HIPAA-Compliant Software Checklist

HIPAA-COMPLIANT SOFTWARE CHECKLIST

Data Encryption - All data transmitted and stored must be encrypted using industry-standard methods. Specify encryption standards used (e.g., AES 256-bit).

◯ Yes ◯ No ◯ NA

Access Controls - Implement robust user authentication and authorization mechanisms. Detail types of access controls (e.g., role-based access, multi-factor authentication).

◯ Yes ◯ No ◯ NA

Audit Controls - Software should record and examine activity logs to track access and changes to PHI. Describe audit control capabilities and log retention policies.

◯ Yes ◯ No ◯ NA

Data Backup and Recovery - Regular backups and a clear recovery plan to prevent data loss. Outline backup frequency, storage locations, and recovery procedures.

◯ Yes ◯ No ◯ NA

Data Integrity - Measures to ensure data is not altered or destroyed improperly. Explain data integrity safeguards (e.g., checksums, version controls).

◯ Yes ◯ No ◯ NA

Transmission Security - Secure transmission of data, especially over public networks. Indicate types of transmission security (e.g., SSL/TLS encryption).

◯ Yes ◯ No ◯ NA

Automatic Logoff - Feature to automatically log off users after periods of inactivity. Specify inactivity duration before automatic logoff.

◯ Yes ◯ No ◯ NA

Disaster Recovery Plan - A comprehensive plan for restoring any lost data and maintaining business continuity. Provide details of the disaster recovery strategy and testing frequency.

◯ Yes ◯ No ◯ NA

Breach Notification Protocol - Mechanism for reporting any unauthorized access or data breaches. Detail the breach notification process and timelines.

◯ Yes ◯ No ◯ NA

User Training and Awareness - Regular training for users on HIPAA compliance and software use. Outline training frequency and content.

◯ Yes ◯ No ◯ NA

Regular Software Updates - Ensuring the software is regularly updated for security patches and compliance. Describe update schedule and patch management process.

◯ Yes ◯ No ◯ NA

Vendor Agreements and Business Associate Compliance - Agreements with vendors must comply with HIPAA requirements. List criteria for vendor compliance and monitoring methods.

◯ Yes ◯ No ◯ NA

Patient Consent and Authorization - Mechanisms for obtaining and recording patient consent for PHI use. Detail consent forms and authorization processes.

◯ Yes ◯ No ◯ NA

Privacy Policy and Notice of Privacy Practices - A clear privacy policy that aligns with HIPAA regulations. Provide a summary of the policy and how it's communicated to patients.

◯ Yes ◯ No ◯ NA

Risk Assessment and Management - Regular risk assessments to identify and mitigate potential vulnerabilities. Outline risk assessment methodology and frequency.

◯ Yes ◯ No ◯ NA

Incident Response Plan - A plan for responding to security incidents and potential breaches. Detail steps for incident identification, reporting, and remediation.

◯ Yes ◯ No ◯ NA

PHI De-identification Protocols - Procedures for de-identifying PHI where appropriate. Describe methods used for de-identification and re-identification protocols.

◯ Yes ◯ No ◯ NA

Physical Security Measures - Physical safeguards for protecting electronic systems, equipment, and data. List physical security controls (e.g., secure server rooms, access logs).

◯ Yes ◯ No ◯ NA

Compliance with State Laws - Adherence to state laws that may have more stringent requirements than HIPAA. Specify additional state-specific compliance measures.

◯ Yes ◯ No ◯ NA

Doctor's Signature

Name: _____ **Date:** _____ dd / mm / yyyy