

HIPAA COMPLIANCE EVALUATION GUIDE

PROTECT HEALTHCARE DATA WITH ABSOLUTE

THE SECURITY RULE

While the HIPAA Privacy Rule speaks to *which* data is to be protected, the Security Rule establishes *how* that data is protected. Covered Entities (CEs) must comply with both measures and are liable to fines if either of these rules are violated.

Within the Security Rule, there are three safeguard categories to ensure data is protected and standards are followed.

Safeguard Categories:

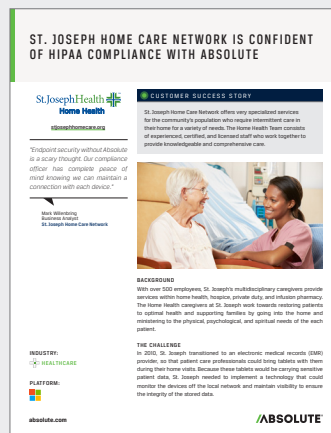
1. **Administrative**
2. **Physical**
3. **Technical**

Administrative safeguards relate to processes and policies that increase the probability of data protection. These include practices such as access controls, role permissions, monitoring, and training to create an environment where data protection and privacy are embedded in regular operations.



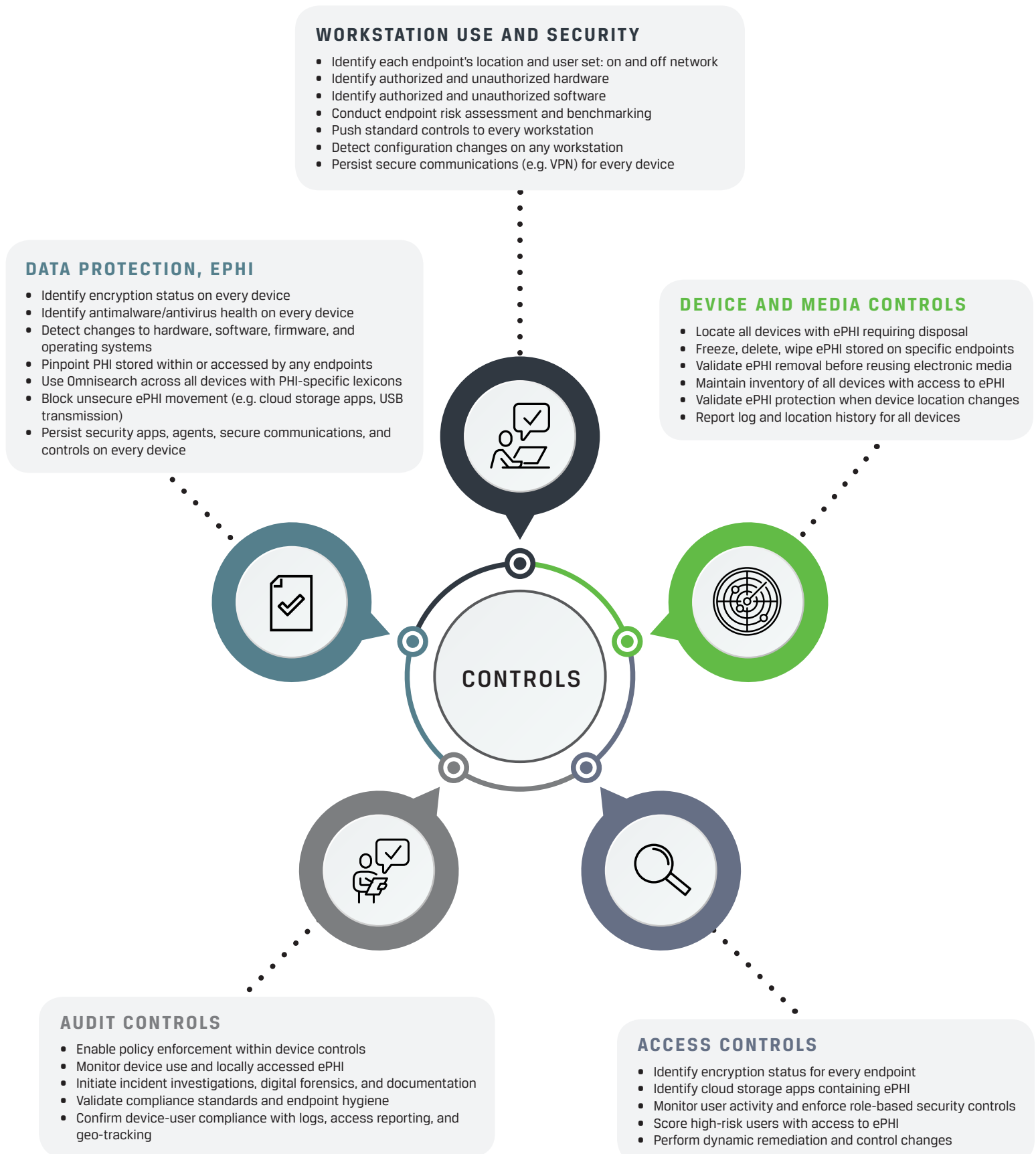
Physical safeguards are the tangible garrisons for ePHI – locked rooms, server cages, secure workstations, and disposal facilities – that provide a material space where ePHI can be shielded from unauthorized access.

Finally, technical safeguards are the ways technology is pressed into service to protect ePHI throughout its lifecycle. Technical safeguards are usually the implements that IT and IT security teams are tasked with establishing and maintaining.



St. Joseph Home Care Network is confident of HIPAA Compliance with Absolute.









[DOWNLOAD THE CASE STUDY](#)


























HOW ABSOLUTE ENABLES HIPAA COMPLIANCE ACROSS AN ENDPOINT POPULATION







To comply with these regulations, CEs and their business associates must implement administrative, physical, and technical safeguards across their endpoint populations. The following are specific technical capabilities that Absolute provides to avoid penalties for noncompliance:

WORKSTATION USE AND SECURITY 	ABSOLUTE CAPABILITY
Identify each endpoint's location and user set: on and off network	
Identify authorized and unauthorized hardware	
Identify authorized and unauthorized software	
Endpoint risk assessment and benchmarking	
Push standard controls to every workstation	
Detect configuration changes on any workstation	
Persist secure communications (e.g. VPN) for every device	

DEVICE AND MEDIA CONTROLS 	ABSOLUTE CAPABILITY
Locate all devices with ePHI requiring disposal	
Freeze, delete, wipe ePHI stored on specific endpoints	
Validate ePHI removal before reusing electronic media	
Maintain inventory of all devices with access to ePHI	
Validate ePHI protection when device location changes	
Report log and location history for all devices	

ACCESS CONTROLS 	ABSOLUTE CAPABILITY
Identify encryption status for every endpoint	
Identify cloud storage apps containing ePHI	
Monitor user activity and enforce role-based security controls	
Score high-risk users accessing to ePHI	
Dynamic remediation and control changes	

DATA PROTECTION, EPHI 	ABSOLUTE CAPABILITY
Identify encryption status on every device	
Identify antimalware / antivirus health on every device	
Detect changes to hardware, software, firmware, and operating systems	
Pinpoint PHI stored within or accessed by any endpoints	
Use Omnisearch across all devices with PHI-specific lexicons	
Block unsecured ePHI movement (e.g. cloud storage apps, USB transmission)	
Persist security apps, agents, secure communications, and controls on every device	

AUDIT CONTROLS 	ABSOLUTE CAPABILITY
Enable policy enforcement within device controls	
Monitor device use and locally accessed ePHI	
Incident investigations, digital forensics, and documentation	
Validate compliance standards and endpoint hygiene	
Confirm device-user compliance with logs, access reporting, and geo-tracking	



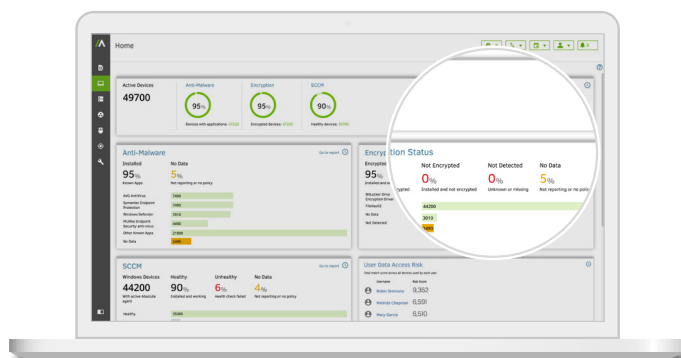


TAKEAWAYS

Each safeguard of the HIPAA Security Rule serves to fortify ePHI and ensure information confidentiality, integrity, and availability. As the digital healthcare revolution continues, organizations around the globe rely on Absolute for persistent endpoint visibility and control. Absolute provides healthcare organizations with an unrivaled view and complete command of their endpoint population, to enable data protection and eliminate compliance failures. With Absolute, you're always audit-ready. For more information about our solutions for healthcare, please visit: absolute.com/healthcare.



REQUEST YOUR FREE TRIAL TODAY



absolute.com/eval

ABOUT ABSOLUTE

Absolute provides visibility and resilience for every endpoint with self-healing endpoint security and always-connected IT asset management to protect devices, data, applications and users – on and off the network. Bridging the gap between security and IT operations, only Absolute gives enterprises visibility they can act on to protect every endpoint, remediate vulnerabilities, and ensure compliance in the face of insider and external threats. Absolute's patented Persistence technology is already embedded in the firmware of most PC and mobile devices and trusted by over 12,000 customers worldwide.