End-User Device Security for HIPAA

What Every Healthcare Company Must Know

An Infinitra Innovations Initiative

healthtechcompliance.com

5 Ways Data Leaks From Devices

Every device that touches ePHI is a potential data leak.

Copy/Paste

Clipboard exfiltration

Screenshots

Screen capture tools

Phone Photos

Physical camera capture

USB/Drives

File transfer to external media

Printing

Local printer output

HIPAA violations can cost up to $50,000 per record exposed

The 3 Pillars of Device Security

HIPAA requires all three working together. Technology alone is not enough.

Administrative

Safeguards

50%

- ✓ Workforce policies
- ✓ Annual training
- ✓ Sanctions for violations
- ✓ Access management

Physical

Safeguards

20%

- ✓ Privacy screens
- ✓ Device positioning
- ✓ Camera-free zones
- ✓ Facility access controls

Technical

Safeguards

30%

- ✓ MFA & encryption
- ✓ Screen capture protection
- ✓ Clipboard restrictions
- ✓ Audit logging

Technical Controls You Must Configure

These are NOT turned on by default. You must actively configure them.

Multi-Factor Auth

REQUIRED

Required for ALL users
under 2026 HIPAA updates

Encryption

REQUIRED

At rest (AES-256) and
in transit (TLS 1.2+)

Clipboard Control

REQUIRED

Disable or restrict to
paste-only direction

Screen Capture

RECOMMENDED

Block local screenshots
and screen recordings

USB/Drive Block

REQUIRED

Disable local drive and
USB device mapping

Audit Logging

REQUIRED

Log all access with
6-year retention

What You Can & Can't Prevent

CAN Prevent with Technology

- ✓ Copy/paste to local devices
- ✓ Screenshots via client tools
- ✓ File transfer to USB/drives
- ✓ Printing to local printers
- ✓ Screen sharing via apps
- ✓ Access from untrusted devices

CANNOT Prevent with Technology

- ✗ Phone photos of screens
- ✗ Memorizing patient data
- ✗ Verbal disclosure of PHI
- ✗ Screenshots within the VM
- ✗ Social engineering attacks

Technology handles 90% of the risk. Policy, training, and legal deterrents cover the rest.

The Human Layer: What Closes the Gap

When technology can't prevent it, policy and training must.

Written Workforce Policy

Explicitly prohibit photographing, copying, or sharing ePHI. Get signed acknowledgment from every employee.

Annual HIPAA Training

Device-specific training covering what's allowed and what's not. Generic training is not enough.

Sanctions & Consequences

Real enforcement: disciplinary action, termination, and HIPAA criminal penalties up to $250K and 10 years.

Physical Workspace Controls

Privacy screens, device positioning away from public areas, camera-free zones in clinical areas.

An auditor won't ask: "Can you guarantee no one takes a phone photo?"
They'll ask: "Have you implemented reasonable safeguards to prevent it?"

Your Device Security Checklist

✓	Sign a BAA with your cloud/VDI provider	CRITICAL
✓	Enable encryption at rest and in transit	CRITICAL
✓	Enforce MFA for all users accessing ePHI	CRITICAL
✓	Disable clipboard, USB, and local drive mapping	HIGH
✓	Enable screen capture protection	HIGH
✓	Set automatic session timeout (15 min)	HIGH
✓	Implement audit logging with 6-year retention	CRITICAL
✓	Create and enforce written workforce policy	CRITICAL
✓	Conduct annual device-specific HIPAA training	HIGH
✓	Restrict access to trusted devices and IPs only	MEDIUM

Not sure where you stand? Take the free HIPAA assessment at healthtechcompliance.com

Not Sure Where You Stand?

Take the free HIPAA Compliance Assessment

navigator.healthtechcompliance.com

50 questions | 15 minutes | Free | No email required

An Infinitra Innovations Initiative

Built by Ex-AWS Leaders: Saida Babu Chanda & Yogananda Karra