ULAM LABS

HIPPA-Compliant Software Checklist

HIPPA-Compliant Software Checklist

ULAM LABS

Overview

Building HIPAA-compliant digital health products in 2025 is about designing secure architectures, applying technical safeguards, and cultivating an engineering culture where privacy and security are part of everyday decisions.

☐ Foundational Setup

- Identify all systems and services that handle PHI/ePHI
- Classify all vendors touching PHI and ensure BAAs are signed
- Assign a Privacy Officer and Security Officer roles internally

☐ Access & Identity Management

- Implement Role-Based Access Control (RBAC) across all systems
- Enforce Multi-Factor Authentication (MFA) for all users with PHI access
- Limit access to the minimum necessary based on job roles
- Maintain detailed access logs and audit trails

☐ Technical overview

- Encrypt PHI at rest using AES-256 or equivalent
- Encrypt PHI in transit using TLS 1.2+
- Enable automatic logoff and session timeouts
- Set up intrusion detection and anomaly alerts

☐ DevSecOps Integration

- Integrate security checks into CI/CD pipelines
- Perform static and dynamic code analysis with PHI in mind
- Limit local development access to real data (or use anonymized datasets)
- Use infrastructure-as-code to control and audit environment configs

HIPPA-Compliant Software Checklist

ULAM LABS

Overview

From RBAC and audit logs to encryption, secure mobile development, and risk assessments - every layer of your stack and process needs to align with HIPAA standards.

Staying compliant is an ongoing effort and one that starts early in the product design phase.

☐ Auditing & Monitoring

- Conduct annual (and post-change) risk assessments
- Schedule recurring security audits and penetration testing
- Implement real-time monitoring for unauthorized access or data exfiltration
- Keep versioned, documented audit logs for all PHI systems

☐ Policies & Training

- Provide role-specific HIPAA training for devs, ops, and contractors
- Document policies for data access, incident response, and system use
- Create a clear breach response plan, with defined escalation paths
- Review and update all security and privacy policies annually

☐ Data Handling & Lifecycle

- Define and follow secure data backup and retention policies
- Ensure secure disposal of devices and storage media
- Protect APIs and endpoints that expose patient data
- Avoid storing PHI in logs, error messages, or test environments

We build HIPPA-compliant software

Contact us