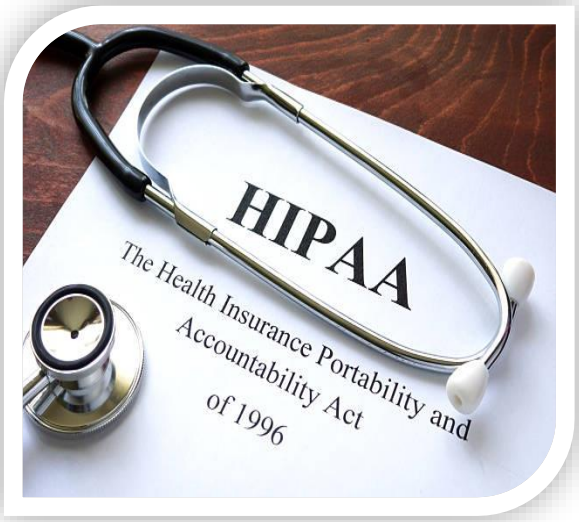
HIPAA Compliance 101 Guide - Community Care HUBs



Introduction

Welcome to the HIPAA compliance guide tailored specifically for Community Care HUBs operating within Washington State. This document compiles essential information from a wide array of sources, offering a robust framework for understanding and implementing HIPAA security measures. Aimed at ensuring the confidentiality, integrity, and availability of electronic Protected Health Information (ePHI), this guide serves as a comprehensive resource for navigating the complexities of HIPAA compliance in a community care setting.

Part 1: Understanding HIPAA and IT Security

1.1 Key Concepts and Goals

- The Health Insurance Portability and Accountability Act (HIPAA) establishes regulatory standards to safeguard sensitive patient health information from unauthorized access. With a primary focus on securing electronic Protected Health Information (ePHI), HIPAA's overarching goal is to protect patient privacy while enabling the seamless flow of health information necessary to provide high-quality health care.

1.2 Primary Areas of Focus

a) Information System Infrastructure: Developing secure, centralized, and scalable IT systems is vital for supporting the operations of a Community Care HUB.

b) Policy Development and Compliance: Crafting standardized HIPAA security and privacy policies and procedures tailored to the specific needs and operational realities of your Community Care HUB.
c) Data Security and Privacy: Adoption of comprehensive strategies to ensure the confidentiality, integrity, and availability of ePHI. Measures should include encryption, secure access controls, and annual audits.
d) Operational Compliance: Integrating HIPAA policies across all operational domains, including human resources, IT, and patient services, to ensure that all activities are conducted within the bounds of HIPAA regulations.

Sample Use Case: Navigating Contracts with Payors

For Community Care HUBs, establishing and maintaining robust IT and HIPAA security measures is not just a regulatory requirement—it's a critical step in forging essential partnerships.

Consider the scenario where a HUB seeks to sign a service agreement with major healthcare payors like Molina or Premera. These agreements often necessitate the HUB to undergo security assessments, demonstrating a stringent level of IT and HIPAA compliance.

Such prerequisites ensure that the HUB can protect sensitive health information effectively, aligning with the payors' commitment to patient privacy and data security. Failure to meet these requirements could limit the HUB's ability to collaborate with key payors, potentially impacting the range and quality of care available to patients.

This use case highlights the direct correlation between HIPAA compliance and the operational capabilities and growth opportunities for Community Care HUBs. By adhering to the guidelines outlined in this document, HUBs can navigate these agreements confidently, ensuring they are positioned to expand their services and enhance patient care.

Part 2: Setting Up for Success

2.1 Assemble the Team

Assembling a dedicated team is the first step towards HIPAA compliance. This team should include IT professionals, security officers, privacy officers, and other key personnel who possess a deep understanding of HIPAA mandates. Engaging stakeholders from across the organization ensures a holistic approach to compliance.

2.2 Define the Scope of Assessment

The scope of HIPAA compliance assessment should encompass all IT assets, including hardware, software, and electronic data storage systems. Factors such as the size of the organization, the complexity of its operations, and available resources will influence the scope of this assessment. It is also recommended to create a PHI data flow map to visually represent the flow of PHI withing your organization. This will aid in identifying all points of interaction with PHI, ensuring that no area is overlooked.

2.3 Review HIPAA Documentation

Regularly reviewing and updating HIPAA documentation is essential. This includes privacy policies, risk analyses, and breach notification procedures, ensuring they reflect current regulations and best practices.

Part 3: Policies and Procedures

3.1 Establish IT Security Policies (sample template)

These should cover:

EASY	MEDIUM	HARD
1 Acceptable Use Policy	11 Acquisition Assessment Policy	21 Disaster Recovery Plan
2 Backup and Recovery Policy	12 Access Control Policy	22 EMR-EHR Audit Policy
3 HIPAA Security Officer Designation Policy	13 External Information System Services Policy	23 Incident Response Policy
4 Hardware/Software Acquisition Policy	14 Information Classification Policy	24 IT Audit Policy
5 HR-IT Onboarding Policy	15 Physical and Environmental Security Policy	25 Position Risk Categorization Policy
6 Media Protection Policy	16 Role-based Security Training Policy	26 Security Management Policy
7 Mobile Device Responsibility Policy	17 Security Awareness Training Policy	27 System Integrity Policy
8 Password Policy	18 Social Engineering Awareness Policy	
9 Separation of Duties Policy	19 Workforce Security Policy	
10 Software Installation Policy	20 Workstation Security (For HIPAA) Policy	

3.2 HIPAA Privacy Policies

These should cover:

EASY	MEDIUM	HARD
1 Right to an Accounting of Disclosures Policy	19 Business Associate Policy	26 Treatment, Payment, and Healthcare Cyber Operations Policy
2 Right to File a Complaint Policy	20 Data Use Agreement Policy	27 Law Enforcement Identification and Location Policy
3 Right to Request Amendments Policy	21 De-Identification of PHI Policy	28 Limited Data Set and Data Use Agreements Policy
4 Right to Request Confidential Communication Policy	22 Fundraising Communications Data Set Policy	
5 Right to Request a Restriction Policy	23 No Authorizations Required to Use and	
6 Sale of PHI Policy	24 Disclose PHI Policy	
7 Use and Disclosure Policy	25 Record Retention Policy	
8 Workforce Training Policy		
9 Administrative Policy		
10 Authorization Policy		
11 Breach Notification Policy		
12 Designated Record Set Policy		
13 Fundraising Communications Policy		
14 Marketing Communications Policy		
15 Minimum Necessary Policy		
16 Notices and Individual Rights Policy		
17 Opportunity to Agree or Object to a Use or Disclosure of PHI Policy		
18 Personal Representatives Policy		

Part 4: Training and Awareness

4.1 Assess Training Programs

Implementing comprehensive training programs on HIPAA compliance and security incident response is critical. Training should be mandatory for all employees, with specialized, role-based training for IT staff, security, and privacy officers.

4.2 Security Awareness

Cultivating a culture of security within the organization is essential. Regular training updates and awareness sessions help maintain vigilance and ensure ongoing compliance.

Part 5: Risk Assessment and Management

5.1 Conduct a Risk Assessment

A thorough risk assessment process is necessary to identify, evaluate, and prioritize risks to ePHI. This should be an ongoing effort, with annual reassessments to adapt to new threats and vulnerabilities.

5.2 Develop an Action Plan

Developing a clear action plan to address identified security gaps and vulnerabilities is crucial. Assign responsibility for implementing each action item to ensure accountability.

Part 6: Monitoring and Review

6.1 Create a Security Assessment Report

Summarize the findings, recommendations, compliance status, and results of the risk assessment in a comprehensive security assessment report. Share this report with key stakeholders to inform ongoing compliance efforts.

6.2 Continuous Improvement

Recognize that HIPAA compliance is a dynamic, ongoing process. Regular reviews and updates to policies, procedures, and training programs are necessary to address new threats, technological advancements, and changes in regulatory requirements.

Conclusion

This guide provides a foundational framework for Community Care HUBs in Washington State embarking on their journey towards HIPAA compliance. By integrating rigorous IT security policies, regular training initiatives, and a proactive approach to risk management, HUBs can effectively safeguard sensitive health information and foster a culture of compliance.

NIST 800-53 CONTROLS

NIST CONTROL FAMILIES	HIPAA Required Controls
AC - ACCESS CONTROL	• AC-2 • AC-6 • AC-18
AT – AWARENESS AND TRAINING	• AT-3
AU- AUDIT AND ACCOUNTABILITY	• AU-2[• AU-3 • AU-4 • AU-7
CA – SECURITY ASSESSMENT AND AUTHORIZATION	
CM – CONFIGURATION MANAGEMENT	• CM-8
CP – CONTINGENCY PLANNING	• CP-2 • CP-4 • CP-10
IA – IDENTIFICATION AND AUTHORIZATION	• IA-2 • IA-5
IR- INCIDENT RESPONSE	• IR-2 • IR-3 • IR-6
MA – MAINTENANCE	• MA-2
MP – MEDIA PROTECTION	• MP-5
PE – PHYSICAL/ENVIRONMENTAL PROTECTION	• PE-8
PL – PLANNING	• PL-2
PS – PERSONNEL SECURITY	• PS-2 • PS-5 • PS-7
RA- RISK ASSESSMENT	
SA – SYSTEM AND SERVICES ACQUISITION	• SA-4 • SA-9
SC – SYSTEM AND COMMUNICATIONS PROTECTION	
SI – SYSTEM AND INFORMATION INTEGRITY	
PM – PROGRAM MANAGEMENT	
PC – PRIVACY CONTROL	
SRM – SUPPLY CHAIN RISK MANAGEMENT	

Sample Policy Template

Procedure Title

Effective:	Click or tap to enter a date.	**Last Revised:**	Click or tap to enter a date.	**Next Review:**	Click or tap to enter a date.
Prepared by:	Click or tap here to enter text.		**Date:**	Click or tap to enter a date.	

Purpose

Body text… Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Scope

Body text… Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Procedures

Body text… Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Exceptions

Body text… Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Revision History

Date	Action	Name
	Draft updated and finalized for review	
	Review and approval	