



Devices containing PHI data can be anywhere and must be secured and managed remotely. Ideally, solutions should be SaaS-based or installable using existing servers and hardware components:

Endpoint Security

- Differing levels of risk (misplaced, lost, stolen) require different levels of security
- Pre-emptive security measures should be in place to prevent a reportable breach before it happens
- No reliance on end user behavior
- Lost or stolen devices should be recoverable so hardware budgets can be spent meaningfully
- Provable method of data removal
- Understand the cause of a reportable security breach so it doesn't happen again

Endpoint Management

- Block viruses and bad downloads so the device does not become a point of risk
- Measure and manage vulnerability using standard Security Content Automation Protocol reports
- Protect the network from faulty updates using automated patch management
- Reduce footprint and increase efficiencies through effective power management policies
- Collect data from each device for proactive maintenance before the device is compromised
- Remote management console that can be used by all IT administrators to manage all devices

Healthcare organizations are held to the highest standard when it comes to managing and protecting patient healthcare information (PHI). Rules and requirements are provided by a variety of regulatory and industry bodies including HIPAA, HITECH, and HIMSS. Federal stimulus packages also exist, such as Meaningful Use to ensure hospitals and care facilities leverage technology to properly manage electronic health records (EHR).

And while it's your responsibility to navigate through this landscape and deliver on these mandates, you must also keep pace with a healthcare environment that never stands still. A few years ago it was the adoption of laptops for mainstream use in healthcare. Today it's iPads, tablets, and other ultra portable devices.

This expansion of endpoint type is simply a reflection of the reality within healthcare which has spent the past decade morphing into a model of mobility. With government pushing healthcare out of the hospital and into the home to reduce the cost of care, an IT strategy that supports mobility has become an absolute requirement.

If your healthcare organization is entrusted to manage PHI, then you need to have the right tools to secure and manage your endpoints.



Absolute® Software helps healthcare organizations around the world remotely secure and manage their endpoints. From institutes and universities to large hospitals and community healthcare centers, Absolute Software provides remote and persistent solutions so that our customers can track, locate, secure, and manage their IT deployments. Anytime, anywhere.



"Computrace immediately gave us visibility into our laptop population. We can see where the laptop is, who is logging in and what software is installed. It also allows us to verify that the laptop's encryption is up to our standard – which is key for regulatory compliance. It has taken us from 30% IT asset auditing capability to well over 95% on computers that are outside our facilities."

Brad Myrvold | Systems Manager of Desktop Technology | Allina Hospitals & Clinics



"Absolute Manage provides new ways to automate the setup and configuration of our machines, so it's safe to say the software isn't just helping us streamline and manage our current process.. It's also enabling us to think ahead and prepare for the future in ways that we haven't had the time or capacity for in the past."

Michael Scarpelli | Technical Support Manager | La Jolla Institute for Allergy & Immunology



"As we began increasing the number of laptops across our organization, we saw a corresponding rise in laptop theft. I was attending a Microsoft training course where a colleague suggested that we investigate Computrace. The more we learned about the product, it became obvious that Computrace could significantly benefit our computer security strategy."

Alison Wells | Manager of Client Services | Community Medical Centers

Endpoint Security

Computrace® Products

Centrally track and secure IT assets within a single cloud-based console. Easily identify computers that have gone missing, enforce software policies, remotely invoke pre-emptive and reactive security measures to safeguard each device and the data it contains.

Absolute Secure Drive

Self-encrypting drives (SEDs) are the latest evolution of encryption, built directly into the hardware of each device at the factory. Absolute Secure Drive provides the console through which you can configure and set up each SED, administer users, authentication methods, policies, and system maintenance through to end of life.

Endpoint Management

Absolute Manage

Manage PC, Mac, iOS, Android, and Windows® Phone devices from within a single console using a Mac or a PC. Remotely perform standard maintenance routines and take strategic and responsive measures based upon the requirements of each device.

Mobile Device Management

Remotely manage iOS, Android, and Windows® Phone devices wirelessly (over 3G or Wi-Fi). Configure, query, and even wipe or lock each device. Manage and deploy profiles to configure email, restrict applications, set up VPN, disable camera and send messages to end users.

For more information visit: www.absolute.com/healthcare

Absolute®Software

www.absolute.com