HIPAA Compliance Checklist for EHR Systems (2025)

1. Access Control & Authentication

[ ] Ensure unique user identification with separate logins for each user.

[ ] Implement role-based access control (RBAC) to assign permissions based on user roles.

[ ] Enable multi-factor authentication (MFA) to enhance security.

[ ] Set up automatic log-off after inactivity to prevent unauthorized access.

2. Data Encryption & Security

[ ] Encrypt patient data in transit and at rest using AES-256 or equivalent.

[ ] Verify HIPAA-compliant cloud hosting (AWS, Azure, Google Cloud, etc.).

[ ] Maintain audit logs to track all PHI access and modifications.

[ ] Ensure end-to-end encryption for patient communication (emails, messages).

3. Data Integrity & Backup

[ ] Implement automated data backups with secure storage and easy restoration.

[ ] Maintain audit trails to track record access and modifications.

[ ] Establish data integrity checks to detect unauthorized tampering.

4. Patient Rights & Consent Management

[ ] Secure the patient portal with encryption and authentication.

[ ] Enable patient access to download, review, and correct records securely.

[ ] Support electronic consent collection for data sharing.

[ ] Implement de-identification & anonymization for compliance in research or analytics.

5. Interoperability & Compliance with 21st Century Cures Act

[ ] Ensure FHIR & HL7 support for seamless data exchange.

[ ] Prevent information blocking by allowing easy data sharing.

[ ] Secure API endpoints to prevent unauthorized access and data breaches.

6. Business Associate Agreements (BAA)

[ ] Ensure EHR vendors sign a BAA for HIPAA compliance.

[ ] Verify third-party integrations (billing, labs, imaging) comply with HIPAA.

7. Security Incident Response & Breach Notification

[ ] Conduct regular HIPAA security risk assessments.

[ ] Establish breach detection and reporting protocols.

[ ] Ensure HIPAA breach notification compliance for affected patients and authorities.

8. Training & Policies

[ ] Provide HIPAA training for all EHR users.

[ ] Implement user activity monitoring to track system usage.

[ ] Enforce security policies for password management, device security, and remote access.