eSENTIRE

CHECKLIST

HIPAA Security Compliance Checklist

Meeting HIPAA Security compliance for electronic protected health information (ePHI) while mitigating risk from an evolving threat landscape with constrained resources can be challenging. At eSentire, we work with healthcare delivery organizations ranging from individual practices to major hospitals and their business associates to ensure they have the systems, processes, and controls in place to protect their practice, patient data, and most importantly, critical operations.

In this document, we've mapped the HIPAA Security Standards, both required and addressable, to eSentire's service portfolio to demonstrate how we can support you in adhering to compliance requirements through our 24/7 cybersecurity services.

HIPAA Security Standards	Sections	Implementation Specifications (R)=Required, (A)=Addressable	Explanation	eSentire Services
Administrative Safeguards				
Security Management Process	164.308(a)(1)(ii)(A)	Risk Analysis (R)	Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.	eSentire Managed Risk Programs ✔ Managed Vulnerability Service ✔ vCISO ✔ External Penetration Test
	164.308(a)(1)(ii)(B)	Risk Management (R)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).	eSentire Managed Risk Programs ✔ vCISO ✔ Managed Phishing and Security Awareness Training OR eSentire Managed Detection and Response (MDR)
	164.308(a)(1)(ii)(C)	Sanction Policy (R)	Apply appropriate sanctions against workforce members who fail to comply with the securitypolicies and procedures of the covered entity or business associate.	eSentire Managed Risk Program
	164.308(a)(1)(ii)(D)	Information System Activity Review (R)	Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.	eSentire MDR
Assigned Security Responsibility	164.308(a)(2)	(R)	Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate.	eSentire Managed Risk Programs ✔ vCISO

HIPAA Security Standards	Sections	Implementation Specifications (R)=Required, (A)=Addressable	Explanation	eSentire Services
Workforce Security	164.308(a)(3)(ii)(A)	Authorization and/or Supervision (A)	Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.	eSentire Managed Risk Programs ✔ vCISO
	164.308(a)(3)(ii)(B)	Workforce Clearance Procedure (A)	Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.	eSentire Managed Risk Programs ✔ vCISO
	164.308(a)(3)(ii)(C)	Termination Procedures (A)	Implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.	eSentire Managed Risk Programs ✔ vCISO OR eSentire MDR
Information Access Management	164.308(a)(4)(ii)(A)	Isolating Healthcare Clearinghouse Function (R)	Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the coveredentity or business associate.	eSentire Managed Risk Programs ✔ vCISO
	164.308(a)(4)(ii)(B)	Access Authorization (A)	Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.	eSentire Managed Risk Programs ✔ vCISO OR eSentire MDR
	164.308(a)(4)(ii)(C)	Access Establishment and Modification (A)	Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.	eSentire Managed Risk Programs ✔ vCISO OR eSentire MDR
Security Awareness and Training	164.308(a)(5)(ii)(A)	Security Reminders (A)	Periodic security updates.	eSentire Managed Risk Programs ✔ Managed Phishing and Security Awareness Training ✔ vCISO executive support in proactive cyber roadmap development
	164.308(a)(5)(ii)(B)	Protection from Malicious Software (A)	Procedures for guarding against, detecting, and reporting malicious software.	
	164.308(a)(5)(ii)(C)	Log-in Monitoring (A)	Procedures for monitoring log-in attempts and reporting discrepancies.	
	164.308(a)(6)(ii)(D)	Password Management (A)	Procedures for creating, changing, and safeguarding passwords.	
Security Incident Procedures	164.308(a)(6) (ii)	Response and Reporting (R)	Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.	eSentire MDR OR Digital Forensics and Incident Response
Contingency Plan	164.308(a)(7)(ii)(A)	Data Backup Plan (R)	Establish and implement procedures to create and maintain retrievable exact copies of electronic protectedhealth information.	eSentire MDR OR Digital Forensics and Incident Response
	164.308(a)(7)(ii)(B)	Disaster Recovery Plan (R)	Establish (and implement as needed) procedures to restore any loss of data.	
	164.308(a)(7)(ii)(C)	Emergency Mode Operation Plan (R)	Establish procedures to enable continuation of critical business processes for protection of the security of ePHI while operating in emergency mode.	
	164.308(a)(7)(ii)(D)	Testing and Revision Procedure (A)	Implement procedures for periodic testing and revision of contingency plans.	
	164.308(a)(7)(ii)(E)	Applications and Data Criticality Analysis (A)	Assess the relative criticality of specific applications and data in support of other contingency plan components.	

HIPAA Security Standards	Sections	Implementation Specifications (R)=Required, (A)=Addressable	Explanation	eSentire Services
Evaluation	164.308(a)(8)	(R)	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, that establishes the extent to which a covered entity's or business associate's security policies and procedures meet the requirements of this subpart.	eSentire MDR OR Digital Forensics and Incident Response
Business Associate Contracts and Other Arrangement	164.308(b)(4)	Written Contract or Other Arrangement (R)	Document the satisfactory assurances required by paragraph (b)(1) or (b)(2) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of § 164.314(a).	eSentire Managed Risk Programs ✔ Adherence to compliance requirements ✔ Third party risk security assessments ✔ Compromise assessment services
Technnical Safeguards				
Access Control	164.312(a)(2)(i)	Unique User Identification (R)	Assign a unique name and/or number for identifying and tracking user identity.	eSentire Managed Risk Programs OR eSentire MDR
	164.312(a)(2)(ii)	Emergency Access Procedure (R)	Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.	
	164.312(a)(2)(iii)	Automatic Logoff (A)	Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.	
	164.312(a)(2)(iv)	Encryption and Decryption (A)	Implement a mechanism to encrypt and decrypt electronic protected health information.	
Audit Controls	164.312(b)	(R)	Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	eSentire Managed Risk Programs OR eSentire MDR
Integrity	164.312(c)(2)	Mechanism to Authenticate Electronic Protected Health Information (A)	Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.	eSentire Managed Risk Programs OR eSentire MDR
Person or Entity Authentication	164.312(d)	(R)	Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.	eSentire Managed Risk Programs OR eSentire MDR
Transmission Security	164.312(e)(2)(i)	Integrity Controls (A)	Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.	eSentire Managed Risk Programs OR eSentire MDR
	164.312(e)(2)(ii)	Encryption (A)	Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.	

How eSentire can help

We are recognized globally as the Authority in Managed Detection and Response because we hunt, investigate, and stop known and unknown cyber threats before they become business disrupting events. We were founded in 2001 to secure the environments of the world's most targeted industry - financial services. Over the last two decades we have scaled our cybersecurity services offering to hunt and disrupt threats across every industry on a global scale. With two 24/7 Security Operations Centers (SOCs), hundreds of cyber experts, and 1000+ customers across 70+ countries, we have scaled to deliver cybersecurity services across highly regulated industries with a proven track record of success in securing businesses across the healthcare sector including healthcare institutions, medical technology providers, and pharmaceutical companies.

At eSentire, we go beyond the market's capability in threat response and specifically address cybersecurity risks for the manufacturing sector. eSentire's multi-signal MDR approach ingests endpoint, network, log, cloud, asset and vulnerability data that enables complete attack surface visibility. Enriched detections from the eSentire Threat Response Unit are applied to captured data identifying known & unknown threats including suspicious activity and zero-day attacks. With two 24/7 Security Operations Centers staffed with cyber experts and Elite Threat Hunters, an industry-leading XDR Cloud Platform, and refined security operations processes, eSentire can detect and respond to cybersecurity threats in the manufacturing industry with a Mean Time to Contain of 15 minutes.

At eSentire, We Support Healthcare Delivery Organizations By:

- Supporting patient care with secure services including 24/7 threat detection, investigation and complete response
- Protecting and preventing healthcare organizations from operational disruption caused by ransomware gangs and state-sponsored actors
- Securing patients' electronic protected health information (ePHI)
- Mitigating third-party risk
- Ensuring you and your business associates meet HIPAA compliance requirements

We recognize that there is no end to cyber risk. Preventative technologies will be bypassed, and defenses will fail. That's why we prioritize Response by delivering MDR[3] - Response, Remediation and Results. Our cybersecurity services include:

Managed Risk and Vulnerability: Strategic services including Vulnerability Management and Managed Phishing and Security Awareness Training to identify gaps, build defensive strategies, operationalize risk mitigation, and continuously advance your cybersecurity program.

Managed Detection and Response: We deliver complete and robust Response by combining cutting-edge machine learning XDR, 24/7 threat hunting expertise and security operations leadership. We hunt and disrupt known & unknown threats before they impact your healthcare operations and patients.

Digital Forensics and Incident Response: Battle-tested Incident Commander-level expertise driving incident response, remediation, recovery, and root cause analysis. Our On Demand 24/7 Incident Response retainers include Emergency Incident Response, Security Incident Response Planning Services and an industry-leading 4-hour Threat Suppression SLA.

Learn how we can help defend your organization with advanced detection, 24/7 threat hunting, deep investigation, and end-to-end coverage that protects your organization and patients.

Reach out to connect with an eSentire security specialist.

Get Started

If you're experiencing a security incident or breach contact us **1-866-579-2200**

eSENTIRE