HIPAA-Compliant Software Checklist

Criteria	Description	Details/ Requirements	Compliance Status (Yes/No/NA)
Data Encryption	All data transmitted and stored must be encrypted using industry-standard methods.	Specify encryption standards used (e.g., AES 256-bit).	
Access Controls	Implement robust user authentication and authorization mechanisms.	Detail types of access controls (e.g., role-based access, multi-factor authentication).	
Audit Controls	Software should record and examine activity logs to track access and changes to PHI.	Describe audit control capabilities and log retention policies.	
Data Backup and Recovery	Regular backups and a clear recovery plan to prevent data loss.	Outline backup frequency, storage locations, and recovery procedures.	
Data Integrity	Measures to ensure data is not altered or destroyed improperly.	Explain data integrity safeguards (e.g., checksums, version controls).	
Transmission Security	Secure transmission of data, especially over public networks.	Indicate types of transmission security (e.g., SSL/TLS encryption).	
Automatic Logoff	Feature to automatically log off users after periods of inactivity.	Specify inactivity duration before automatic logoff.	
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.	
Breach Notification Protocol	Mechanism for reporting any unauthorized access or data breaches.	Detail the breach notification process and timelines.	

User Training and Awareness	Regular training for users on HIPAA compliance and software use.	Outline training frequency and content.	
Regular Software Updates	Ensuring the software is regularly updated for security patches and compliance.	Describe update schedule and patch management process.	
Vendor Agreements and Business Associate Compliance	Agreements with vendors must comply with HIPAA requirements.	List criteria for vendor compliance and monitoring methods.	
Patient Consent and Authorization	Mechanisms for obtaining and recording patient consent for PHI use.	Detail consent forms and authorization processes.	
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.	
Risk Assessment and Management	Regular risk assessments to identify and mitigate potential vulnerabilities.	Outline risk assessment methodology and frequency.	
Incident Response Plan	A plan for responding to security incidents and potential breaches.	Detail steps for incident identification, reporting, and remediation.	
PHI De-identification Protocols	Procedures for de-identifying PHI where appropriate.	Describe methods used for de-identification and re-identification protocols.	
Physical Security Measures	Physical safeguards for protecting electronic systems, equipment, and data.	List physical security controls (e.g., secure server rooms, access logs).	
Compliance with State Laws	Adherence to state laws that may have more stringent requirements than HIPAA.	Specify additional state-specific compliance measures.	

Doctor's Signature: ___________________________

Name: _______________________________________ Date: ____________________________