BOSTON MEDICAL CENTER

EXCEPTIONAL CARE. WITHOUT EXCEPTION.

*Wave Systems' EMBASSY® software enforces centrally managed and unrivaled data security for the hospital's 400 laptops.*

# Boston Medical Center

## Industry

Healthcare

## Benefits Summary

- Eliminates the IT overhead and costs associated with configuring and maintaining software-based encryption.
- Increases security with foolproof key protection and centralized policy control of SED security features
- Transparent to end users with zero impact on system or application performance
- Provides proof of compliance with the newly revised HIPAA and HITECH regulations for protected health information

*Storing and exchanging data electronically has enabled healthcare providers to accelerate patient care, expand opportunities for collaboration and streamline administration costs. But with these benefits come risks. Digitally stored medical histories, billing information and clinical trial data are all more susceptible to online attack and theft. Plus, increasing laptop use by medical and administrative staff has put more and more data beyond the relative safety of the network firewall.*

*Data breaches continue to increase in every industry. But the healthcare sector has been among the hardest hit — representing almost one out of every six breaches in 2009. That ratio rose to almost one in four in 2010. And the costs are staggering. The economic impact of a single data breach is approximately $2 million, according to the Ponemon Institute.[1] The total collective impact on US hospitals over two years is estimated to be $12 billion, according to the same study.*

*Driving these costs is the fact that federal and state regulations don't make a practical distinction between lost and stolen data. If a laptop goes missing, healthcare providers can expect to pay stiff fines and other costs under the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act. Yet, even today, many healthcare organizations have not made protecting patient data a top priority.*

## THE CHALLENGE:

*Provide full-disk encryption (FDE) on 400 laptops while minimizing impact on computer performance as well as the time and cost required for IT maintenance.*

As one of New England's leading healthcare institutions and an early adopter of electronic medical records, Boston Medical Center (BMC) was quick to recognize the benefits — and risks — of electronic information. Generally, the hospital discourages staff from storing sensitive data on its fleet of 400 laptops. However, the 639-bed licensed academic medical center also serves as a teaching affiliate for the Boston University School of Medicine. So, IT employees recognized that BMC staff would often need to transport patient records, clinical and pharmaceutical trial data and even billing information beyond the relative safety of the hospital's network firewall.

"Between due diligence, federal regulations, and a desire to avoid the ugly headlines that invariably follow a data breach, BMC started putting controls in place to help mitigate the risks involved with laptops and mobile devices," said Mark Mulvaney Jr., a Network Security Engineer in BMC's IT department.

[1] Ponemon Institute, Benchmark Study on Patient Privacy and Data Security, Nov. 2010.

Early on, that meant equipping laptops with aftermarket full-disk encryption (FDE) software. But Mulvaney found this to be a problematic solution. For one, software encrypted laptops remain vulnerable to attack and, thus, do not fully address data breach regulations requiring providers to guarantee the security of data on a lost or stolen laptop.

Further, software FDE solutions were time consuming to install and configure, and they put a significant drag on a laptop's operating resources, which led some users to disable the encryption altogether, without the knowledge of BMC's IT department.

"When you first install software FDE, it's not that bad," said Mulvaney. "But after installing a few patches and updates, laptop performance degrades exponentially. Six months down the road, it gets bad enough that you're looking at reimaging the laptop, after which you need to install the FDE software again and redo the encryption — a process that can take half a day."

## THE SOLUTION:

*Self-encrypting hard drives managed with Wave Systems' EMBASSY Trusted Drive Manager and EMBASSY Remote Administration Server (ERAS).*

All of these issues motivated Mulvaney to advocate that BMC replace software encryption on its laptops with self-encrypting hard drives. Available from Dell, BMC's laptop vendor, self-encrypting drives (SEDs) store encryption keys within the drive hardware itself. Since the keys never leave the drive, SEDs are not susceptible to traditional software attacks. In addition, they impose no drag on a laptop's operating resources, ensuring ironclad data security that never distracts end users.

Mulvaney also recognized that a complete data protection solution required more than encryption. It also required simple activation of encrypted drives. His search for a solution led him to Wave Systems, a leading provider of encryption management solutions. Wave's EMBASSY software transformed BMC's self-encrypting drives into a complete managed enterprise encryption solution: one that centrally provisions security policies, limits access to only authorized users and — perhaps most importantly — provides proof that data remains safe in the event of a lost or stolen PC.

## THE BENEFITS:

*Quick to install, simple to administer and virtually impossible to penetrate data security. Plus, the ability to remotely control security policies from a central location.*

BMC cost-effectively phased in SED-equipped laptops by replacing legacy equipment that came in for regular maintenance or service. After two years, the hospital had upgraded nearly half of its laptops. Hence, the most immediate impact of the new technology was felt by IT staff, who spent far less time installing and configuring encryption.

"With FDE software, such activities averaged half a day," said Mulvaney. "Hardware SEDs managed by Wave software take about 30 minutes to set up. Plus, it's simple enough that I can now delegate administration tasks, such as provisioning, to IT techs."

Many benefits of Wave-managed SEDs are illustrated by what happens less, or not at all. For example, Mulvaney reported a notable drop in help desk calls about slow computers once the hospital switched to hardware-based encryption. While that suggests fewer users feel they need to switch encryption off to improve laptop performance, it's more likely they're unaware of the transparent, yet superior, data security on their laptops. More to the point, users are now unable to disable encryption of their drives.

Such management functions are only available to centralized IT staff via Wave software. Wave's ERAS software provides all the administration, reporting and access control BMC requires for policy-based security.

Other events less likely to occur with Wave software are the heavy fines and negative headlines that often follow the loss or theft of a laptop. SEDs controlled by Wave provide an audit trail required for data privacy compliance regulations. That means BMC can now ensure superior data protection, and still prove a laptop was encrypted if and when it is lost or stolen. This proof is critical to achieve "Safe Harbor" from stiff fines, public disclosure, and negative publicity for the hospital and Boston University.

Wave Systems Corp.
480 Pleasant Street, Lee, MA 01238
(877) 228-WAVE • fax (413) 243-0045
www.wave.com

wave®
Simplifying Encryption and Authentication