



Customer

Baptist Memorial Health Care

Challenge

To provide Baptist Memorial Health Care's employees with a standard-issue USB storage device that secures mobile data and offers 100 percent privacy via data encryption and password protection.

Solution

Kingston® DataTraveler® Elite -- Privacy edition (DTEP)USB Flash drive

Results

- Employees can safely back-up data from their local workstations, securing 100 percent of data on-the-fly through 128-bit hardware-based AES encryption
- User-friendly interface eliminates the need for IT intervention, freeing up valuable resources
- In the event the USB drive is lost or stolen, a complex password protocol and fail-safe security mechanism locks out would-be attackers after 25 failed password attempts
- Compliance with HIPAA and other regulations

Kingston® DataTraveler® Elite -- Privacy Protects Sensitive Data; Promotes Regulatory Compliance at Baptist Memorial Health Care

Regarded as one of the premier health care systems in the nation, Baptist Memorial Health Care is an award-winning network dedicated to providing compassionate, high-quality care for patients. With 14 hospitals throughout the mid-South, Baptist combines convenience with excellence of care -- two reasons the healthcare organization has been named among the top health care systems in the country for several years.

In response to the Health Insurance Portability and Accountability Act (HIPAA) legislation, which mandates privacy, security and authentication of all patient data, Baptist Memorial Health Care completed an evaluation of its organizational data storage processes, and found widespread use of local storage solutions, such as USB and thumb drives, on a departmental level.

Knowing that the confidentiality of certain data could not be guaranteed on file servers that were accessible to anyone with administration rights, some departments had begun using these local storage devices to house patient and employee records, physician credentials, infection control incident reports and other data. While Baptist Memorial Health Care's Information Services (IS) department did not endorse this use of local data storage, it was unable to provide a viable universal back-up solution.

However, the widespread use of flash memory sticks, iPods and other portable storage devices only left Baptist Memorial Health Care more vulnerable to the loss of sensitive patient data. Worse yet, the health care organization faced the risk of violating the same federal privacy and security regulations that they were trying to comply with by locally storing sensitive data.

“Baptist Memorial Health Care does not permit the use of recordable optical drives; floppy disks do not store a significant amount of data; and, while USB drives offer immense storage capacity, they leave the organization open to risk in terms of data loss and the spread of viruses and other external threats,” said Lenny Goodman, IT director for Desktop Management, Baptist Memorial Health Care. “We needed a solution that would provide all of our employees with a standard-issue storage device that offered data encryption and password protection features.”

Laying the Groundwork for Preventing Data Loss

Goodman had two specific needs when it came to finding a storage device that would protect patient data and other sensitive information – 100 percent of the data had to be encrypted, and password protection was mandatory. In addition, Goodman wanted a solution that was plug-and-play, and offered a user-friendly interface that would ensure fail-safe security best practices without IT staff intervention.

Before Goodman could procure a solution that would meet these needs, he had to raise executive awareness of the situation. Once the hospital’s management was on-board, he worked with the communications team to develop an official, enforceable written policy regarding the use of USB drives.

It was now up to Goodman to audit and secure endpoint connections throughout the hospital so that non-secure devices would be disabled, and to replace these non-secure devices with a standardized USB storage solution.

Kingston and Safend: A Prescription for Success

As Goodman searched for the ideal USB storage solution, he found that there were a number of devices on the market that offered encryption, password protection and other security features, yet none offered 100 percent data encryption coupled with mandatory password protection.

To find a solution that would meet these specific requirements, Goodman engaged Safend, a leading international provider of end-point security solutions. It is through Safend that Goodman was introduced to Kingston’s DataTraveler Elite -- Privacy (DTEP) edition.

Baptist Memorial Health Care was one of the first organizations to deploy Kingston’s DTEP. In fact, the healthcare organization served as beta test site for the USB Flash drive. It was during this phase that Goodman and his team of IT professionals

collaborated with Kingston, adding features that were needed to meet Baptist Memorial Health Care's requirements.

As a result of this cooperative effort, when DTEP was introduced in March 2006, it became the industry's first fully-secure USB drive to offer 100 percent privacy, automatically encrypt data on-the-fly using 128-bit AES hardware encryption, and permit users to view encrypted files without the need for additional software. In addition, the entire drive is protected by a complex password protocol mechanism that locks out would-be attackers after 25 failed password attempts.

In addition to its encryption and password protection features, Goodman was also pleased to find that Data Traveler Elite -- Privacy does not install any software on the host machine, thereby helping Baptist Memorial Health Care avoid lock down issues that already prevent users from installing software programs on corporate machines.

For Goodman, though, preventing security risks was only part of the equation. In order to curb the inappropriate use of corporate resources, he deployed Safend's Protector software in conjunction with Kingston's DTEP.

Safend Protector software controls connectivity among peripheral devices and desktop and laptops, enabling IT managers to set granular policies dictating which devices – via type, model, and unique serial number – can be used within the organization, and/or for any particular domain, department, computer, or user.

The combination of Kingston's DTEP and Safend's Protector software provides Baptist Memorial Health Care with an innovative and comprehensive solution to address security concerns regarding removable media and peripheral devices.

"Safend's auditor and protector capabilities help us to comply with HIPAA data accountability requirements by identifying all end-point devices used within our network, detecting the use of approved USB devices including Kingston's DTEP, and protecting our network against the use of unapproved devices. The Kingston-Safend solution really meets our needs for security and ease-of-use," said Goodman.

Conclusion

To date, Baptist Memorial Health Care has deployed 100 DTEP USB drives across its vast network, and has plans to implement an additional 500 to 700 units through 2007. Baptist Memorial Health Care employees are using the USB drives to back-up data stored on local workstations, and in the transfer of data from networked machines to and from off-network machines used for R&D purposes.

The benefits of DTEP do not end with the outstanding security features or user-friendly interface. "We expect that with Kingston's secure USB drives, our organization will experience significant long-term cost savings by averting penalties for non-compliance

with HIPAA and other regulations, as well as the costs associated with data loss,” said Goodman.