COMMUNITY CLINIC ASSOCIATION OF LOS ANGELES COUNTY

Healthcare Policy & Procedure Template Library

User Guide

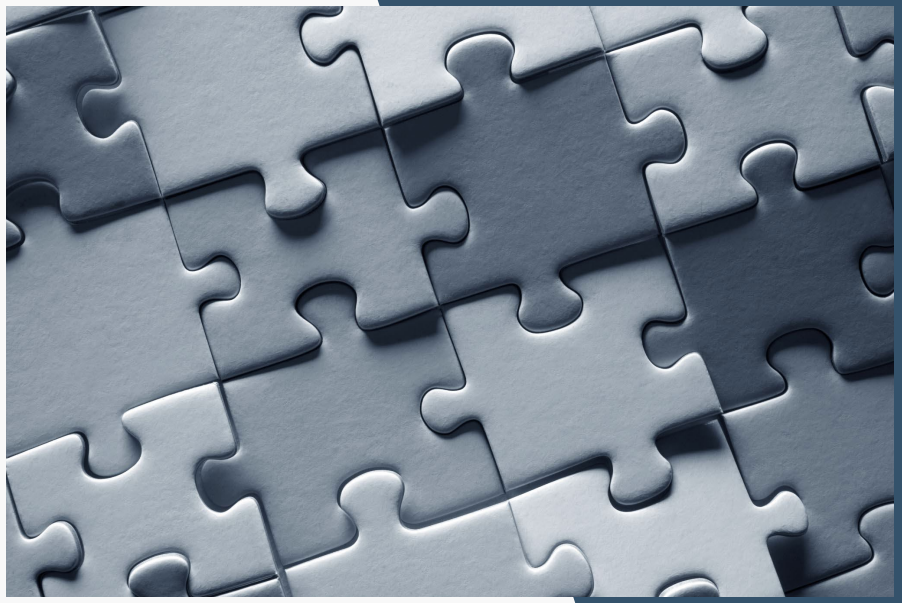
Offered in collaboration with the Community Clinic Association of Los Angeles County

online business systems

Effective Policies:

Organizational policies and procedures are just one piece in building a security-focused culture. Effective policies and procedures:

- Translate compliance requirements to business, process, culture, and patient needs.
- Drive uniformity and consistency in behavior and process to improve compliance.
- Simplify complex requirements for practical application.



online business systems

COMMUNITY CLINIC ASSOCIATION OF LOS ANGELES COUNTY

Overview

There is no golden list of policies and procedures. Different organizations are subject to different requirements, vary in infrastructure and organizational makeup, and represent unique cultures. Because of this, this library is not intended to be a "checkbox" item on the long list of items healthcare organizations need to do. Instead, the intent of this library is to provide a strong starting point each organization can leverage to adapt to its unique operational, organizational, and cultural needs.

Organizations should require all employees, and applicable contractors, board members, volunteers, and other Workforce Members to read and acknowledge the policies and procedures on a regular basis. Effective policies help translate complicated requirements and drive uniform adoption of behavior across an organization.

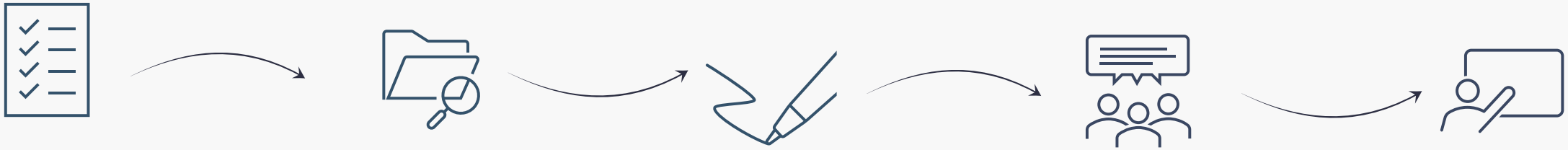
Applicable Regulations and Standards

Templates included in this library are derived from federal healthcare regulations and best practice standards. Given the range of federal and state compliance needs, content is primarily focused on the following:

- HIPAA Security Rule (45 CFR Part 160 and Subparts A and C of Part 164)
- OCR HIPAA Audit Protocol
- Cybersecurity Act of 2015 Section 405(d) – Health Industry Cybersecurity Practices (HICP), *Cybersecurity Practices for Medium and Large Organizations*
- NIST SP 800-66 v1 – *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*
- ISO/IEC 27001: Information security, cybersecurity and privacy protection — Information security management systems — Requirements
- ISO/IEC 27002: Information technology — Security techniques — Code of practice for information security control
- Healthcare & Public Health Sector Coordinating Councils Coordinated Healthcare Incident Response Plan (CHIRP)

Specific references are included in each template for traceability. Templates are designed to be more comprehensive, so organizations can best select content based on your needs.

How to Use



Identify Needs

Leverage the HIPAA Gap Analysis tool to identify gaps in current policies and procedures.

Prioritize Content

Prioritize gaps based on organizational priorities and risk assessment needs .

Revise Documents

Update provided templates or borrow sample language from the library to incorporate into your existing documentation set.

Review & Approve

Review revised documentation with appropriate review committee and organizational members and document approval.

Implement & Communicate

Incorporate updates into training and communicate changes and requirements to Workforce Members.

Identify Needs

We assume each organization has some level of documented policies and procedures in place. The challenge is how to identify your needs and prioritize effort to updating your existing set.

As stated, there is not a single list of policies and procedures required for healthcare organizations. As HIPAA is a foundational compliance requirement across all healthcare covered entities and business associates, we have provided a HIPAA Gap Analysis tool that organizations can leverage to map existing documentation to HIPAA Security Rule Standards and Implementation Specifications. This Gap Analysis also reflects guidelines derived from the OCR Audit Protocol, which is used in the Phase 2 HIPAA Audit Program. Policies included in this Library have been mapped to specific requirements so organizations can easily identify sample content that may be required to enhance its documentation.

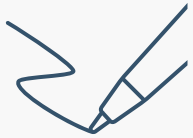
Instructions on how to use this HIPAA Gap Analysis tool are provided in the tool.

Prioritize Content

Given the priority of patient care and competing demands for staff attention, documentation tends to fall last on the list of priorities.

We recommend that once an organization identifies its needs, it prioritizes updates on its general Information Security Program and Security Risk Management policy first to establish a firm foundation for its security program and selected controls. Given HIPAA's emphasis on risk-based selection, organizations should leverage its most recent risk assessment results to identify policy and procedures based on identified risk to the organization. It can then develop a project with targeted goals for implementing additional policy and procedure updates that reflect risk-based priorities.

Once priorities are set, the organization should review the **Library Inventory Map** to identify templates to target. The map provides a high-level overview of each template, content categories included in that template, applicable regulations and standards it covers, as well as supporting documentation and considerations the organization could leverage in its updates.



Revise Documents

The Template Library includes individual Word documents that can be used as a starting point. To Revise the Documents:

1. Identify the desired section/template and create a copy of the document. You may copy the Template file or cut content sections from it to paste into your own documents.
2. Update the Document header table with the appropriate Author and Policy #. The Effective Date should be updated after official approval per the organizational review and approval process.
3. Organizational-specific content or optional content is highlighted in <red font>. This includes references to recommended procedures, plans, or other documents that are not included in the Library.
    a. Do a global "find and replace" for the term <Organization> and replace with the appropriate company name.
    b. Update other content identified in <red>. This may be streamlined by searching "<>" within the document.
4. Update any additional state, local, or other references or standards as needed to Section 7.
5. Add in any additional referenced documentation, including organizational specific policies, procedures, or other plans to Section 8.
6. Update the Revision History accordingly in Section 9.
7. **Carefully review the language and assure it is applicable to your practice and business operation. Modify it as necessary to assure language is easy for your workforce members to understand.**
8. Save the document in the appropriate working folder for review.

Generic Policy and Procedure Templates have been provided to support the creation of additional policies or procedures not included in this Library.

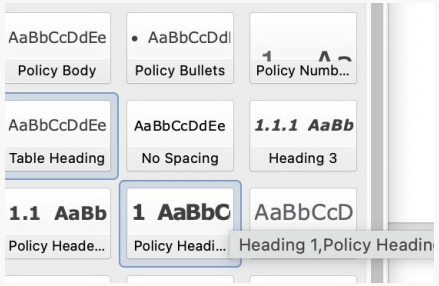
Policy Template

The Policy template is organized as follows:

Instructions and Notes	This table provides the Template user with instructions specific to the policy revision. When applicable, Online has provided additional guidance or best practice considerations to further inform organizational-specific updates.
Purpose	This section is used to provide an introduction and background information and establish the need for the policy.
Scope	This section establishes those who might be affected by the policy, and what may be excluded from the policy.
Policy	This section provides suggested policy statements and content. Due to the detailed nature of some of the regulations, this sometimes results in very detailed policy statements. Given the variation across organizations, several policy statements are highlighted in red font to identify options for organization consideration. Template users should understand their overall regulatory landscape and requirements needed prior to making substantive changes to the policy sections.
Responsibility	This section generally outlines high level roles accountable for the policy and the high-level responsibilities those roles have in supporting the policy. Generic titles for personnel responsible for implementing the policy should be listed to reduce the need to update if named staff leave the position. Detailed actions by roles should be further outlined in supporting procedures.
Exceptions	This section provides a sample method for allowing and documenting exceptions to the policy. This section should be revised to reflect each organization's specific exception process.
Compliance	This section provides a sample policy compliance statement for consideration. This section should be revised to reflect each organization's needs.
Applicable Laws, Regulations/ Requirements	This section lists applicable regulatory references and best practice standards considered in the policy creation.
Referenced Documents	This table summarizes documents that are referenced throughout the policy template. Online has listed referenced documents included in the Library. Organizations will need to add any additional documents, such as titles to organizational-specific procedures or forms.
Revision History	This table captures the revision history of the template and should be used to document updates made throughout the lifecycle of the document.

Style Guide

Templates provided in the Library were developed with the following style and formatting guidelines.



- Templates include specific Styles that can be used to update content. Each Style is title is prefaced with the term "Policy."
- Terms or content that requires organizational-specific updates is highlighted in red font.
- When referencing another policy, procedure, or document, the title of the document is included in ***Bold, Italic font***. Note that referenced documents which Online recommends an organization have in place but are NOT included in the library are highlighted in ***Red, Bold, Italic font.***
- To streamline updates to definitions, acronyms, or other terms, Online has included a global Policy and Procedure Definitions Guide to avoid the need to regularly define terms and acronyms throughout the documents. Where appropriate, acronyms are spelled out in the first use of each document.

Review and Approve

Once prioritized revisions are made, the organization should conduct a formal review with its appropriate governing board to finalize the Policy or document. Approval dates should be captured in Effective Date in each Policy.

Organizations should conduct a routine annual review of all organizational policies, procedures, and key plans. The frequency may be more often based on systems and operational changes, or other identified risks.

It's important to note that under the HIPAA regulations, covered entities must retain policies and procedures for at least six years, from either the date of creation, or the last "effective date," whichever date is later.

Implement and Communicate

Given the goal of building **Effective Policies** and procedures, the most important step is to implement the revised policy or procedure within your organization.

This can be done in many ways. Often, this is included as part of an employee's onboarding or annual security training or can be sent out as a special notice via email or other communication forums.

Online recommends that organizations require some form of formal acknowledgement that the employee has read and understands the policy or procedure, and includes that acknowledgement with employment records.

Library Inventory Map

Policy Templates

- Information Security Program Policy
- Security Risk Management Policy
- Asset and Data Management Policy
- Workforce Security
- Identity Management and Access Control Policy
- Remote Access Policy
- Security Awareness and Training Policy
- Security Incident Response Policy
- Business Continuity and Disaster Recovery
- Third-Party Management Policy
- Facility Access Policy
- Acceptable Use Policy
- Device and Media Controls Policy
- Logging and Monitoring Policy
- Transmission and Storage Policy
- Bring Your Own Device (BYOD) Policy

Supporting Materials:

- HIPAA Gap Analysis Tool
- Policies and Procedures Definition Template
- Policy Template
- Procedure Template
- Sanction Procedure
- Security Incident Response Plan, including sample forms and documentation templates
- Ransomware Playbook Sample
- Technical Testing Considerations
- Sample Third-Party Vendor Assessment Questionnaire

Policy Templates

Information Security Program Policy

General Description	The Information Security Program Policy establishes an organizational wide information system security program and sets forth governance and other general program requirements. Topics include: ***General Security Program Policy, Compliance, Governance, Responsibility, Policy Management, Independent Reviews of Security Services***	
Referenced Requirements and Standards	• HIPAA § 164.308(a)(2): Assigned Responsibility • HIPAA § 164.308(a)(8): Evaluation • HIPAA § 164.316(b)(1): (includes Time Limit, Availability, Updates) • Health Industry Cybersecurity Practices (HICP): 10.M.A: Roles and Responsibilities • NIST SP 800-66 Section 4.21 • NIST SP 800-53 Security Controls Mapping RA-1, PL-1, PL-2, PL-3, RA-1, RA-3 • ISO/IEC 27001: A.5 Security policy • ISO/IEC 27002: 2005 Section 5: Security Policy	
Supporting Documentation	**Included:** • Policy and Procedures Definitions Guide • Third-Party Management Policy	**Recommended:** • Policy Review and Modification Procedure • Records Management Procedure
Other Considerations	• H.R. 7898 or the 2021 HITECH Act amendment requires Health and Human Services (HHS) to take into account if an organization can demonstrate Recognized Security Practices have been in place for the last 12 months prior to a security incident. The organization should update document to reflect Recognized Security Practices guidelines, methodologies, processes to the extent possible. • As roles and responsibilities vary across organizations, the organization should update to reflect its own organization structure, roles, and responsibilities.	
Link	*<insert hyperlink to document>*	

Security Risk Management Policy

General Description	This Policy outlines the scope, responsibilities, and processes associated with risk identification, assessment and analysis, mitigation, acceptance, and continuous monitoring. Topics include: ***Risk Analysis, Risk Management, Ongoing Evaluation***	
Referenced Requirements and Standards	• HIPAA §164.308(a)(1): Security Management Processes • HIPAA §164.308(a)(1)(ii)(A) Security Management Process -- Risk Analysis • HIPAA §164.308(a)(1)(ii)(B) Security Management Process -- Risk Management • NIST SP 800-66 Appendix E • NIST SP 800-53 Security Controls Mapping RA-2, RA-3, RA-4, PL-6 • ISO/IEC 27002: 2005: Section 4 • ISO/IEC 27002: 2005, Section 15.2 Compliance with security policies and standards, and technical compliance	
Supporting Documentation	**Included:** • Policy and Procedures Definitions Guide • Third-Party Management Policy	**Recommended:** • Risk Assessment Procedure
Other Considerations	• H.R. 7898 or the 2021 HITECH Act amendment requires Health and Human Services (HHS) to take into account if an organization can demonstrate Recognized Security Practices have been in place for the last 12 months prior to a security incident. The organization should update document to reflect Recognized Security Practices guidelines, methodologies, processes to the extent possible. • Organizations can leverage the ONC's Security Risk Assessment tool which can be downloaded to guide the internal Security Risk Assessment process. • As roles and responsibilities vary across organizations, the organization should update this template to reflect its own organization structure, roles, and responsibilities. • Some organizations may have an existing risk management policy that includes clinical risk assessment and quality management. Security Risk Management could be considered a subsection of a broader Risk Management Policy. • Note that Third-Party Security Risk Management is further outlined in the supporting Third-Party Management Policy.	
Link	*<insert hyperlink to document>*	

Asset and Data Management Policy

General Description	Asset and Data Management Policy establishes requirement for the management of data and assets. The recording, documenting, classifying, and maintenance of data and assets is critical for protecting the confidentiality, integrity, and availability of confidential data and organizational data. Topics include: ***Consistent Protection, Classification, Handling and Protection Rules, Retention, Asset Control, Exchanges of Information and Software***	
Referenced Requirements and Standards	• HIPAA § 164.308(a)(7)(ii)(E): Applications and Data Criticality Analysis • HIPAA § 164.310(d)(2)(iii): Accountability • HIPAA § 164.316(b)(1) (includes Time Limit, Availability, Updates) • Health Industry Cybersecurity Practices (HICP): 4.M.A: Classification of Data, 7.M.D: Patch Management, Configuration Management, Change Management, 9.M.D: Asset Management, 10.M.A: Data Classification 10.M.A: Roles and Responsibilities	
Supporting Documentation	**Included:** • Policy and Procedures Definitions Guide • Device and Media Controls Policy • Acceptable Use Policy • Remote Access Policy	**Recommended:** • Information Handling Guidelines • Record Management Policy
Other Considerations	• Due to the potential variation in data classification levels, this template has provided a sample for reference. Although HIPAA classification guidelines require grouping data according to its level of sensitivity, it does not dictate a structure. Classification of data should be used to determine baseline security controls for the protection of data.	
Link	*<insert hyperlink to document>*	

Workforce Security Policy

General Description	Workforce Security ensures that all members of the organization's workforce have appropriate access to confidential data, including ePHI, to support job functions, while establishing policy to prevent inappropriate access to data. Topics include: ***Workforce Security, Workforce Clearance, Authorization, Separation of Duties, Transfers, Modifications, and Terminations, Sanctions***	
Referenced Requirements and Standards	• HIPAA §164.308(a)(2)(iii): Sanctions Policy • HIPAA §164.308(a)(3)(i): Workforce Security • HIPAA §164.308(a)(3)(ii)(A): Authorization and/or supervision • HIPAA §164.308(a)(3)(ii)(B): Workforce clearance procedure • HIPAA §164.308(a)(3)(ii)(C): Termination procedures • NIST SP 800-53: CA-6 Security Authorization • ISO/IEC 27001: 2005 - Section 5 Management responsibility • ISO/IEC 27002: 2005 - Section 7.1 Responsibility for Assets • NIST SP 800-66: Section 4.3. Workforce Security • NIST SP 800-53: AC-2, PS-1, PS-3, PS-4, PS-5, PS-6 • ISO/IEC 27001: 2005 - Sections A.8.3 Termination or change of employment, A.8.1.2 Screening • ISO/IEC 27002: 2005 - Section 8 The Company manager Security	
Supporting Documentation	**Included:** • Sanction Procedure • Security Awareness and Training Policy • Identity Management and Access Control Policy	**Recommended:** • Employment Screening Procedure • Access Management Procedure
Other Considerations	• Each organization will likely have different names for forms required to support the process. Where applicable, the organization should insert the appropriate form or ticket type specific to their organization. • The terms Workforce Member and employee are used within the content as there may be policy statements that apply to only employees or contracted staff or third parties. Under 45 CFR Part 160, HIPAA defines "Workforce" to mean "employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity or business associate, is under the direct control of such covered entity or business associate, whether or not they are paid by the covered entity or business associate."	
Link	*<insert hyperlink to document>*	

Identity Management and Access Control Policy

General Description	The Identity Management and Access Control Policy governs Workforce Member access to information resources, including systems, workstations, and confidential data. Topics include: ***Access Establishment, Access Management, Identity Management, Emergency Access Procedure, Automatic Logoff***	
Referenced Requirements and Standards	• HIPAA §164.308(a)(4)(i): Information System Management • HIPAA §164.308(a)(4)(ii)(B): Access authorization • HIPAA §164.308(a)(4)(ii)(C): Access establishment and modification • HIPAA §164.308(a)(5)(ii)(D): Password Management • HIPAA §164.312(a)(1): Access Control • HIPAA §164.312(a)(2)(i): Unique User Identification • HIPAA §164.312(a)(2)(ii): Emergency Access Procedure • HIPAA §164.312(a)(2)(iii): Automatic Logoff • HIPAA §164.312 (c)(1): Integrity • HIPAA §164.312 (c)(2)(i): Mechanism to Authenticate Electronic Protected Health Information • HIPAA §164.312 (d): Person or Entity Authentication • Health Industry Cybersecurity Practices (HICP): 3.M.A: Identity, 3.M.B: Provisioning, Transfers, and De-provisioning Procedures, 3.M.C: Authentication, 9.M.C: Identity and Access Management, 10.M.A: IT Controls • NIST SP 800-53 Security Controls Mapping AC-1, AC-2, AC-3, AC-17, PS-7 • ISO/IEC 27001: 2005 A.11.2 User access management • NIST SP 800-53 Security Controls Mapping: IA-2, IA-4, IA-5, IA-6, IA-7 • ISO/IEC 27002: 2005 Section 11.2.3 User password management	
Supporting Documentation	**Included:** • Asset and Data Management Policy • Third-Party Management Policy • Logging and Monitoring Policy • Sanctions Procedure • Security Awareness and Training Policy	**Recommended:** • Access Management Procedure • User Access Review Procedure • Emergency Mode Procedure
Other Considerations		
Link	*<insert hyperlink to document>*	

Remote Access Policy

General Description	Remote Work and Access Policy sets forth requirements and acceptable criteria for remote access to the organization's network, information systems, and assets: ***Remote Work, Remote Access***	
Referenced Requirements and Standards	• HIPAA §164.308(a)(3) Workforce Security • HIPAA §164.308(a)(5)(i) Security Awareness and Training • HIPAA §164.308(a)(5)(ii)(A): Security Reminders • HIPAA §164.308(a)(5)(ii)(B): Protection from Malicious Software • HIPAA §164.308(a)(5)(ii)(C): Log-in Monitoring • HIPAA §164.308(a)(6)(ii): Response and Reporting • HIPAA §164.308(a)(5)(ii)(D): Password Management • HIPAA § 164.316(b)(1) (includes Time Limit, Availability, Updates) • Health Industry Cybersecurity Practices (HICP): 10.M.A: Acceptable Use/E-Mail Use, 10.M.A: Laptop, Portable Devices, and Remote Use • HIPAA NIST SP 800-66 Section 4.21 • NIST SP 800-66 Section 4.21 • NIST SP 800-53 Security Controls Mapping RA-1, PL-1, PL-2, PL-3, RA-1, RA-3 • ISO/IEC 27001: A.5 Security policy • ISO/IEC 27002: 2005 Section 5: Security Policy	
Supporting Documentation	**Included:** • Policy and Procedures Definitions Guide • Sanctions Procedure • Third-Party Management Policy • Transmission and Storage Policy	**Recommended:** • NA
Other Considerations	• Some organizations may have a special Remote Work Agreement or Form that needs to be signed by the member requesting remote access. If so, that should be added to this Policy. In some cases, organizations require members to sign the policy directly.	
Link	*<insert hyperlink to document>*	

Security Awareness and Training Policy

General Description	This policy outlines scope, responsibilities, processes associated with security awareness training, privacy, and cyber security awareness and training. Topics include: ***Information Security and Privacy Training, Information Security and Privacy Awareness***	
Referenced Requirements and Standards	• HIPAA §164.308(a)(3) Workforce Security • HIPAA §164.308(a)(5)(i) Security Awareness and Training • HIPAA §164.308(a)(5)(ii)(A): Security Reminders • HIPAA §164.308(a)(5)(ii)(B): Protection from Malicious Software • HIPAA §164.308(a)(5)(ii)(C): Log-in Monitoring • HIPAA §164.308(a)(6)(ii): Response and Reporting • HIPAA §164.308(a)(5)(ii)(D): Password Management • HIPAA § 164.316(b)(1) (includes Time Limit, Availability, Updates) • Health Industry Cybersecurity Practices (HICP): 10.M.A: Acceptable Use/E-Mail Use, 10.M.A: Laptop, Portable Devices, and Remote Use • HIPAA NIST SP 800-66 Section 4.21 • NIST SP 800-66 Section 4.21 • NIST SP 800-53 Security Controls Mapping RA-1, PL-1, PL-2, PL-3, RA-1, RA-3 • ISO/IEC 27001: A.5 Security policy • ISO/IEC 27002: 2005 Section 5: Security Policy	
Supporting Documentation	**Included:** • Policy and Procedures Definitions Guide	**Recommended:** • Security Training and Awareness Plan
Other Considerations	• Given the scope of this library, this policy is focused on security training. Organizations often include Privacy related topics and should update this Policy accordingly.	
Link	*<insert hyperlink to document>*	

Security Incident Response Policy

General Description	This Policy outlines the scope, responsibilities, and guidelines for responding to security incidents within the organization. Topics include: ***Security Incident Management, Security Incident and Breach Response Team, Security Incident Response, Training and Testing, Updates***	
Referenced Requirements and Standards	• HIPAA §164.308(a)(6)(i): Security Incident Response • HIPAA §164.308(a)(6)(ii): Response and Reporting • Health Industry Cybersecurity Practices (HICP): 8.M.B: Incident Response, 10.M.A: Incident Reporting and Checklist • NIST SP 800-66 Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) 4.6. Security Incident Procedures • NIST SP 800-53 Security Controls Mapping: IR-4, IR-5, IR-6, IR-7 • ISO/IEC 27002: 2005 Section 13 Information security incident management • ISO/IEC 27001: 2005 Section A.13 Information security incident management	
Supporting Documentation	**Included:** • Policy and Procedures Definitions Guide • Security Incident Response Plan	**Recommended:** • HIPAA Data Breach Reporting Policy
Other Considerations	• This policy may be incorporated into a broader incident response policy which covers environmental, chemical, and other emergency response and incidents. • Online recommends the details related to Incident Response are outlined in a supporting Incident Response Plan (IRP) which should include specific procedures and playbooks related to security related incidents, such as Ransomware .	
Link	*<insert hyperlink to document>*	

Business Continuity and Disaster Recovery Policy

General Description	Business Continuity and Disaster Recovery Policy serves as a basis for the Business Continuity and Disaster Recovery Plan (BC/DR Plan) for handling responses to system emergencies involving confidential data, including ePHI.. Topics include: ***Business Continuity Governance, Criticality, Backups, Recovery, Emergency Mode, Testing and Revision***	
Referenced Requirements and Standards	• HIPAA §164.308(a)(7)(i): Contingency Plan • HIPAA §164.308(a)(7)(ii)(A): Data Backup Plan • HIPAA §164.308(a)(7)(ii)(B): Disaster Recovery Plan • HIPAA §164.308(a)(7)(ii)(C): Emergency Mode Operation Plan • HIPAA §164.308(a)(7)(ii)(D): Testing and Revision Procedures • Health Industry Cybersecurity Practices (HICP): 4.M.D: Backup Strategies, 10.M.A: Disaster Recovery Plan	
Supporting Documentation	**Included:** • Policy and Procedures Definitions Guide • Business Continuity/Disaster Recovery Plan • Asset and Data Management Policy	**Recommended:** • Data Backup Procedures
Other Considerations	• NA	
Link	*<insert hyperlink to document>*	

Third Party Management Policy

General Description	This policy outlines the requirements for the management of third-parties and Business Associates (BAs) who have access to and handle confidential data, including ePHI, and information resources. Topics include: ***Third-Party Agreements , Third-Party Management, Third-Party Security Controls***	
Referenced Requirements and Standards	• HIPAA §164.308(a)(3)(ii)(A): Authorization and/or supervision • HIPAA §164.308(a)(3)(ii)(B): Workforce clearance procedure • HIPAA §164.308(a)(3)(ii)(C): Termination procedures • HIPAA §164.308(a)(4)(i): Information System Management • HIPAA §164.308(a)(4)(ii)(B): Access authorization • HIPAA §164.308(a)(4)(ii)(C): Access establishment and modification • HIPAA §164.308(b)(1): Business Associates Contract and Other Arrangements • HIPAA §164.308(a)(6)(i): Security Incident Response • HIPAA § 164.316(b)(1): (includes Time Limit, Availability, Updates)	
Supporting Documentation	**Included:** • Policy and Procedures Definitions Guide • Data and Asset Management Policy • Security Risk Management Policy • Identity Management and Access Control Policy • Acceptable Use Policy • Remote Access Policy • Security Incident Response Policy	**Recommended:** • Access Management Procedure
Other Considerations	• NA	
Link	*<insert hyperlink to document>*	

Facility Access Policy

General Description	The Facility Access Policy details how physical access to the organization's facilities and applications is controlled, while ensuring properly authorized access is allowed. Topics include: ***Facility Security Plan, Facility and Physical Access Controls, Contingency Operations, Maintenance Procedures***	
Referenced Requirements and Standards	• HIPAA §164.310 (a)(1): Facility Access Controls • HIPAA §164.310 (a)(2)(i): Contingency Operations • HIPAA §164.310 (a)(2)(ii): Facility Security Plan • HIPAA §164.310 (a)(2)(iii): Access Control Validation Procedures • HIPAA §164.310 (a)(2)(iv): Maintenance Records • NIST SP 800-66 Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) 4.10. Facility Access Controls • NIST SP 800-53 Security Controls Mapping: PE-1, PE-2, PE-3, PE-4, PE-5, CP-2, CP-6, CP-7, PE-17, PL-2, PL-6, AC-3, PE-6, PE-7, PE-8, MA-1122, MA-2, MA-6 • ISO/IEC 27002: 2005 Sections 9 Physical And Environmental Security • ISO/IEC 27001: 2005 Section A.9 Physical and Environmental security	
Supporting Documentation	**Included:** • Policy and Procedures Definitions Guide • Business Continuity and Disaster Recovery Plan	**Recommended:** • Facility Security Plan • Access Control and Validation Procedure • Maintenance Records Procedure
Other Considerations	• Given the variation of physical controls in place at organizations, this policy was developed assuming that detailed controls will be included in an organization's corresponding Facility Security Plan.	
Link	*<insert hyperlink to document>*	

Acceptable Use Policy

General Description	The Acceptable Use Policy outlines the acceptable use of information resources, including workstations, information systems, applications, equipment, or other resources that may store confidential information. Topics include: ***General Use, Workstation Security, Unacceptable Use, Clean Desk, Terms and Conditions of Employment***	
Referenced Requirements and Standards	• HIPAA §164.310(b) Workstation Use • HIPAA §164.310(c) Workstation Security • HIPAA §164.310(d)(2)(iii): Accountability • HIPAA §164.312(a)(2)(iii): Automatic Logoff • Health Industry Cybersecurity Practices (HICP): 10.M.A: Acceptable Use/E-Mail Use • NIST SP 800-53: CA-6 Security Authorization • ISO/IEC 27001: 2005 - Section 5 Management responsibility • ISO/IEC 27002: 2005 - Section 7.1 Responsibility for Assets • NIST SP 800-66: Section 4.3. Workforce Security • NIST SP 800-53: AC-2, PS-1, PS-3, PS-4, PS-5, PS-6 • ISO/IEC 27001: 2005 - Sections A.8.3 Termination or change of employment, A.8.1.2 Screening	
Supporting Documentation	**Included:** • Policy and Procedures Definitions Guide • Identity Management and Access Control Policy • Remote Access Policy	**Recommended:** • System Configuration Procedures
Other Considerations	• Organizations have different processes and requirements for employee forms and documentation. Insert appropriate forms or documents that formalize the employee's agreement to policies and their responsibility to the company. • Online recommends that the organization configure systems to automatically save downloads to a secure, shared drive to the extent possible	
Link	*<insert hyperlink to document>*	

Device and Media Controls Policy

General Description	The Device and Media Controls Policy governs the receipt and removal of hardware and electronic media that contain confidential data, including ePHI, in and out of organizational facilities and movement within facilities. Topics include: ***Accountability, Data Backup and Storage, Media Reuse, Disposal***	
Referenced Requirements and Standards	• HIPAA Security Rule 164.310(d)(1): Device and Media Controls • HIPAA Security Rule 164.310(d)(2)(i): Disposal • HIPAA Security Rule 164.310(d)(2)(ii): Media Reuse • HIPAA Security Rule 164.310(d)(2)(iii): Accountability • HIPAA Security Rule 164.310(d)(2)(iii): Data Backup and Storage • Health Industry Cybersecurity Practices (HICP): 5.M.C: Secure Storage for Inactive Devices, 5.M.D: Decommissioning Assets • HIPAA NIST SP 800-66 Section 4.21 • NIST SP 800-66 Section 4.21 • NIST SP 800-53 Security Controls Mapping RA-1, PL-1, PL-2, PL-3, RA-1, RA-3 • ISO/IEC 27001: A.5 Security policy • ISO/IEC 27002: 2005 Section 5: Security Policy	
Supporting Documentation	**Included:** • Policy and Procedures Definitions Guide • Identity Management and Access Control Policy • Remote Access Policy	**Recommended:** • System Configuration Procedures
Other Considerations	• Given the variation of disposal, Online suggests the organization reference NIST 800-88: Guidelines for Media Disposal for best practice recommendations.	
Link	*<insert hyperlink to document>*	

Logging and Monitoring Policy

General Description	This Policy governs logging which will take place on the network, system, and application level to monitor login, access, activity, and movement of data. Topics include: ***Audit Logs and Monitoring, Audit Activities***	
Referenced Requirements and Standards	• HIPAA §164.312(b) Audit Controls • HIPAA §164.308(a)(1)(ii)(D) Security Management Process --Information System Activity Review • NIST SP 800-66 Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule Section Audit Controls • NIST SP 800-53 Security Controls Mapping AU-1, AU-2, AU-3, AU-4, AU-6, AU-7 • ISO/IEC 27002: 2005 15.3 Information Systems Audit Considerations; 10.10.1 Audit logging • ISO/IEC 27001: 2005 A.15.3 Information Systems Audit Considerations	
Supporting Documentation	**Included:** • Policy and Procedures Definitions Guide	**Recommended:** • Audit Procedures
Other Considerations	• Depending on the size of the organization, a SIEM or other Monitoring Mechanism may be in place. Each organization should update this content appropriately to reflect its current monitoring approach	
Link	*<insert hyperlink to document>*	

Transmission and Storage Policy

General Description	The Transmission and Storage Policy establishes guidelines for Workforce Members to ensure the secure transmission and storage of confidential data, including electronic protected health information (ePHI). Topics include: ***Protection From Malicious Software, Encryption and Decryption, Integrity Controls, Network and Systems Management and Administration***	
Referenced Requirements and Standards	• HIPAA §164.312(a)(2)(iv): Encryption and Decryption • HIPAA §164.312 (c)(1): Integrity • HIPAA §164.312 (e)(1): Transmission Security • HIPAA §164.312 (e)(2)(i): Integrity Controls • HIPAA §164.312 (e)(2)(ii): Encryption	
Supporting Documentation	**Included:** • Policy and Procedures Definitions Guide • Acceptable Use Policy • Remote Access Policy • Workforce Security Policy	**Recommended:** • *NA*
Other Considerations	• If you outsource your data operations, change this to indicate that you require your outsourced entity to have a policy/procedure that includes these activities. • For 3.2.1, although the HIPAA Security Rule includes encryption as an "addressable standard" and does not specify encryption protocols, the Breach Notification Rule requires breach notification for "unsecured PHI" (often referred to as the Breach Safe Harbor). • OCR does not specify HIPAA email encryption requirements, but it points to National Institute of Standards and Technology (NIST) SP 800-45 Version 2. NIST recommends the use of Advanced Encryption Standard (AES) 128, 192 or 256-bit encryption, OpenPGP, and S/MIME. • As most organizations allow some use of personal mobile phones, organizations should consider deploying HIPAA-compliant mobile platforms (e.g. for secure text) which reflect encryption requirements by encrypting PHI both at rest and in transit	
Link	*<insert hyperlink to document>*	

Bring Your Own Device (BYOD) Policy

General Description	The Bring Your Own Device (BYOD) Policy establishes practices and requirements for the safe use of all personal devices when accessing the corporate network. Topics include: ***Devices and Support, Acceptable Use, Reimbursement, Security, Accountability***	
Referenced Requirements and Standards	• HIPAA §164.310 (b): Workstation Use • HIPAA §164.310 (c): Workstation Security • HIPAA §164.312(a)(1): Access Control • HIPAA §164.312(a)(2)(i): Unique User Identification • HIPAA §164.312(a)(2)(iii): Automatic Logoff • HIPAA §164.310(d)(2)(iii): Accountability • HIPAA §164.312 (e)(2)(i): Integrity Controls • Health Industry Cybersecurity Practices (HICP): 10.M.A: Personal Devices	
Supporting Documentation	**Included:** • Policy and Procedures Definitions Guide • Acceptable Use Policy • Identity Management and Access Control Policy	**Recommended:** • *NA*
Other Considerations	• Online recommends organization consult NIST SP 800-46 v2: Guide to Enterprise Telework, Remote Access, and BYOD Security for best practice controls and security considerations • Some organizations require the employee to sign the policy or some form acknowledging the policy for documentation purposes.	
Link	*<insert hyperlink to document>*	

Version History

Version	Date	Editor	Notes
v1	August 16, 2023	M.Erikson	Initial Release to CCALAC