Built-in Protection in Laptop PCs Improves Compliance with New Healthcare Rules

Absolute Software[1] and Intel deliver a powerful solution for complying with the security requirements of government rules and regulations for the healthcare industry. Computrace,* a leading IT asset-management and data-protection solution from Absolute Software, is taking advantage of Intel® Anti-Theft Technology (Intel® AT),[2] which is designed into the system hardware. The combination of Computrace and Intel AT delivers intelligent, automated, policy-based protection against loss or theft for laptops helping to protect patient data and minimize risk for hospitals who must comply with new rules and regulations. If a laptop is reported lost or stolen, IT can remotely delete data or instruct the system to lock itself down to prevent any OS from booting – from any boot device. If the laptop is off the network, information technology (IT) administrators can be confident of a lockdown – via a local timer that can expire and disable the machine if it doesn't check in with the Absolute Software server in the specified time. Either way, the laptop "bricks" itself. Best of all, even if the hard drive is reformatted or replaced, the built-in, anti-theft security measures remain in place. Getting the system operational again is easy – authorized users can quickly restore the system with a one-time reactivation passphrase provided by IT. IT now has a more reliable, robust approach to securing confidential data, improving compliance, and minimizing financial and/or legal risk from data and system breaches from lost or stolen laptops.

Absolute® Software

intel®

Table of Contents

Executive Summary

In the healthcare industry, keeping patient data secure is not just a challenge, it is a legal necessity. Loss and theft of laptops makes sensitive data vulnerable. Worse, an unauthorized user might use a lost or stolen laptop to access the hospital's computer systems. Healthcare organizations must also comply with increasingly stringent regulations, such as HIPPA and HITECH, to protect patient data and privacy. Compounding the problem is that with more mobile workers, healthcare organizations also need to be able to secure confidential data even when systems are off-site and/or not connected to a network.

Enter Absolute Software's Computrace,*[1] with Intel® Anti-Theft Technology (Intel® AT).[2] An industry leader in security solutions, Computrace delivers a robust solution for tracking assets, performing remote data wipes after a theft, and recovering stolen assets. Intel AT enhances Computrace with timers and poison pills that allow IT to use automated policies to lock down a PC – whether the laptop is on or off the hospital network, and even if the OS is re-imaged, the hard drive is replaced, or the boot order is changed to a different device (such as a USB key, CD, DVD, or another hard drive). When activated, the anti-theft responses block the boot process regardless of the boot device, and render the laptop a "brick" without destroying the data. This protects the system while retaining the data. To reactivate a system that was locked down, the user simply enters a strong, one-time passphrase in the preboot reactivation screen, and the system is returned to its normal working state. Rapid response and recovery is a key advantage for healthcare professionals who might need to quickly continue work once a laptop is recovered. It also allows hospitals to act rapidly to protect patient records, while gaining the time needed to conduct a thorough investigation into the extent of a potential breach.

Computrace with Intel AT can help hospitals maintain the trust clients have in them in terms of managing confidential data. In turn, this can help hospitals retain patients who might otherwise seek out providers with a better track record of protecting data. With Computrace and Intel AT, IT can better protect assets and sensitive data, improve compliance with government and industry rules and regulations, and help reduce losses and business risk.

Client-side protection helps defend healthcare data against breaches

Absolute Software and Intel deliver an integrated solution that helps protect healthcare IT assets and confidential data for hospitals, clinics, and mobile healthcare workers.

Challenges in defending healthcare data

The healthcare industry faces significant challenges in complying with the security aspects of government and industry regulations and rules. For example, for an information technology (IT) administrator at a hospital, the problem of protecting patient data is complex. Confidential patient data must be shared between departments, from patient intake to nurse's stations, from emergency rooms to ICU, and from radiology to therapy. In addition, many medical workers are mobile, including nurse practitioners, midwives, physical therapists, physicians who make rounds at small clinics, and medical researchers at other facilities. Such workers must also have access to patient data in order to provide high-quality care.

Compounding the security challenge is the need to share patient information with non-employee medical personnel, such as non-hospital physicians, visiting specialists, therapists at remote clinics, and technicians at off-site labs. One of the most critical concerns is that a stolen laptop could be used, not only to gain access to patient data stored on the system, but to gain access to hospital systems themselves. IT needs a robust, comprehensive solution to protect patient data, regardless of a laptop's location.

New laws, stricter compliance

Besides the Health Insurance Portability and Accountability Act (HIPAA), hospitals and other healthcare organizations must also comply with the health data breach notification rule, as well as the Health Information Technology for Economic and Clinical Health Act (HITECH). The latter two acts went into effect in 2009.

The new rules changed the regulations for privacy and security of HIPAA. One of the consequences is stiffer penalties, along with requirements that healthcare organizations notify the public when a data breach occurs that violates the privacy regulations. Compliance with these and other government and industry regulations requires that IT administrators have a robust solution to data loss and theft, as well as the ability to track the response and recovery efforts taken to protect patient data.

Confidential data remains vulnerable

Unfortunately, many hospitals are struggling to comply with the new legislation. For example, one of the four main goals of compliance with HITECH is to help hospitals shift from paper-based record keeping to electronic data management. Another goal is to protect identifiable health information from misuse through electronic access. However, as hospitals continue to shift to electronic databases, more data becomes vulnerable to electronic attacks. According to one industry study, approximately 52% of large hospitals, 33% of medium hospitals, and 25% of small hospitals had at least one data breach in 2009.[3] Other industry research, including the Ponemon study, has revealed other critical security issues, such as business risk and consequences of data breaches:

- The average cost of a data breach in 2009 was $6.75M, with the most expensive breach costing $31M to resolve, and the least expensive costing $750,000.[4]
- 92% of IT security professionals reported laptop theft or loss in their organization.[5]
- Lost or stolen laptops result in a data breach 71% of the time.[5]
- Healthcare organizations were responsible for 20.5% of exposed records in 2008 – the second highest percentage, behind only the government/military sector, in data breaches.[6]

The rate at which customers "jump ship" is higher for healthcare organizations

Hospitals are concerned with protecting patient data, but must also be concerned with their reputation. According to the Ponemon study, healthcare organizations and financial services firms were more likely than other types of organizations to lose customers after a data breach. And, healthcare organizations experienced a 6% customer attrition rate (churn rate) after a data-loss incident, as compared to a 5% churn rate for financial services firms, and a 2% churn rate for other industries, such as technology and retail, and 1% or less for manufacturing, energy, and media.[4]

Costs are higher for the healthcare industry

The cost of a data breach is not only significant, but climbing, especially for healthcare organizations. The Ponemon study shows that 36% of all data breaches in the study involved a lost or stolen laptop (or other mobile data-bearing device).[4] The cost of redress and victim-communication activities are also rising, including an the increase in legal defense costs against class action lawsuits that result from customer, consumer, or employee data loss.[4]

- The average cost of a data breach for a healthcare organization was $294 per customer record – about 10% to 20% more than almost all other industries.[4]
- Lost business makes up nearly 50% of the cost of a data breach.[4]

Traditional solutions	Computrace* with Intel® AT	Benefits of Computrace and Intel AT
SW-based	HW/BIOS/SW-based	• Tamper-resistant hardware-based capabilities • Reduces corporate risk • Addresses compliance through flexible IT policies • Allows rapid response to loss or theft, even without a network connection • Allows a controlled, intelligent, client-side response to loss or theft, regardless of the state of the OS, BIOS, or hard drive
No PC disable	Local/remote PC disable	
Relies on network connectivity	Works with and without network connectivity	
Typically relies on OS and/or hard drive	PC Disable (via timer expiry) remains active even if OS is missing or reinstalled, hard drive is reimaged or replaced, or BIOS is reflashed	

Table 1. Advantages of client-side intelligence in theft management

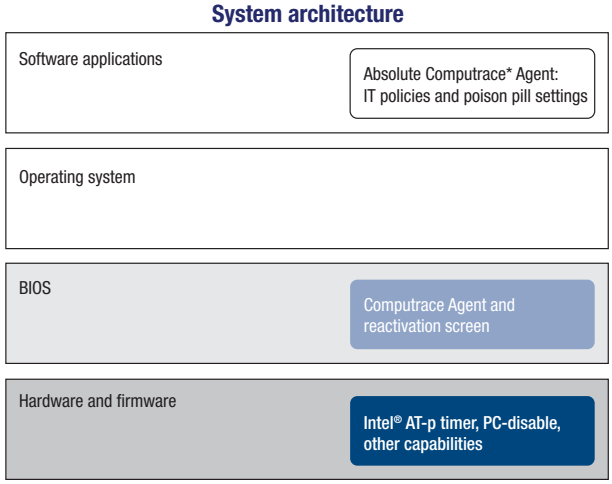

Figure 1. Architecture for Absolute's Computrace,* as enabled by Intel® Anti-Theft Technology – PC Protection

In addition, with recent legislation and its stiffer penalties, violations of state and federal laws can increase those costs with risk of additional legal action. For example, the state of Connecticut recently filed a lawsuit against one of the nation's largest healthcare companies for allegedly failing to secure confidential medical records of over 440,000 patients – and waiting six months before informing consumers and authorities about the breach.[7]

With hackers using sophisticated malware, and 12,000 laptops stolen every week from airports alone, hospitals are asking for help.[5] If they can track the laptop, they can be more confident that it is in their control. If a hospital can't track a laptop, or if IT suspects that a machine is lost or stolen, a rapid response can make the difference between protecting patient data and retaining clients, or exposing data and losing more than 6% of the organization's customers.[4]

Keeping sensitive healthcare data out of the wrong hands

Absolute and Intel have collaborated closely to deliver intelligent client-side protection for healthcare data stored on laptops. Computrace has traditionally allowed IT administrators to remotely delete data from a laptop to help protect it from unauthorized access. Enabled by Intel AT, Computrace now delivers new capabilities (see Table 1) that let IT rapidly lock-down a laptop if the system is lost or stolen to prevent the system from booting. IT can then rapidly reactivate the system once it is back in the hands of an authorized user. Computrace with Intel AT delivers a powerful and comprehensive set of options to respond to loss, theft, or suspicious circumstances:

- **Flag systems** that are or might be lost or stolen.
- **Send a data-destruct command** to erase confidential data, by file, file location, or file type, or by erasing the entire contents of the hard disk.
- **Recover stolen laptops,** with help from the Absolute Theft Recovery Team, and create an audit log that reports which files were accessed after the theft.
- **Disable a laptop** that doesn't check in within an IT-defined period of time.
- **Send a poison-pill** to lock down the laptop (turn it into an unusable "brick") and prevent any OS from booting.
- **Unlock a notebook** once security is reestablished.

Complementing other security measures

Computrace with Intel AT complements encryption layers and other security measures that might be required by government rules and other regulations. For example, Computrace with Intel AT allows IT to establish policies for security responses that range from rapid, client-side, lock-down to full data destruction and the physical recovery of stolen computers. The new security capabilities can integrate with existing encryption solution preboot authentication modules.

Tamper-resistant technology

Because Intel AT is designed into the laptop's hardware (see Figure 1), the anti-theft capabilities are more protected from tampering. The capabilities include timer expiry and PC disable, and do not depend on the OS. This means they can work even if the laptop is not connected to the network, the OS or BIOS is reinstalled, or the

Figure 2. IT can specify different theft responses, as appropriate. For example, a poison-pill lock-down as been requested for user 4, as well as a timer-expiry lock-down.

hard drive is reformatted or replaced. Also, because the Computrace Agent is embedded in the BIOS firmware of most PCs, it can survive hard drive reformats and replacements.[8]

In addition, PC Disable, once activated, also works regardless of boot device – hard drive, USB key, CD, DVD, and so on. For example, a thief cannot simply change the boot order to a USB key and access the system. The laptop will not boot until the strong recovery passphrase is entered.

Rapid lock-down, rapid recovery

When a laptop is lost or stolen, it is critical that IT respond rapidly to a data breach. The priority is to protect patient data and mitigate liabilities and losses, until the laptop can be recovered. For example, if an organization discovers a loss or theft the same day it happens, the average cost of a lost laptop drops to about $9,000.[3] However, if it takes more than a week to find out about the loss, the average cost of that laptop increases to $115,000.[3] Having several options for managing lost systems gives IT the flexibility to respond as necessary.

Use case: Laptop stolen at an airport

In this case, a neurology specialist (Dr. Bartlett) is traveling to an international conference, and her laptop is stolen at the airport. Dr. Bartlett immediately calls IT, and the administrator flags the laptop in the central database (see Figure 2).

As is typical, the thief does not wait long to power up the laptop and connect to the Internet to find out if the system is working and what kind of data is on it. However, protected by Computrace with Intel AT, the laptop begins its check-in with the Computrace Monitoring Center. As soon as the laptop checks in, it receives the poison pill set in the server by IT. The laptop then disables itself to prevent a reboot. To the thief, the rendezvous (check-in) process is invisible. All the thief sees is that when the system reboots, it is inoperable – it won't load the OS.

PC disable – a preboot capability

The PC disable capability is triggered before the system boots. Because the capability is designed into the laptop's hardware and activated preboot, it works even if the OS or BIOS is reinstalled, other security solutions have been removed, or the hard drive has been reformatted or replaced. Because the capability is activated preboot, even if a thief tries to boot from another device (hard drive, USB key, CD, DVD, etc.), the poison pill remains in effect, blocking the boot process itself. This is why a laptop can remain locked down even if another boot device is installed.

Timer expiry provides intelligent local response

One of the key problems with laptop security is that anti-theft software-only products can be installed and uninstalled relatively easily. Software-only approaches also require that the OS is loaded and working properly, which means that the anti-theft

	Time expiry	Poison pill	Reactivation
Network Required?	No	Yes	No
Mechanism	Local, hardware-based timer expires if not reset by central server at specified interval.	Poison pill flag is set in central server. Poison pill is then automatically delivered to laptop when laptop connects to Internet.	One-time recovery token is entered in the reactivation (pre-boot) screen. Timer is reset; system can boot to its normal working state.
Effect	PC boot process is blocked.	PC boot process is blocked.	N/A
Data destroyed?	No	No	N/A
Recovery	Full system recovery via strong reactivation passphrase.	Full system recovery via strong reactivation passphrase.	Full system recovery via strong reactivation passphrase.
Benefits	Fully automated, policy-based response – no IT interaction required, no network required.	Rapid, flexible, policy-based response.	Easy, fast recovery.

Table 2. Intel® Anti-Theft Technology (Intel® AT) features

software fails if the OS is compromised or inoperable. In addition, if a laptop has a software-only agent, a thief can often circumvent the agent by reformatting or replacing the hard drive to make the laptop usable again. Or the thief can remove the hard drive to another system to access the data on that disk. The result is that IT cannot be confident that patient data on a laptop is secure if the laptop is not controlled by the authorized user.

Enabled by Intel AT, Computrace provides a local, intelligent and automated response to suspicious circumstances through the use of hardware-based Intel AT timers. When the timer expires, the laptop becomes inoperable.

How does it work?

Intel AT timers establish rendezvous requirements for laptops. A rendezvous is an authorized check-in via the Internet with the theft-management server, such as the Computrace Monitoring Center. This check-in must occur within the IT-defined time period. If the timer expires, Intel AT identifies a suspicious circumstance and blocks the machine's boot process. When locked down, the laptop cannot boot any OS from any boot device, including hard drive, USB key, CD, DVD, or other device.

Because the expiry timer is built into the laptop hardware, it works even if the laptop does not connect to the network to receive other instructions from IT. For example, the timer can work if central server communication is disabled via port blocking, or the agent is prevented from running. The timer can continue to work even if the OS is reinstalled, the BIOS is reflashed, other security solutions have been removed, or the hard drive has been reformatted or replaced. Even if a thief tries to boot from a secondary device, the boot process won't work. For example, since the timer disables the laptop's boot process, replacing the hard drive does not circumvent the blocked boot.

Use case: Undetected theft, but missed check-in locks down laptop

In this case, a physician (Dr. Andrews) is leading a pilot study for a new cardiovascular medical device. When Dr. Andrews leaves to speak at a medical conference, he forgets to lock his office, and his laptop is stolen from his desk. The thief does not immediately power up the laptop, but hides it in a safe, temporary place until it can be moved to a better location. Since Dr. Andrews will be gone for several more days, the theft is not immediately noticed.

In this example, IT policy is that the laptop must check in with the Absolute Software Monitoring Center each day to upload its asset information. After being stolen, the daily check-in was missed. The next time the laptop powers up, it enters "theft mode." The laptop then disables itself. Even if the thief tries to power up the system later, the OS will not boot, so use of the laptop is thwarted.

Data protection during lock-down – rapid and easy recovery

Computrace has traditionally provided IT with powerful mechanisms to remotely erase sensitive data if a laptop is lost or stolen. Although erasing a single file can be done quickly, erasing all files of a particular type or destructively overwriting the hard disk can take some time. The longer the system remains active, the more time an unauthorized user has to try to access patient data – and the more costly the data breach.

In addition, there are many cases in which a laptop might not be in the control of the authorized user, but it is not stolen, only "missing." For example, a nurse might accidentally leave a laptop behind at a clinic and return for it the next day, or a specialist might forget a laptop after a consult and have it delivered to him later. In such cases, the indicators for a destructive data erase might be a false positive – not fully warranted. Worse, a destructive response could require a lot of time for restore tasks – rebuilding the OS, restoring user files (if there were back-ups available), restoring user settings, and so on.

Enabled by Intel AT, Computrace allows IT to lock down a potentially missing system without a destructive data wipe.

Allina Hospitals & Clinics

Headquartered in Minneapolis, Minnesota, Allina Hospitals & Clinics (Allina) is an organization of 11 hospitals. The organization employs 23,000 people to provide healthcare services in Minnesota and Western Wisconsin.[10]

Allina has an extensive fleet of 3,800 mobile PCs. For the IT team however, the increase in mobile systems presents a challenge in managing systems and protecting patient data, with critical ramifications.

Having experienced a sharp increase in laptop theft – including an incident that required public disclosure of breached health information, Allina looked to Computrace with Intel AT for a high-tech solution for managing the systems and protecting against data breaches.

"Because of the sensitive nature of our patients' information, we must have the highest level of protection against theft or data breaches," says Brad Myrvold, Manager of Desktop Technology at Allina. "If a computer is lost or stolen, Computrace with Intel AT is a lifeline. If we are concerned about the information on a laptop, we use Computrace to remotely delete the data. Even if the machine is out of reach, we can still 'brick' the system through a local timer. This is a very effective tool for protecting confidential data and reducing risk."

Because data is not destroyed (just blocked) during a lockdown, recovery can be rapid and easy. The user simply enters a strong, one-time passphrase in the reactivation screen – the only screen available after a lock-down. Entering the passphrase resets the local timer(s) and allows the system to boot to its normal working state. This provides IT with a simple, inexpensive way to restore a laptop without compromising patient data or the laptop's other security features, such as government-required encryption.

For systems that are indeed stolen, IT can work with the Absolute Theft Recovery Team of law enforcement experts, investigate the theft, catch the thief, and recover the device. If theft recovery proves difficult (for example, the laptop has been taken to another country), IT can "brick" the system to make it inoperable.

Customizing the lock-down screen

Computrace makes it easy to customize the pre-boot lockdown screen with a customized message that is downloaded with the poison pill. If the machine is returned to the user, and the user tries to boot their own laptop, they might see a preboot reactivation screen with a message such as, "This laptop has been reported lost. Please call (phone number) to return the system."

Traditionally, Absolute has been able to recover 3 out of 4 stolen laptops that call in to the Absolute Software Monitoring Center.[8,9] This high rate of recovery is one of the advantages of Absolute security solutions. Adding customized lock-down screens makes it even easier for users to return to work once a missing laptop is found.

Key advantage – Compliance with health data breach notification rule

A key aspect of the data breach notification rule is that, if confidential data remains protected – if the loss of data does not pose a significant risk or cause significant harm, the organization is not required to notify the public or other agencies of the breach. With the cost of a data breach so high – including the loss of patients – the rule provides even more incentive for hospitals to implement robust anti-theft technologies that help prevent unauthorized access to patient data.

However, moving too quickly in response of a breach – especially during the detection, escalation, and notification phases – can cause inefficiencies that actually increase costs.[4] For example, the Ponemon study showed that healthcare companies who notify patients too quickly of potential exposure of records paid 12% more than other companies.[4]

Computrace with Intel AT provides a robust method to comply with the new rules without incurring unnecessary costs. First, Computrace can delete confidential data and determine whether it has been accessed by thieves. Computrace can also provide a record of which data was deleted and the time of the deletion. Computrace with Intel AT can then "brick" the laptop to help protect the system even after it is lost or stolen. Again, Computrace automatically logs when a poison pill was successful and/or the expected time the Intel AT timer will expire and lock down the PC. Finally, after a laptop is recovered, Absolute Software's forensic team can examine the PC to see if confidential files were actually accessed while the laptop was in unauthorized hands. This helps hospitals minimize risk, avoid costly and premature notifications of unauthorized data access, and gain the time to respond appropriately with a thorough investigation of the breach.

Use case: End-of-life disable while still protecting patient data

The Absolute Computrace solution is also effective at the end of a PC's life cycle to protect sensitive data that might be left on a system that is being discarded.

IT simply uses Computrace to trigger a full system data-destruct. Once the data on the hard drive is erased, IT can further disable the system using the poison pill feature enabled by Intel AT. Only an authorized IT administrator can then unlock the PC for reconfiguration or some other authorized use.

Easy deployment

Computrace with Intel AT can be installed and activated locally, before the PC is deployed to the user. Computrace with Intel AT can also be installed and activated remotely, like a typical patch or other software update via IT's existing deployment application. Select models of laptops will ship preconfigured, or "ready," for Intel AT. IT administrators simply install and activate the Computrace Agent to manage the laptops as usual, before or after deploying them to users.

Protecting patient data and defending against unauthorized access to hospital systems

With Computrace and Intel AT, healthcare IT administrators can protect patient data and hospital systems even after a critical laptop is lost or stolen. Laptops can also be secured even if the theft or loss is not realized immediately, whether or not the system is connected to the Internet or network, and regardless of the state of the OS, BIOS, or hard drive. With Computrace and Intel AT, IT has a rapid, inexpensive way to reactivate a "bricked" laptop and also return it to its normal operating state. This enhanced protection extends IT's security capabilities on and off the network to protect assets and confidential data, improve compliance, and minimize business losses and risk.

To learn more about Intel Anti-Theft technology, visit: **www.intel.com/technology/anti-theft**.

For more information about Absolute Software products that support Intel AT, visit: **www.absolute.com/intel**.

Absolute® Software

intel®

[1] All information about Absolute Software was provided by Absolute Software.

[2] No computer system can provide absolute security under all conditions. Intel® Anti-Theft Technology (Intel® AT) for PC protection (also referred to as the 'poison pill' in some documents) requires the computer system to have an Intel AT-enabled chipset, BIOS, firmware release, software and an Intel AT-capable Service Provider/ISV application and service subscription. Intel AT (PC Protection) performs the encrypted data access disable by preventing access to or deleting cryptographic material (e.g. encryption keys) required to access previously encrypted data. ISV-provided Intel-AT-capable encryption software may store this cryptographic material in the PC's chipset. In order to restore access to data when the system is recovered, this cryptographic material must be escrowed/backed up in advance in a separate device or server provided by the security ISV/service provider. The detection (triggers), response (actions), and recovery mechanisms only work after the Intel AT functionality has been activated and configured. The activation process requires an enrollment procedure in order to obtain a license from an authorized security vendor/service provider for each PC or batch of PCs. Activation also requires setup and configuration by the purchaser or service provider and may require scripting with the console. Certain functionality may not be offered by some ISVs or service providers. Certain functionality may not be available in all countries. Intel assumes no liability for lost or stolen data and/or systems or any other damages resulting thereof.

[3] Source: 2009 HIMSS Analytics Report: Evaluating HITECH's Impact on Healthcare Privacy and Security sponsored by ID Experts, November 2009. http://www.himssanalytics.org/docs/ID_Experts_111509.pdf.

[4] Source: The Cost of a Data Breach, The Ponemon Institute, LLC, January 2010.

[5] Source: The Cost of a Lost Laptop, The Ponemon Institute, LLC. April 2009.

[6] Source: Identity Theft Resource Center 2008 Data Breach Stats, Identity Theft Resource Center (ITRC), January 2, 2009. http://www.idtheftcenter.org/artman2/uploads/1/ITRC_Breach_Stats_Report_2008_final.pdf.

[7] Source: Connecticut Sues Health Net For Data Breach Involving 446,000 Patients, All Headline News, January 19, 2010.

[8] For a list of PCs with Computrace embedded in the BIOS firmware, visit www.absolute.com/firmware.

[9] Source: The Absolute knowledge base.

[10] All information about Allina Hospitals & Clinics was provided by Allina Hospitals & Clinics.

0210/WW/OCG/XX/PDF

♻ Please Recycle

Order Number: 323461-001US