical devices connected to the network infrastructure.
65	**Data Breach Discovery** HIPAA Reference § 164.404 (a) STD	The purpose is to assist employees of the organization in defining and identifying potential security breaches of protected information, such as Protected Health Information (PHI), personal information or other confidential information.
66	**Data Breach Management** HIPAA Reference § 164.404 (a) STD	The purpose is to provide guidance on decisions made and actions taken following the identification of a data breach. This policy is designed to minimize the loss and destruction of data, mitigate the weakness that was exploited, and restore all computing and other impacted services to organization.
67	**Data Breach Notification** HIPAA Reference § 164.404 (a) STD	The purpose of this policy is to ensure the HIPAA Administrative Simplification Requirements Subpart B (Notification in the Case of Breach of Unsecured PHI) and with additional state regulation(s), as applicable, with respect to unsecured PHI, Personal Identifiable Information (PII), or other confidential information, and to provide methods and content of notification are complied with.
68	**Data Breach Notification to the Secretary of HHS** HIPAA Reference § 164.404 (a) STD	The purpose is to provide guidance on when and how to notify the Department of Health and Human Services (HHS) following a breach of protected information.
69	**Data Breach Notification to Individuals** HIPAA Reference § 164.404 (a) STD	The purpose is to provide guidance on when and how to notify the impacted patient(s) following a breach of protected information.

#	Policy Name	Policy Description
	Information Security Policies	
70	**Data Breach Notification to Media** HIPAA Reference § 164.404 (a) STD	The purpose is to provide specific guidance on when and how to notify the media following a breach of protected information.
71	**Social Media Policy** HIPAA Reference § 164.308 (a)(5)(i) STD	The purpose is to ensure staff members who use social media, either as part of their job or in a personal capacity, understand the organization's expectations for social media engagements concerning the organization, its services, staff, patients, its competitors, its vendors and/or business-related individuals or organizations.
71	**Mobile Devices Policy** HIPAA Reference § 164.310 (d)(1) STD	The purpose is to address the appropriate protection of Sensitive Electronic Information (SEI) when it is stored, transferred or accessed on mobile devices such as: laptops / smart phones (devices with operating systems) or removable media such as: USB Flash drives / memory cards / floppy disks / CDs / DVDs.
72	**Secure Text Message Policy** HIPAA Reference § 164.312 (e)(1) STD	The purpose is to ensure the risk associated with text messaging sensitive information in a clinical setting is managed appropriately to safeguard both the privacy and security of the information exchanged. Under the regulatory mandates (164.308 (a) (1) (ii) (A) and (B)), text messaging is addressed as part of the organization comprehensive risk analysis and management strategy.
73	**Firewall Policy** HIPAA Reference § 164.308 (a)(1)(ii)(B) SPEC	The purpose is to ensure establishment of configuration standards, installs and maintenance of firewall configurations, and restriction of connections between untrusted networks and networks/systems containing, or providing access to, sensitive information.
74	**Isolating Health Care Clearinghouse Policy** HIPAA Reference § 164.308 (a)(4)(ii)(A) SPEC	The purpose is to describe how clearinghouse functions are isolated so that electronic Protected Health Information (ePHI) in the clearinghouse is separated from other functions that the organization performs.
75	**Baseline Configuration Policy** HIPAA Reference § 164.308 (a)(1)(ii)(B) SPEC	The purpose is to ensure that systems are securely configured and deployed in a repeatable manor that addresses the confidentiality, integrity, and availability of sensitive information that may be stored, processed, or transmitted by such systems.
76	**Acceptable Use Policy** HIPAA Reference § 164.310 (b) STD	The purpose is to outline the acceptable use of computer equipment. Inappropriate use exposes to risks including virus attacks, compromise of network systems and services, and legal issues.
77	**Data & Hardware Acquisition Policy** HIPAA Reference § 164.310 (d)(2)(iii) SPEC	The purpose is to ensure that resources are used as effectively as possible and that data security standards are protecting the organization's data, all acquisitions of technology hardware, on-site software, software as a service (SAAS or "cloud") or consulting contracts.
78	**Code of Ethics and Business Conduct Policy** HIPAA Reference § 164.308 (a)(1)(ii)(B)	The purpose of this policy aims to provide guidance to behave ethically and in accordance with the values and applicable laws. The goal is not simply to follow the legal rules that applies, but to behave ethically in all situations.
79	**Vendor Risk Management Policy** HIPAA Reference § 164.308 (a)(1)(ii)(A) SPEC § 164.308 (a)(1)(ii)(B) SPEC § 164.308 (b)(1) STD	The purpose is to establish the organization commitment to comprehensive and effective asset management controls pertaining to supplier relationships and vendor risk management. The controls protect the organization from data loss and information exposure to vendors that maintain access to the systems and networks as may be required by regulatory mandates.

Figure 2: Security Policy Index.

The organization must create library of security procedures so that security practices are followed consistently. Examples of procedures that are typically developed are included in Figure 3.

#	Policy Name	Policy Description
	Information Security Procedures	
1	**Information Security Strategy Procedure** HIPAA Reference § 164.308 (a)(1)(i)	To provide procedures for implementation of reasonable and appropriate safeguards to ensure the confidentiality, integrity, and availability (CIA) of information assets by protecting those assets from unauthorized access, modification, destruction, and disclosure.
2	***Security Management Process Procedure*** HIPAA Reference § 164.308 (a)(1)(i)	To implement procedures to prevent, detect, contain, and correct security violations.
3	**Risk Analysis Procedure** HIPAA Reference §164.308 (a)(1)(ii)(A)	To outline procedures used to conduct an accurate and thorough assessment of the risks and vulnerabilities to the confidentiality, integrity, and availability of sensitive information held by the organization.
4	**Risk Management Procedure** HIPAA Reference §164.308 (a)(1)(ii)(B)	To implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with impacted regulations.
5	**Sanction Procedure** HIPAA Reference §164.308 (a)(1)(ii)(C)	To apply appropriate sanctions against workforce members who fail to comply with the security policies or procedures of ORGANIZATION_NAME.
6	**Information System Activity Review Procedure** HIPAA Reference §164.308 (a)(1)(ii)(D)	To regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.
7	***Assigned Security Responsibility Procedure*** HIPAA Reference §164.308 (a)(2)	To identify the security official responsible for the development and implementation of the policies and procedures required by the HIPAA Security Rule 164.308(a)(2).
8	***Workforce Security Procedure*** HIPAA Reference §164.308 (a)(3)(i)	To implement policies and procedures to ensure all workforce members of the have appropriate access to sensitive information and to prevent workforce members who should not have access from obtaining access to sensitive information.
9	**Authorization and/or Supervision Procedure** HIPAA Reference §164.308 (a)(3)(ii)(A)	To implement procedures for the authorization and/or supervision of workforce members who work with sensitive information or in locations where it may be accessed.
10	**Workforce Clearance Procedure** HIPAA Reference §164.308 (a)(3)(ii)(B)	To implement procedures to determine the access of a workforce member to sensitive information is appropriate.
11	**Termination Procedure** HIPAA Reference §164.308 (a)(3)(ii)(C)	To implement procedures for quickly, securely, and completely terminating access to sensitive information when the employment of a workforce member or other arrangement ends.
12	***Information Access Management Procedure*** HIPAA Reference §164.308 (a)(4)(i)	To implement policies and procedures for authorizing access to sensitive information.
13	**Access Authorization Procedure** HIPAA Reference §164.308 (a)(4)(ii)(B)	To implement policies and procedures for granting access to sensitive information, for example, authorization required to access a workstation, transaction, program, process, or other mechanism.
14	**Access Establishment and Modification Procedure** HIPAA Reference §164.308 (a)(4)(ii)(C)	To implement policies and procedures that, based ORGANIZATION_NAME's access authorization procedures, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.
15	***Security Awareness and Training Procedure*** HIPAA Reference §164.308 (a)(5)(i)	To implement a security awareness and training program for all ORGANIZATION_NAME workforce members, including management.

#	Policy Name	Policy Description
	Information Security Procedures	
16	**Security Reminders Procedure** HIPAA Reference §164.308 (a)(5)(ii)(A)	To implement and ensure periodic security reminders are distributed to all workforce members.
17	**Protection from Malicious Software Procedure** HIPAA Reference §164.308 (a)(5)(ii)(B)	To implement procedures for guarding against, detecting, and reporting malicious software.
18	**Log-in Monitoring Procedure** HIPAA Reference §164.308 (a)(5)(ii)(C)	To implement procedures for monitoring log-in attempts and reporting discrepancies.
19	**Password Management Procedure** HIPAA Reference §164.308 (a)(5)(ii)(D)	To establish procedures for creating, changing, and safeguarding passwords.
20	***Security Incident Procedures*** HIPAA Reference §164.308 (a)(6)(i)	To thoroughly address the policy and procedures related to security incidents.
21	**Security Incident Procedure for Compromised IT Resources** HIPAA Reference §164.308 (a)(6)(i)	Implement procedures to address security incidents. Compromised IT resources include attack/exploit, backdoor or Trojan, denial of service (DoS), malware, unauthorized access, etc.
22	**Security Incident Procedure for Suspicious Activity** HIPAA Reference §164.308 (a)(6)(i)	Implement procedures to address security incidents. Examples of suspicious activity include sweeps, scans, unusual connection, excessive bandwidth, excessive internet usage, inappropriate use of the email system, etc.
23	**Security Incident Procedure for Violations of IT Procedure** HIPAA Reference §164.308 (a)(6)(i)	Implement procedures to address security incidents. Examples of suspicious activity include excessive or disruptive use of Internet or e-mail, unauthorized access, privacy, spam, inappropriate content, suspicious activity, etc.
24	**Security Incident Procedure for Vulnerabilities** HIPAA Reference §164.308 (a)(6)(i)	Implement procedures to address security incidents. Vulnerabilities include patch or upgrade requirements, weak passwords, unrestricted access, etc.
25	**Security Incident Response and Reporting Procedure** HIPAA Reference §164.308 (a)(6)(i)	Implement procedures to report security incidents.
26	**Response and Reporting Procedure** HIPAA Reference §164.308 (a)(6)(ii)	To identify and respond to suspected or known security incidents, mitigate, to the extent practicable, harmful effects of security incidents known to ORGANIZATION_NAME, and document security incidents and their outcomes.
27	***Contingency Plan Procedure*** HIPAA Reference §164.308 (a)(7)(i)	To 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 containing sensitive information.
28	**Data Backup Plan Procedure** HIPAA Reference §164.308 (a)(7)(ii)(A)	To establish and implement procedures to create and maintain retrievable exact copies of sensitive information in the event of equipment failure or damage.
29	**Disaster Recovery Plan Procedure** HIPAA Reference §164.308 (a)(5)(i)	To establish and implement as needed procedures to restore any loss of data.

#	Policy Name	Policy Description
	Information Security Procedures	
30	**Emergency Mode Operation Plan Procedure** HIPAA Reference §164.308 (a)(7)(ii)(C)	To establish and implement procedures to enable continuation of critical business processes for protection of the security of sensitive information while operating in an emergency mode, as needed.
31	**Testing and Revision Procedures** HIPAA Reference §164.308 (a)(7)(ii)(D)	To implement procedures for periodic testing and revision of contingency plans.
32	**Applications and Data Criticality Analysis Procedure** HIPAA Reference §164.308 (a)(7)(ii)(E)	To assess the relative criticality of specific applications and data in support of other contingency plan components.
33	***Evaluation Procedure*** HIPAA Reference §164.308 (a)(8)	To perform a technical and non-technical evaluation establishing the extent to which ORGANIZATION_NAME's security policies and procedures meet the requirements of impacted regulations.
34	***Business Associate Agreements and Other Arrangements Procedure*** HIPAA Reference §164.308 (b)(1)	To obtain satisfactory assurances the Business Associate will appropriately safeguard all sensitive information in accordance with applicable regulations.
35	***Facility Access Controls Procedure*** HIPAA Reference §164.310 (a)(1)	To implement policies and procedures to limit physical access to ORGANIZATION_NAME's electronic information systems and the facility or facilities in which they are housed, while ensuring properly authorized access is allowed.
36	**Contingency Operations Procedure** HIPAA Reference §164.310 (a)(2)(i)	To establish and implement as needed procedures allowing facility access in support of restoration of lost data under the Disaster Recovery Plan and Emergency Mode Operations Plan in the event of an emergency.

#	Policy Name	Policy Description
	Information Security Procedures	
37	**Facility Security Plan Procedure** HIPAA Reference §164.310 (a)(2)(ii)	To implement policies and procedures to safeguard the facility and equipment from unauthorized physical access, tampering, and theft.
38	**Access Control and Validation Procedures** HIPAA Reference §164.310 (a)(2)(iii)	To establish procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control access to software programs for testing and revision. Also, to ensure workforce members are able to access only the information appropriate and required for their position.
39	**Maintenance Records Procedure** HIPAA Reference §164.310 (a)(2)(iv)	To implement policies and procedures to document repairs and modifications to the physical components of a facility related to security (for example, hardware, walls, doors, and locks).
40	***Workstation Use* Procedure** HIPAA Reference §164.310 (b)	To 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 sensitive information.
41	***Workstation Security* Procedure** HIPAA Reference §164.310 (c)	To implement physical safeguards for all workstations accessing sensitive information and to restrict access to authorized users.
42	**Device and Media Controls Procedure** HIPAA Reference §164.310 (d)(1)	To implement policies and procedures that govern the receipt and removal of hardware and electronic media containing sensitive information in and out of a facility, and their movement within a facility.
43	**Disposal Procedure** HIPAA Reference §164.310 (d)(2)(i)	To implement policies and procedures to address the final disposition of sensitive information and/or the hardware or electronic media on which it is stored.

#	Policy Name	Policy Description
	Information Security Procedures	
44	**Media Re-Use Procedure** HIPAA Reference §164.310 (d)(2)(ii)	To implement procedures for removal of sensitive information from electronic media before being made available for re-use.
45	**Accountability Procedure** HIPAA Reference §164.310 (d)(2)(iii)	To maintain a record of the movements of hardware and electronic media and any person responsible for that movement.
46	**Data Backup and Storage Procedure** HIPAA Reference §164.310 (d)(2)(iv)	To create a retrievable, exact copy of sensitive information, when needed, prior to the movement of equipment.
47	***Access Control Procedure*** HIPAA Reference §164.312 (a)(1)	To implement technical policies and procedures for electronic information systems maintaining sensitive information to allow access only to those persons or software programs that have been granted access rights as specified by regulation or business process.
48	**Unique User Identification Procedure** HIPAA Reference §164.312 (a)(2)(i)	To assign a unique name and/or number for identifying and tracking user identity.
49	**Emergency Access Procedure** HIPAA Reference §164.312 (a)(2)(ii)	To establish and implement authorized access to sensitive information during an emergency, as necessary.
50	**Automatic Logoff Procedure** HIPAA Reference §164.312 (a)(2)(iii)	To implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

#	Policy Name	Policy Description
	Information Security Procedures	
51	**Encryption and Decryption Procedure** HIPAA Reference §164.312 (a)(2)(iv)	To implement a mechanism to encrypt and decrypt sensitive information. The Encryption and Decryption Procedure is intended to assist workforce members in making a decision about the use of encryption technologies as a method of protecting data stored on systems that process sensitive information.
52	***Audit Controls Procedure*** HIPAA Reference §164.312 (b)	To implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems containing or using sensitive information.
53	***Integrity Procedure*** HIPAA Reference §164.312 (c)(1)	To implement policies and procedures to protect sensitive information from improper alteration or destruction.
54	**Mechanism to Authenticate Sensitive Information Procedure** HIPAA Reference §164.312 (c)(2)	To implement electronic mechanisms to document sensitive information has not been altered or destroyed in any unauthorized manner.
55	***Person or Entity Authentication Procedure*** HIPAA Reference §164.312 (d)	To implement procedures to verify the person or entity seeking access to sensitive information is the one claimed.
56	***Transmission Security Procedure*** HIPAA Reference §164.312 (e)(1)	To implement technical security measures to guard against unauthorized access to sensitive information being transmitted over an electronic communications network.
57	**Integrity Controls Procedure** HIPAA Reference §164.312 (e)(2)(i)	To implement security measures to ensure electronically transmitted sensitive information is not improperly modified without detection until disposed of.

#	Policy Name	Policy Description
	Information Security Procedures	
58	**Encryption Procedure** HIPAA Reference §164.312 (e)(2)(ii)	To implement a mechanism to encrypt sensitive information in transit whenever deemed appropriate.
59	***Policies and Procedures Standard Procedure*** HIPAA Reference §164.316 (a)	To implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, and other requirements of impacted regulations.
60	***Documentation Standard Procedure*** HIPAA Reference §164.316 (b)(1)	To maintain the policies and procedures implemented to comply with the impacted regulation in written (or electronic) form and if an action, activity or assessment is required to maintain a written (which may be electronic) record of that action, activity or assessment.
61	**Information Classification Procedure** HIPAA Reference §164.308 (a)(1)(ii)(B)	To address information classification categories, acceptable access, and use of information such as ePHI and other sensitive information.
62	**Network Security Procedure** HIPAA Reference §164.308 (a)(1)(ii)(B)	To establish standards for secure communication devices and data on equipment owned and/or operated by ORGANIZATION_NAME. By securing ORGANIZATION_NAME's network and infrastructure, ORGANIZATION_NAME will minimize unauthorized access to the organization's proprietary information and technology.
63	**Email Security Procedure** HIPAA Reference §164.312 (e)(1)	To protect the confidentiality and integrity of sensitive information which may be sent or received via email.
64	**Remote Access Procedure** HIPAA Reference §164.308 (a)(1)(i)	To implement security measures sufficient to reduce risks and vulnerabilities of remote access connections to ORGANIZATION_NAME's enterprise infrastructure to a reasonable and appropriate level.

#	Policy Name	Policy Description
	Information Security Procedures	
65	**VPN Procedure** HIPAA Reference §164.312 (a)(1)	To implement security measures sufficient to reduce the risks and vulnerabilities of ORGANIZATION_NAME's VPN infrastructure to a reasonable and appropriate level.
66	**Wireless Security Procedure** HIPAA Reference §164.312 (e)(2)(ii)	To implement security measures sufficient to reduce risks and vulnerabilities of ORGANIZATION_NAME's wireless infrastructure to a reasonable and appropriate level.
67	**Wireless IP Phone Procedure** HIPAA Reference §164.312 (e)(2)(ii)	To implement security measures sufficient to reduce risks and vulnerabilities of ORGANIZATION_NAME's wireless IP phones to a reasonable and appropriate level.
68	**Bring Your Own Device (BYOD) Procedure** HIPAA Reference §164.310 (d)(1)	To address the rights and obligations of both owners of a device used for ORGANIZATION_NAME work and ORGANIZATION_NAME's rights and obligations to protect and own its data on these devices.
69	**Biomedical Device Security Procedure** HIPAA Reference §164.310 (d)(1)	To provide reasonable and appropriate safeguards to ensure the confidentiality, integrity, and availability (CIA) of biomedical devices connected to the network infrastructure.
70	**Data Breach Notification Procedure** HIPAA Reference §164.404 (a)	To comply with the HIPAA Administrative Simplification Requirements Subpart B (Notification in the Case of Breach of Unsecured Protected Health Information) and with additional state regulation(s), as applicable, with respect to unsecured Protected Health Information (PHI), Personal Identifiable Information (PII), or other confidential information, and to provide methods and content of notification.

#	Policy Name	Policy Description
	Information Security Procedures	
71	**Social Media Procedure** HIPAA Reference §164.308 (a)(5)(i)	To ensure workforce members who use social media, either as part of their job or in a personal capacity, understand the organization's expectations for social media engagements concerning ORGANIZATION_NAME, its services, staff, patients, competitors, vendors, and/or business-related individuals or organizations.
72	**Mobile Devices Procedure** HIPAA Reference §164.310 (d)(1)	To address the appropriate protection of sensitive electronic information (SEI) when it is stored, transferred or accessed on mobile devices such as: Laptops / Smart Phones (devices with operating systems) or removable media such as: USB Flash drives / Memory cards / Floppy Disks / CDs / DVDs. This procedure is not intended to address non-classified data.
73	**Secure Text Message Procedure** HIPAA Reference §164.312 (e)(1)	To ensure the risk associated with text messaging sensitive information in a clinical setting is managed appropriately to safeguard both the privacy and security of the information exchanged. Under the HIPAA Security Rule (164.308 (a) (1) (ii) (A) and (B)), text messaging is addressed as part of ORGANIZATION_NAME's comprehensive risk analysis and management strategy.
74	**Firewall Procedure** HIPAA Reference §164.308 (a)(1)(ii)(B)	To ensure ORGANIZATION_NAME establishes configuration standards, installs and maintains firewall configurations, and restricts connections between untrusted networks and networks/systems containing, or providing access to, sensitive information.
75	**Patch Management Procedure** HIPAA Reference §164.308 (a)(1)(ii)(B)	To ensure the security of ORGANIZATION_NAME member data by installing security patches in timely fashion. To accomplish this, ORGANIZATION_NAME will utilize comprehensive patch management solutions to identify missing patches and distribute security patches automatically wherever possible.

#	Policy Name	Policy Description
	Information Security Procedures	
76	**Baseline Configuration Procedure** HIPAA Reference §164.308 (a)(1)(ii)(B)	To ensure systems are securely configured and deployed in a repeatable manner that addresses the confidentiality, integrity, and availability of sensitive information that may be stored, processed, or transmitted by such systems. ORGANIZATION_NAME establishes baseline configurations for systems based on identified best practice and vendor recommendations, including standards created by the National Institute of Standards and Technology (NIST), International Organization for Standardization (ISO), and the Center for Internet Security (CIS).
77	**Data & Hardware Acquisition Procedure** HIPAA Reference § 164.310 (d)(2)(iii) SPEC	To ensure that resources are used as effectively as possible and that data security standards are protecting ORGANIZATION_NAME data, all acquisitions of technology hardware, on-site software, software as a service (SAAS or "cloud") or consulting contracts.
78	**Isolating Health Care Clearinghouse Procedure** HIPAA Reference §164.308 (a)(4)(ii)(A)	The purpose is to describe how clearinghouse functions are isolated so that Electronic Protected Health Information (ePHI) in the clearinghouse is separated from other functions ORGANIZATION_NAME performs.
79	**Acceptable Use Procedure** HIPAA Reference §164.310 (b)	To outline the acceptable use of computer equipment at ORGANIZATION_NAME. These rules are in place to protect the workforce member and ORGANIZATION_NAME. Inappropriate use exposes ORGANIZATION_NAME to risks including virus attacks, compromise of network systems and services, and legal issues.

4 CAP Remediation

Objective: CAP Remediation addresses tasks such as:

1. Implement intrusion detection/prevention systems.
2. Secure facilities and server systems.
3. Implement device and media control solutions.
4. Implement authentication solutions.
5. Deploy access control technology.
6. Implement automatic logoff.
7. Activate log-in monitoring and auditing capabilities.
8. Deploy integrity control and encryption technology.
9. Test contingency planning procedures.

Remediation is the step where policies are implemented, and configuration is consistent and based on procedures created. It is in this step that initiatives are launched to "close and lock" the gaps and risks that were identified in Step 2. The objective is two-fold; first, to meet and exceed HIPAA requirements and second, to protect all enterprise assets and communications. It is in this step that pilots are launched, and technologies are deployed.

Organizations must implement security controls that provide for near real time discovery of incidents, as well as other capabilities. Only if security violations are detected on a timely basis can the organization respond with safeguards in the future.

Next, organizations must implement physical security measures to secure facilities and server systems. Both site security and secure access to only authorized personnel must be addressed.

Furthermore, entities must implement solutions for disposal of information, media re-use, accountability, data backup and storage. These solutions must be based on associated policies and procedures. HIPAA contains specific requirements for retaining documents – six years from the date of its creation or the date when it was last in effect, whichever is later.

All organizations must implement person and entity authentication solutions to uniquely identify access to vital enterprise systems and information. For example, organizations may struggle with password management or extensive use of generic logins. Organizations may consider strong authentication solutions such as biometrics, smart cards or authentication tokens.

5 Cybersecurity Supply Chain

Objective: Cybersecurity Supply Chain includes the following activity:

1. To review BA Cyber Supply Chain with all entities, such as business associates, cloud providers or other organizations that access ePHI.

This step results in organizations updating Business Associate Agreements (BAA) or Business Associate Contracts (BACs) to address safeguards, training, and audit requirements for third party vendors such as cloud service providers or other BAs.

Note that all organizations that electronically exchange information with the entity must enter into a contract or other arrangement with persons or entities that meet the definition of a business associate.

The covered entity must obtain satisfactory assurances from the business associate that it will appropriately safeguard the information in accordance with HIPAA requirements.

Prudent organizations will implement periodic audits and "scans" to verify that the agreements are implemented effectively and remain viable. Because the health services industry is characterized by change, your organization's compliance and cybersecurity depends upon effective positive verifications that each and every business partner contract or agreement remains in force.

Business Associate Contracts and Other Arrangement is a HIPAA Security Rule Standard defined within the Administrative Safeguards section (164.308 (b) (1)).

6 Workforce Education

Objective: Workforce Education includes the following activities:

1. To train all members of the workforce on HIPAA mandates.
2. To consistently communicate security requirements among the workforce with security reminders, updates on malicious software, and password management.
3. Regularly perform social engineering exercises to mitigate risk such as phishing and ransomware attacks.

Security is only as strong as the weakest link in the enterprise. Typically, in most organizations, employees are the weakest link. All members of the workforce – and this includes all employees, volunteers as well as management – must be knowledgeable about HIPAA security requirements, the threats the organization may be vulnerable to, and the security policies of the entity.

The objective of the HIPAA Security Rule's Security Awareness and Training standard is to implement a security awareness and training program for all members of its workforce, including management. The implementation specifications for security awareness and training include:

- Security reminders (Addressable)
- Protection from malicious software (Addressable)
- Log-in monitoring (Addressable)
- Password management (Addressable)

7 Active Monitoring

Objective: Active Monitoring includes the following activities:

1. Assess status of compliance gaps and security vulnerabilities.
2. Establish priorities to mitigate risk based on evidence from systems and applications.

The Risk Management standard requires that organizations on a regular basis identify, select, and implement controls, countermeasures, reporting and verification to achieve an appropriate level of risk at an acceptable cost. An active risk management program is vital for credible HIPAA compliance.

Organizations must also repeat the process of identification of all vulnerabilities to ePHI as well as other information assets and determine appropriate security measures to reduce risks to a reasonable and appropriate level.

All organizations should go beyond just meeting HIPAA compliance requirements. The compliance requirements are limited to ePHI. Organizations must evaluate their security requirements for not just all PHI, but all information assets, including cloud, mobile, IoT and others.

The objective of the Evaluation standard within the HIPAA Security Rule is to perform a periodic technical and non-technical evaluation. The evaluation is based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of ePHI, which establishes the extent to which an entity's security policies and procedures meet the requirements defined.

HIPAA requires that organizations periodically conduct an evaluation of their safeguards to demonstrate and document their compliance with the entity's compliance program.

HIPAA & HITECH

ecfirst | HIPAA Academy

ecfirst was the first organization in the United States to deliver HIPAA training, consulting and certification services. The HIPAA Academy is the gold standard in the healthcare industry. ecfirst "*delivers everything HIPAA*". Talk to ecfirst and discuss your HIPAA and HITECH compliance challenges and requirements. ecfirst will create a tailored solution for your organization. Ask about the ecfirst Managed Compliance Program to maintain your HIPAA compliance program.

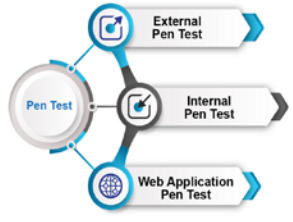
- Perform a comprehensive and thorough HIPAA Risk Assessment.
- Conduct a Cybersecurity Assessment to identify gaps.
- Develop tailored suite of policies and procedures.
- Deliver certification training providing in-depth coverage of HIPAA.
- Remediate cybersecurity and compliance gaps.
- Create customized incident response, cybersecurity, and disaster recovery plans.

HIPAA Compliance Lifecycle

HIPAA Services

- HIPAA Policy Readiness
- HIPAA Procedure Readiness
- HIPAA Evidence Readiness
- HIPAA Professional Consultants
- HIPAA Risk Assessment
- HIPAA Remediation
- HIPAA Cybersecurity Assessment

Trust ecfirst with HIPAA



CHP Certified HIPAA Professional — HIPAA Academy

The industry's first and most comprehensive HIPAA training and certification program.

- Analyze the latest updates in HIPAA Privacy, HIPAA Security and HITECH Breach mandates.
- Examine OCR HIPAA settlements to understand the bar for HIPAA compliance.
- Review HIPAA compliance challenges and best practices for covered entities and business associates.

ecfirst | HIPAA Academy

Ali Pabrai

Global Cyber Defense Thought Leader

MSEE | CISSP (ISSAP | ISSMP) | CMMC (PA, PI, RP) | HITRUST CCSFP | Security+

TOP-RATED SPEAKER

Mr. Ali Pabrai, a global cybersecurity & compliance expert, is the chairman & chief executive of ecfirst. A highly sought after professional, he has successfully delivered solutions to U.S. government agencies, IT firms, healthcare systems, legal & other organizations worldwide. His career was launched with the U.S. Department of Energy's nuclear research facility, Fermi National Accelerator Laboratory. He has served as vice chairman and in several senior officer positions with NASDAQ-based firms.

Mr. Pabrai has led numerous engagements worldwide for ISO 27001, PCI DSS, NIST, CMMC, GDPR, CCPA, FERPA, HITRUST CSF and HIPAA/HITECH. Mr. Pabrai served as an Interim CISO for a health system with 40+ locations.

U.S. Department of Defense CMMC Program

Mr. Pabrai has presented passionate briefs to tens of thousands globally, including the USA, United Kingdom, France, Taiwan, Singapore, Canada, India, UAE, Saudi Arabia, Philippines, Japan, Ireland, Bahrain, Jordan, South Africa, Egypt, Ghana and other countries.

He is a globally renowned speaker who has been featured as a keynote as well as moderated cybersecurity conferences. Mr. Pabrai is the author of several published works. Clients that Mr. Pabrai has delivered to have included the U.S. Defense Intelligence Agency (DIA), and the U.S. Naval Surface Warfare Center.

Mr. Pabrai was appointed and served (2017) as a member of the select HITRUST CSF Assessor Council. Mr. Pabrai is a proud member of the InfraGard (FBI).

"We have had the true pleasure of working with Ali Pabrai at conferences all over the world during the past few years – with one unanimous word that keeps resounding among audiences and staff alike – *AWESOME!*"
Michael Mach | *Conference Program Manager* | *ISACA*

ISACA

FBI Conference

"Pabrai's presentation style is engaging, and he encourages questions and discussions. I would recommend him for future presentations and trainings."
Josh More | *Cyber Sector Chief* | *Iowa FBI InfraGard*

"On behalf of the Idaho InfraGard (FBI), I would like to thank Pabrai for presenting at our conference. Pabrai is the kind of speaker you want to bring to executives and staff. He says it in a simple, no nonsense way, in a manner that everyone can understand."
Rachel Zahn | *President* | *InfraGard (FBI)* | *Idaho Alliance*

"You delivered a fantastic presentation and we all felt your passion for cyber security."
James E Lamadrid | *Supervisory Special Agent* | *Federal Bureau of Investigation (FBI)* | *Cyber Task Force*

"Thank you Pabrai. Your enthusiasm and relevance for the Information Security material you presented at our combined Infragard (FBI) conference in Idaho Falls was very well received and pertinent to both our chapter as an organization and the constituents in attendance."

"As a government employee, I appreciated the simplified insight of highlighting the importance of compliance and funding compared to information security success beyond qualitative metrics. I heard many times over that your specific information with measurable results made your material directly relevant to individuals, businesses and organizations. Thanks again and I hope you are able to join us again in the future."
Clark Harshbarger | *FBI*

Author


Getting Started with HIPAA — First published book on HIPAA


UNIX Internetworking — First book on UNIX & Networks


Internet & TCP/IP Network Security — First book on TCP/IP security

HITRUST®
Authorized External Assessor