gemalto
security to be free

HIPAA Compliance Checklist

Hospitals, clinics, and any other health care providers that manage private health information today must adhere to strict policies for ensuring that data is secure at all times. These organizations can face steep penalties if this data is stolen or compromised. Gemalto can help address many of the critical security challenges of keeping private health information private and secure.

The Health Insurance Portability and Accountability Act (HIPAA) regulates the use and disclosure of certain information held by health plans, health insurers, and medical service providers that engage in many types of transactions. Gemalto can help address many of the critical challenges of ensuring the security of sensitive data adhering to health information privacy standards.

In the pages that follow, we provide some specific guidance from the HIPAA standard, and illustrate how Gemalto can help address these specific mandates.

Regulation	Best Practice	Sample Questions
§ 164.308 (a)(1) Security Management Process: Implement policies and procedures to prevent, detect, contain, and correct security violations.	**Identity Relevant Information Systems** > Identify all information systems that house ePHI > Analyze business functions and verify ownership and control of information systems.	1. Does the hardware and software include removable media and remote access devices? 2. Have the types of information and uses of that information been identified and the sensitivity of each type of information been evaluated?
Gemalto Solutions > Two-Factor Authentication > Application Encryption > Database Encryption > File Encryption > Instance and Virtual Machine Encryption > Network Encryption > Key Management > Hardware Security Modules	**Conduct Risk Assessment** > Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI.	1. Is the facility located in a region prone to any natural disasters? 2. Has responsibility been assigned to check all hardware? 3. Is there an analysis of current safeguards and identifiable risks? 4. Have all processes involving ePHI been considered, including creating, receiving, maintaining, and transmitting?
	Acquire IT Systems and Services > Additional hardware, software or services may be needed to adequately protect information. Should consider the sensitivity of the data, security policies, and IT environment.	1. Will new security controls work with the existing IT architecture? 2. Has a cost-benefit analysis been conducted to determine the reasonableness of the investment given the security risks identified?
	Create and Deploy Policies and Procedures > Create policies that clearly establish roles and responsibilities and assign ultimate responsibility for the implementation of each control to particular individuals or offices.	1. Is there a formal system security and contingency plan?

Regulation	Best Practice	Sample Questions
§ 164.308 (a)(3) Workforce Security: Implement policies and procedures to ensure that all members of its workforce have appropriate access to ePHI, and prevent those workforce members who do not have access from obtaining access to ePHI. **Gemalto Solutions** > Two-Factor Authentication > Key Management > Hardware Security Modules	**Implement Procedures for Authorization and Supervision** > Implement procedures for the authorization and supervision of workforce members who work with ePHI or locations where it might be accessed.	1. Have lines of authority been established? 2. Does workforce know of the identity and roles of their supervisors?
	Establish Clear Job Descriptions and Responsibilities > Define roles and responsibilities for all job functions. > Assign appropriate levels of security oversight and access.	1. Are there written descriptions correlated with levels of access?
	Establish Termination Procedures > Implement procedures for terminating access to ePHI when the employment of a workforce member ends. > Deactivate computer access accounts.	1. Will new security controls work with the existing IT architecture? 2. Has a cost-benefit analysis been conducted to determine the reasonableness of the investment given the security risks identified?
§ 164.308 (a)(4) Information Access Management: Implement policies and procedures for authorizing access to ePHI that are consistent with the applicable requirements. **Gemalto Solutions** > Two-Factor Authentication > Application Encryption > Database Encryption > File Encryption > Instance and Virtual Machine Encryption > Key Management > Hardware Security Modules	**Implement Policies and Procedures for Authorizing Access** > Implement policies and procedures for granting access through workstations, programs, transactions, etc. > Decide how access will be granted to workforce. > Select the basis for restricting access. > Select access control method (identity-based, role-based). > If full disk encryption is used, add an additional layer of protection with two-factor authentication.	1. Do the organizations IT systems have the capacity to set access controls? 2. Does the organization grant remote access to ePHI? 3. What method of access controls are used?
	Implement Policies and Procedures for Access Establishment and Modification > Establish standards for granting access.	1. Are duties separated such that only the minimum necessary ePHI is made available to each staff members based on job requirements?
	Evaluate Existing Security Measures Related to Access Controls > Evaluate the security features of access controls already in place, or those of any planned for implementation > Determine if these security features involve alignment with existing controls and policies.	1. Are authentication mechanisms used to verify the identity of those accessing systems protected from inappropriate manipulation? 2. Does management regularly review the list of access authorizations, including remote access authorizations?

Regulation	Best Practice	Sample Questions
§ 164.308 (a)(7) Contingency Plan: Establish policies and procedures for responding to an emergency or other occurrence that damages systems that contain ePHI.	**Develop Contingency Planning Policy** > Define the organization's overall contingency objectives.	1. What critical services must be provided within specified time frames? 2. Have cross-functional dependencies been identified so as to determine how the failure in one system may negatively impact another one?
Gemalto Solutions > Two-Factor Authentication > Application Encryption > Database Encryption > File Encryption > Instance and Virtual Machine Encryption > Key Management > Hardware Security Modules > High Speed Encryption	**Conduct an Applications and Data Criticality Analysis** > Identify the activities and material involving ePHI that are critical to business operations. > Identify the critical services or operations, and the manual and automated processes that support them.	1. What hardware are critical to daily operations? 2. What is the impact on desired service levels? 3. What is the nature and degree of impact on the operation if any of the critical resources are not available?
	Identify Preventative Measures > Identify preventative measures for each defined scenario that could result in loss of critical service operation involving the use of ePHI.	1. What alternatives for continuing operations of the organization are available in case of loss of any critical functions?
	Develop Recovery Strategy > Finalize the set of contingency procedures that should be invoked for all identified impacts, including emergency mode operation.	1. Have procedures related to recovery for emergency or disastrous events been documented?
	Data Backup Plan and Disaster Recovery Plan > Establish and implement procedures to create and maintain retrievable exact copies of ePHI, and ensure that backup copies and systems are encrypted.	1. Do data backup procedures exist?
§ 164.310 (a)(1) Facility Access Controls: 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.	**Develop a Facility Security Plan** > Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized access. > Implement appropriate measures to provide physical security protection for ePHI. > Identify points of access to the facility and existing security controls.	1. What are the current procedures for security facilities? 2. Is a workforce member other than the security official responsible for the facility plan?
Gemalto Solutions > Two-Factor Authentication > Hardware Security Modules	**Develop Access Control and Validation Procedures** > Implement procedures to control and validate a persons access to facilities based on their role or function.	1. What are the policies and procedures in place for controlling access by staff, employees, etc? 2. What are the access points in each facility?
	Establish Contingency Operations Procedures > Establish procedures that allow facility access in support of restoration of lost data.	1. Who needs access to ePHI in the vent of a disaster? 2. Who Is responsible for the contingency plan?

Regulation	Best Practice	Sample Questions
§ 164.310 (c)(1) Workstation Security: Implement physical safeguards for all workstations that access ePHI, to restrict access to authorized users. **Gemalto Solutions** > Two-Factor Authentication > Key Management > Hardware Security Modules	**Identify All Methods of Physical Access to Workstations** > Document the different ways workstations are accessed by employees and non-employees.	1. Are laptops used as workstations?
	Identify and Implement Physical Safeguards for Workstations > Implement physical safeguards and other security measures to minimize the possibility of inappropriate access to ePHI through workstations. > If full disk encryption is used, add an additional layer of protection with two-factor authentication.	1. What safeguards are in place for the workstation areas?
§ 164.310 (d)(1) Device and Media Controls: Implement policies and procedures that govern the receipt and removal of hardware and e-media that contain ePHI into and out of a facility. **Gemalto Solutions** > Two-Factor Authentication > Key Management > High Speed Encryption	**Implement Methods for Final Disposal of ePHI** > Implement policies and procedures to address the final disposition of ePHI and the hardware and e-media on which it is stored.	1. What data is maintained and where? 2. Is the data removable?
§ 164.312 (a)(1) Access Control: Implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights as specified. **Gemalto Solutions** > Two-Factor Authentication > Key Management > Hardware Security Modules	**Analyze Workloads and Operations to Identify the Access Needs of All Users** > Identify an approach for access control. > Consider all applications and systems containing ePHI that should be available only to authorized users.	1. Have all applications/systems been identified? 2. What user roles are defined? 3. Are data and systems being accessed remotely?
	Identify Technical Access Control Capabilities > Determine the access control capability of all information systems with ePHI.	1. How are the systems accessed (viewing data, modifying data, creating data)?
	Develop Access Control Policy > Establish a formal policy for access control that will guide the development of procedures.	1. Have rules of behavior been established?

Regulation	Best Practice	Sample Questions
§ 164.312 (a)(1)... Access Control: Implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights as specified.	**Ensure that All System Users Have Been Assigned a Unique Identifier** > Assign a unique name and number for identifying and tracking user identity. > Ensure that system activity can be traced to a specific user. > Ensure that the necessary data is available in the system logs to support audit and other related functions.	1. How should the identifier be established? 2. Should the identifier be self-selected or randomly generated?
Gemalto Solutions > Two-Factor Authentication > Key Management > Hardware Security Modules	**Implement Access Control Procedures Using Selected Hardware** > Implement the policy and procedures using existing or additional hardware solutions.	1. Who will manage the access control procedures?
	Automatic Logoff and Encryption & Decryption > Consider whether the addressable implementation specifications of this standard are reasonable. > Implement a mechanism to encrypt and decrypt ePHI, including full disk encryption, where applicable.	1. What encryption systems are available for the covered entity's ePHI? 2. Is encryption appropriate for storing and maintaining ePHI, as well as while it is transmitted?
§ 164.312 (c)(1) Integrity: Implement policies and procedures to protect ePHI from improper alteration or destruction.	**Identify All Users Who Have Been Authorized to Access ePHI** > Identify all approved users with the ability to alter or destroy data, if reasonable and appropriate. > Address this key activity in conjunction with identification of unauthorized sources.	1. How are users authorized to access the information? 2. Is there an audit trail?
Gemalto Solutions > Two-Factor Authentication > Application Encryption > Database Encryption > File Encryption > Instance and Virtual Machine Encryption > Key Management > Hardware Security Modules	**Identify Any Possible Unauthorized Sources that May Be Able to Intercept the Information and Modify It** > Identify scenarios that may result in modification to the ePHI by unauthorized sources.	1. Where are likely sources that could jeopardize information integrity? 2. What can be done to protect the integrity of the information when it is residing in a system? 3. What procedures and policies can be established to decrease or eliminate alteration of the information during transmission?
	Implement a Mechanism to Authenticate ePHI > Implement electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner. > Consider possible electronic mechanisms for authentication (i.e. digital signature).	1. Are the uses of both electronic and nonelectronic mechanisms necessary? 2. Are appropriate tools available? 3. Are they interoperable?

Regulation	Best Practice	Sample Questions
§ 164.312 (d) Person or Entity Authentication: Implement procedures to verify that a person or entity seeking access to ePHI is the one claimed.	**Determine Authentication Applicability to Current Systems/Applications** > Identify methods available for authentication. > Authentication requires establishing the validity of a transmissions source and verifying an individual's claim that they are authorized for specific access privileges to information and information systems.	1. What authentication methods are available? 2. What are the advantages and disadvantages of each? 3. What is the cost to implement the available methods in your environment? 4. Do you have trained staff to maintain the systems?
Gemalto Solutions > Two-Factor Authentication > Database Encryption > Key Management > Hardware Security Modules	**Evaluate Authentication Options Available** > There are four commonly used authentication approaches: 1. Password 2. Token 3. Biometric 4. Combination of two or more	1. What are the strengths and weaknesses of each option? 2. Which can be best supported with assigned resources? 3. What level of authentication is appropriate based on your assessment of risk to the information/systems?
§ 164.312 (e)(1) Transmission Security: Implement technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communication network.	**Identify Any Possible Unauthorized Sources that May Be Able to Intercept or Modify the Information** > Identify scenarios that may result in modification of the ePHI by unauthorized sources during transmission.	1. What measures exist to protect ePHI in transmission? 2. Is there an auditing process in place to verify that ePHI has been protected against unauthorized access during transmission?
	Implement Integrity Controls > Implement security measures to ensure that electronically transmitted ePHI is not improperly modified without detection until disposed of.	1. What measures are planned to protect ePHI in transmission? 2. Is there assurance that information is not altered during transmission?
Gemalto Solutions > Two-Factor Authentication > Application Encryption > Database Encryption > File Encryption > Instance and Virtual Machine Encryption > Key Management > Hardware Security Modules > High Speed Encryption	**Implement Encryption** > Implement a mechanism to encrypt ePHI whenever deemed appropriate.	1. Is encryption reasonable and appropriate; is it feasible and cost-effective? 2. What encryption algorithms and mechanisms are available? 3. Does the covered entity of the staff to maintain a process for encrypting ePHI during transmission?

ABOUT GEMALTO'S SAFENET IDENTITY AND DATA PROTECTION SOLUTIONS

Gemalto's portfolio of Identity and Data Protection solutions offers one of the most complete portfolios of enterprise security solutions in the world, enabling its customers to enjoy industry-leading protection of data, digital identities, payments and transactions–from the edge to the core. Gemalto's SafeNet Identity and Data Protection solutions enable enterprises across many verticals, including major financial institutions and governments, to take a data-centric approach to security by utilizing innovative encryption methods, best-in-class crypto management techniques, and strong authentication and identity management solutions to protect what matters, where it matters. Through these solutions, Gemalto helps organizations achieve compliance with stringent data privacy regulations and ensure that sensitive corporate assets, customer information, and digital transactions are safe from exposure and manipulation in order to protect customer trust in an increasingly digital world.

Contact Us: For all office locations and contact information, please visit safenet.gemalto.com

Follow Us: blog.gemalto.com/security

GEMALTO.COM

gemalto
security to be free