HIPAA Information Security Policy Outline

bizSHIELD™

The ecfirst and HIPAA Academy *biz*SHIELD™ security methodology identifies seven critical steps for an organization to implement to establish a secure infrastructure. Step 3 is about the development of security policies and procedures. This document includes information security policy templates that may be licensed for use by organizations to create comprehensive policies for their digital business infrastructure. This document addresses policy compliance requirements and standards including HIPAA and others.

The policy templates in this document can be easily customized to meet the specific requirements of any type of organization.

HIPAA Information Security Policy Outline

Figure 1 provides a brief summary of the objective of each security policy and associated procedures.

Information Security Policy / Procedure	Description
Administrative Safeguards	
Information Security Strategy	The purpose is to provide reasonable and appropriate safeguards to ensure the confidentiality, integrity, and availability (CIA) of information assets by protecting those assets from unauthorized access, modification, destruction, or disclosure.
Security Management Process	The purpose is to implement policies and procedures to prevent, detect, contain, and correct security violations.
Risk Analysis	The purpose is to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of sensitive information.
Risk Management	The purpose is implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with impacted regulations.
Sanction Policy	The purpose is to apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the organization.
Information System Activity Review	The purpose is to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.
Assigned Security Responsibility	The purpose of this policy is to identify the security official who is responsible for the development and implementation of policies and procedures.

Information Security Policy / Procedure	Description
Workforce Security	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 do not have access from obtaining access to sensitive information.
Authorization and/or Supervision	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.
Workforce Clearance Procedure	The purpose is to implement procedures to determine that the access of a workforce member to sensitive information is appropriate.
Termination Procedures	The purpose is to implement procedures for terminating access to sensitive information when the employment of a workforce member ends.
Information Access Management	The purpose is to implement policies and procedures for authorizing access to sensitive information.
Access Authorization	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.
Access Establishment and Modification	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.
Security Awareness and Training	The purpose is to implement a security awareness and training program for all members of its workforce, including management.

Information Security Policy / Procedure	Description
Security Reminders	The purpose is to provide periodic security updates to all members of the workforce.
Protection from Malicious Software	The purpose is to develop procedures for guarding against, detecting, and reporting malicious software.
Log-in Monitoring	The purpose is to develop procedures for monitoring log-in attempts and reporting discrepancies.
Password Management	The purpose is to implement procedures for creating, changing and safeguarding passwords.
Security Incident Procedures	The purpose is to address security incidents.
Response and Reporting	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 covered entity; and document security incidents and their outcomes.
Contingency Plan	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.
Data Backup Plan	The purpose is to establish and implement procedures to create and maintain retrievable exact copies of sensitive information.
Disaster Recovery Plan	The purpose is to establish (and implement as needed) procedures to restore any loss of data.
Emergency Mode Operation Plan	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 emergency mode.

Information Security Policy / Procedure	Description
Testing and Revision Procedures	The purpose is to implement procedures for periodic testing and revision of contingency plans.
Applications and Data Criticality Analysis	The purpose is to assess the relative criticality of specific applications and data in support of other contingency plan components.
Evaluation	The purpose is to perform a technical and non-technical evaluation and subsequently, in response to environ-mental or operational changes affecting the security of sensitive information, that establishes the extent to which organization security policies and procedures meet the requirements of compliance requirements and business priorities.
Business Associate Contracts and Other Arrangements	The purpose is to obtain satisfactory assurances with impacted regulations that the business associate will appropriately safeguard all sensitive information.
Physical Safeguards	
Facility Access Controls	The purpose is to 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.
Contingency Operations	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.
Facility Security Plan	The purpose is to implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.

Information Security Policy / Procedure	Description
Access Control and Validation Procedures	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 of access to software programs for testing and revision.
Maintenance Records	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).
Workstation Use	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.
Workstation Security	The purpose is to implement physical safeguards for all workstations that access sensitive information and restrict access to authorized users only.
Device and Media Controls	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 the facility.
Disposal	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.
Media Re-use	The purpose is to implement procedures for removal of sensitive information from electronic media before the media are made available for re-use.

Information Security Policy / Procedure	Description
Accountability	The purpose is to maintain a record of the movements of hardware and electronic media and any person responsible therefore.
Data Backup and Storage	The purpose is to create a retrievable, exact copy of sensitive information, when needed, before movement of equipment.
Technical Safeguards	
Access Control	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.
Unique User Identification	The purpose is to assign a unique name and/or number for identifying and tracking user identity.
Emergency Access Procedure	The purpose is to establish (and implement as needed) procedures for obtaining necessary sensitive information during an emergency.
Automatic Logoff	The purpose is to implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.
Encryption and Decryption	The purpose is to implement a mechanism to encrypt and decrypt sensitive information.
Audit Controls	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.
Integrity	The purpose is to implement policies and procedures to protect sensitive information from improper alteration or destruction.

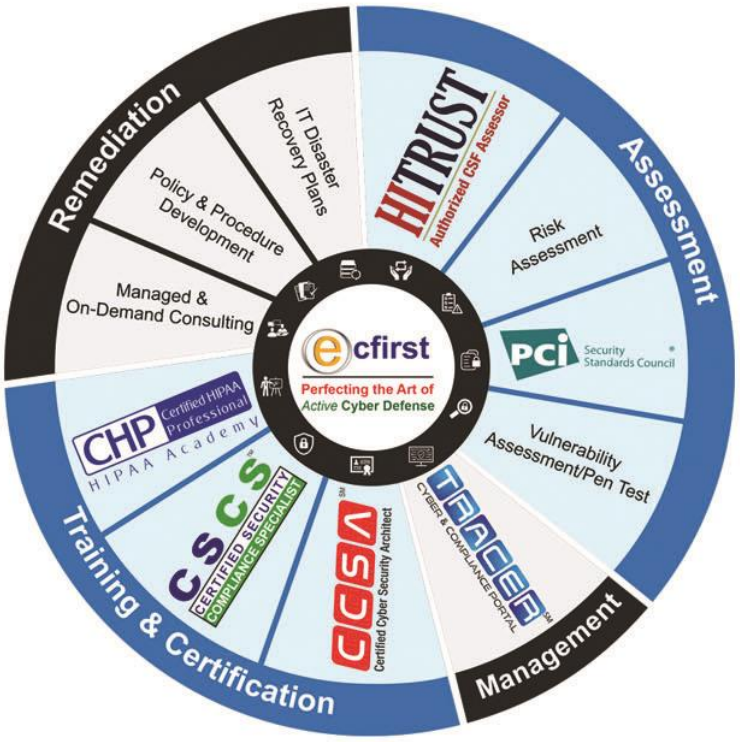
Information Security Policy / Procedure	Description
Mechanism to Authenticate Electronic Protected Health Information	The purpose is to implement electronic mechanisms to corroborate that sensitive information has not been altered or destroyed in an unauthorized manner.
Person or Entity Authentication	The purpose is to implement procedures to verify that a person or entity seeking access to sensitive information is the one claimed.
Transmission Security	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.
Integrity Controls	The purpose is to implement security measures to ensure that electronically transmitted sensitive information is not improperly modified without detection until disposed of.
Encryption	The purpose is to implement a mechanism to encrypt sensitive information whenever deemed appropriate.
Organizational Framework	
Policies and Procedures Standard	The purpose is to implement reasonable and appropriate policies and procedures to comply with applicable regulations.
Documentation	The purpose is to maintain the policies and procedures implemented to comply with regulations in written (or electronic) form and if an action, activity or assessment is required to maintain a written (which may be electronic) record.
Organizational Framework	
Information Classification	The purpose is to assist employees of organization make decisions regarding what information may and may not be

Information Security Policy / Procedure	Description
	released to the public or disclosed to any individual outside of the organization.
Network Security	The purpose is to secure communication devices and data on the organization network.
Email Security	The purpose of this policy is to protect the confidentiality and integrity of sensitive information that may be sent or received via email.
Remote Access Policy	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.
Portable Devices Policy	The purpose is to secure the use of portable devices used by members of the workforce.
VPN Policy	The purpose of this policy is to implement security measures sufficient to reduce the risks and vulnerabilities of the organization's VPN infrastructure to a reasonable and appropriate level.
Wireless Security Policy	The purpose is to implement security measures sufficient to reduce risks and vulnerabilities of organization's wireless infrastructure to a reasonable and appropriate level.
Wireless IP Phone Policy	The purpose is to implement security measures sufficient to reduce risks and vulnerabilities of organization's wireless IP phones to a reasonable and appropriate level.

Figure 1: Summary of Information Security Policies and Procedures.

ecfirst

Perfecting the Art of *Active* Cyber Defense



Client Reference

"BrightOutcome is focused in improving patient health outcomes across the continuum of care. BrightOutcome is deeply committed to securing patient information across our systems and Web-based applications. We have been working with Ali Pabrai and his wonderful team at ecfirst since 2012."

"The ecfirst team literally helped us build our HIPAA practices from ground up, allowing us to offer secure HIPAA-compliant eHealth and health IT solutions to our customers across the U.S. We are actively taking the logical next step in working with ecfirst to pursue the HITRUST certification in order to further expand our market. We see the partnership with ecfirst as an ***integral part*** of our business strategy and have been ***extremely satisfied*** with the ***quality and value*** of the services that ecfirst has rendered."

BrightOutcome
COLLABORATIVE SYMPTOM MANAGEMENT

DerShung Yang | Founder & President

"I just wanted to take a moment and say thank you. Thank you and the ***excellent team*** at ecfirst for ***hard work***, late hours and ***diligence*** during the first round of our HITRUST certification, and now working on our annual risk management and HIPAA compliance assessment."

"We at BRG are always looking to improve and enhance our compliance and cybersecurity posture. This is an area of executive and strategic priority for our organization to secure confidential client information. From HIPAA compliance, cybersecurity pen tests, to the HITRUST certification engagement, we have found ecfirst to be an ***exceptional partner*** that labored incredibly hard for us, with us. The ecfirst insight and diligence to ensuring HITRUST certification mandates are met led to us completing our engagement on budget and time."

BRG
Berkeley Research Group

Chip Goodman | Vice President of Information Technology

John Schelewitz | John.Schelewitz@ecfirst.com | +1.480.663.3225

Delivering Everything Compliance. Everything Security.

1000s of Clients | Clients in all 50 States | Clients on 5 Continents

HITRUST Authorized CSF Assessor | PCI Security Standards Council

Corporate Office

295 NE Venture Drive

Waukee, IA 50263

United States

John T. Schelewitz

Regional Sales Director

ecfirst/HIPAA Academy

Phone: +1.480.663.3225

Email: John.Schelewitz@ecfirst.com

www.ecfirst.com