



HIPAA Endpoint Compliance Checklist

Practical checklist for aligning organizational endpoints with HIPAA technical safeguards using Codeproof UEM.

Note: HIPAA compliance requires administrative, physical, and technical safeguards. Codeproof provides device and application controls that support HIPAA technical safeguards. Your organization remains responsible for overall compliance.

1) Access Control

- Require unique user IDs and strong authentication on devices handling ePHI.
- Enforce auto-lock and idle timeout to prevent unauthorized access.
- Restrict access to ePHI apps only for authorized users.

2) Audit Controls

- Enable device and user activity logging.
- Export logs and compliance reports regularly for audit review.
- Track configuration changes and remote actions (lock/wipe).

3) Integrity

- Prevent improper alteration or destruction of ePHI by enforcing app allowlists.
- Use managed configurations to restrict data movement between apps.
- Detect and block compromised/jailbroken devices.

4) Transmission Security

- Require TLS for all communications involving ePHI.
- Deploy certificates, VPN, and per-app VPN for secure remote access.
- Block legacy protocols and insecure Wi-Fi networks.

5) Device Safeguards

- Enforce device encryption (BitLocker/FileVault, iOS/Android native).
- Require strong passcodes or biometrics for device unlock.
- Use selective wipe to remove work data from BYOD devices.

6) Incident Response

- Enable remote lock, locate (where permitted), selective wipe or full wipe.
- Revoke certificates and credentials when a device is lost or stolen.
- Document incidents with logs and remediation evidence.