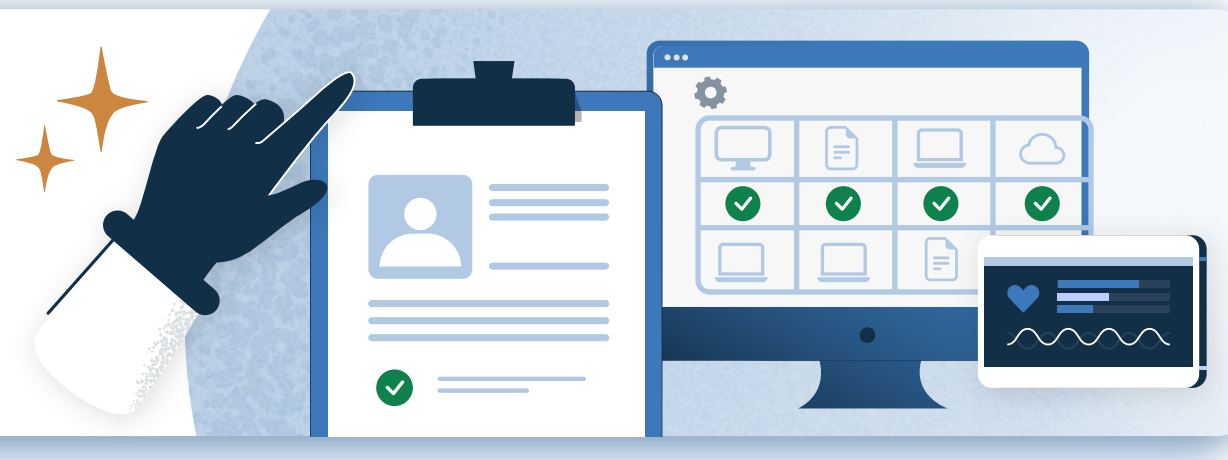
The Prey advantage: HIPAA-compliant device security

When healthcare devices go rogue, every minute counts. A single unaccounted laptop or tablet can turn into a data exposure incident, **risking thousands of patient records** and triggering HIPAA breach notifications.

Prey turns those crisis moments into controlled responses, helping IT and security teams **act fast**, contain risk, and preserve compliance when it matters most.

Containment is compliance



Protecting devices that handle **Electronic Protected Health Information** (ePHI) is a crucial, non-negotiable requirement for HIPAA compliance. The risks lie in the **delay** between a security event and decisive actions.

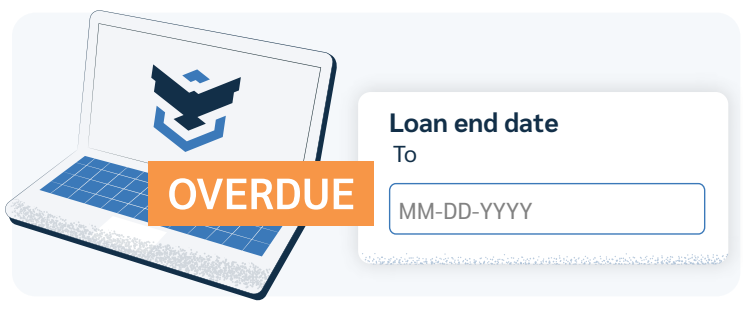
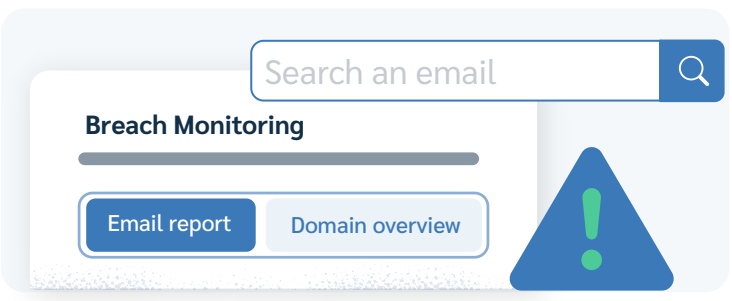
Prey bridges that gap, turning potential breaches into contained, auditable incidents.

From unsecured to secured PHI: How Prey enforces protection

State	HIPAA control	Prey action	Compliance outcome
Unsecured PHI	Access Control	**Remote device lock** Instantly restricts access when a device goes missing or leaves a secure area	Immediate containment. Prevents unauthorized viewing of ePHI.
At-Risk PHI	Transmission & Access Control	**Geofence triggers** Locks devices automatically when they exit approved zones.	Automated enforcement of access restrictions.
Secured PHI (via Encryption)	Encryption (§164.312(a)(2)(iv))	**Remote encryption activation** Enforce BitLocker or OS-native encryption remotely.	Data unreadable to unauthorized users. Qualifies for HIPAA safe harbor.
Secured PHI (via Destruction)	Disposal (§164.310(d)(2))	**Disable device or wipe data** Disables boot access or erases PHI directories.	PHI rendered irretrievable; breach notification not required.
Audit-Ready PHI	Audit Controls (§164.312(b))	**Immutable Audit Logs** Record every lock, wipe, and encryption action.	Proof of compliance for OCR or internal audits.

The Prey guarantee: Auditable actions for every scenario

Prey's cross-platform suite delivers technical safeguards that map directly to federal compliance requirements, ensuring that every remote action is both effective and auditable.

Prey solutions	Compliance Context
Device lock & geofencing We give you immediate containment 	In a lost/stolen scenario, the second the device leaves your secure geofence, we lock the device and display a custom message. This is your primary HIPAA access control measure. Any lost, unsecured device is a potential breach that triggers the **Breach Notification Rule.**
Automated offboarding We automate compliance for your workforce 	Automate device lockouts based on events like an employee's contract end or device assignment conclusion. Prey enforces **HIPAA Access Termination** and Access **Control Standards** by automatically locking the device's screen, replacing manual checklists.
Custom wipe & Kill Switch We guarantee data destruction 	If a device is unrecoverable, you have two options: wipe to remove specific ePHI directories, or trigger Kill Switch (for Windows) to render the whole drive unbootable. This addresses the **HIPAA Disposal Standard** and helps you argue for a "low probability of compromise" during a breach assessment.
Breach Monitoring We grant ongoing monitoring and timely data 	Admins and security teams need automated alerts and manual threat identification processes. All suspicious activity (e.g., malware, unauthorized access) requires rapid quarantining to stop network propagation and isolate damage, fulfilling **HIPAA Security Incident Procedures.**
Audit logs We provide irrefutable evidence 	Every remote action taken, locks, wipes, the Kill Switches, are recorded in an immutable Audit Log. If the OCR comes knocking, you demonstrate due diligence. The requirements for accurate and timely logging fall primarily under the **Technical Safeguards** section of the **HIPAA Security Rule,** specifically the **Audit Controls Standard.**

HIPAA's requirements for audit controls

Fundamentally, HIPAA requires records that serve as an **unchangeable digital witness** to all PHI interactions and administrative security actions.

- **Integrity:** Logs must be protected from improper alteration or destruction. They should be tamper-proof (or stored in a tamper-resistant system).
- **The "log":** Provides undeniable evidence of compliance verification and allows for forensic analysis during a security incident.
- **Security configuration changes:** Logs must track when administrators modify security settings.
- **Contingency plan:** The logs must record all steps taken during a security incident (e.g., reporting that a device was successfully encrypted or killed switched). This demonstrates that the organization followed its documented incident response plan.
- **Access review:** Logs of administrative actions, like granting privilege escalations or modifying access, must be tracked to ensure the **Minimum Necessary Standard** is being followed, even by IT staff.
- **Retention:** Logs must be retained for a minimum of six years, aligning with the general HIPAA documentation requirements. This calls for robust, tamper-proof storage solutions.

Don't just secure your devices, secure your compliance

Book a 15-minute tailored **demo** to see Prey's **Automated Screen Lock** in action and review our unalterable **Audit Log; the evidence your team needs!**

preyproject.com