



**Mobilizing Healthcare Data  
with Secure USB Flash Drives**  
to Protect Patient Privacy and Security

**SanDisk®**



## **WITH MILLIONS OF USB FLASH DRIVES IN USE,**

digital data is constantly on the move. Flash drives let private users easily store, transport and share their photos, videos and text files. But in the world of healthcare, the very same benefits that enable employees to work effectively outside the office pose risks of the loss, theft or misuse of unprotected, confidential data.

The SanDisk® Cruzer® Enterprise USB flash drive with Central Management & Control (CMC) Server Software provides users with unparalleled safety and security in storing and managing sensitive patient information.

## **Combating Data Loss**

Today's headlines recount the grim realities of various healthcare institutions and private organizations losing data or having their data compromised. In January 2008, it was reported that a mobile device stolen from a regional health

insurance provider exposed over 300,000 customers' personal information<sup>1</sup>. This is just one recent incident in a long line of data breaches in the healthcare industry resulting in the potential leak of millions of patients' personally identifiable information.

The extremely devastating consequences of data compromise and security breaches are no less severe with smaller but more frequent data losses. Research by the Ponemon Institute has established that, on average, a single loss of 30,000 customers' personally identifiable information costs an organization nearly \$6 million in internal investigation, customer notification and regulatory compliance expenses<sup>2</sup>.

In addition to direct financial consequences, the health and welfare of patients can be at stake. The unauthorized access or disclosure of sensitive patient information can be terribly embarrassing, compromise employment status and lead to expensive civil litigation.

## **Satisfying Industry Requirements**

For healthcare companies, delivering better patient care, more efficient treatments and higher quality services requires access to enormous amounts of patient data held in disparate locations. Confidentiality of patient data has always been a paramount concern among health workers and patients themselves. The implementation of healthcare regulations such as the Health Insurance Portability and Accountability Act (HIPAA) now has made this concern a legal obligation. All patient data must be both secure and accountable.

The use of USB flash drives to transfer and access medical records to the point-of-care, or from various data repositories, is a vital aspect of patient care. Yet most USB flash drive solutions have no mechanisms to ensure data confidentiality and compliance with regulations. Healthcare providers need a practical way to monitor all data and protect it against loss or unauthorized access, without giving up the ease-of-use and the continued productivity facilitated by USB flash drives.

Multiple regulations impacting healthcare organizations now require encryption. HIPAA addresses the need for encryption of confidential patient information. PCI/DSS necessitates encrypting credit card information, used widely throughout the industry. For healthcare organizations impacted by Sarbanes-Oxley, financial information must be encrypted when other compensating controls are missing – virtually always the case with regards to USB flash drives.

## The Total SanDisk Solution: Central Control, Increased Protection

SanDisk Cruzer Enterprise USB flash drive with SanDisk Central Management & Control (CMC) software is designed to meet the requirements to comply with industry regulations, such as HIPAA and Sarbanes-Oxley (SOX), for the secure storage of sensitive information.

CMC is an innovative server software solution that utilizes the unique hardware and embedded software capabilities of Cruzer Enterprise USB flash drives. The CMC device agent resides on the USB drive, enabling corporate IT departments to centrally manage company-issued Cruzer Enterprise USB flash drives locally and remotely, within and outside the healthcare environment.

CMC provides many functions that include constant monitoring, auditing and tracking. Depending on an organization's particular needs, these functions can incorporate various parameters set for various levels of restrictions and monitoring.

Attaining centralized deployment and provisioning is another feature with tremendous benefits. Management can obtain centralized updates and configurations of drive parameters, remote password administration and remote deactivation of lost or stolen drives through implementation of optional SanDisk CMC software.

Central Management & Control (CMC) software:

- Manages the complete lifecycle of company issued USB drives
- Protects against unauthorized use of sensitive company data
- Protects against possible regulatory compliance failure and associated damages caused by data breaches due to lost or stolen USB drives
- Supports regulatory compliance by tracking and auditing activity, as well as demonstrating the use of strict encryption measures

## Encryption That Ensures the Ultimate Protection

SanDisk Cruzer Enterprise USB flash drive uses powerful, hardware-based 256-bit AES encryption, the most secure block cipher encryption standard adopted to date, complex password protection and a lock-down mechanism when a set number of incorrect password attempts is exceeded to ensure that data on lost or stolen drives cannot be hacked into. These security features enable physicians and other key healthcare providers to transfer data freely, even when sensitive information needs to be transferred to different computers or workstations.



## Increasing Productivity

Organizations do not want to be forced to choose between mobility, ease of use, productivity and security. Complex mobile encryption that is not embraced by users decreases security and hinders worker efficiency. The SanDisk Cruzer Enterprise USB flash drive increases overall enterprise data security by providing centrally managed, secure mobile storage that is transparent to the end user. In this way, both productivity and security remain at high levels.

## Privacy Monitoring Throughout the System

The Cruzer Enterprise USB flash drive, when managed by CMC software, is designed to provide continuous data protection all the way to the point-of-care. Circumventing reliance on the user through mandatory 100% data encryption of all files helps prevent human error. Incorporating security software that cannot be modified or deleted, the Cruzer Enterprise flash drive affords tremendous safeguards. It also supports usage policies that allow for a restricted operating environment to prevent drives from operating on unauthorized PCs. Protection this thorough is essential to not only meet legal requirements but to provide healthcare employees and their patients with peace of mind.



# Mobilizing Healthcare Data with Secure USB Flash Drives

to Protect Patient Privacy and Security

## Key Mandates to Protect Data in Healthcare

**HIPAA** Section 164.312, Technical Safeguards specify a mechanism to encrypt and decrypt electronic protected health information.

**Payment Card Industry / Data Security Standards (PCI/DSS)** requires encryption of credit card data. (Ver 1.1, Section 3), an increasingly popular method of payment to health care providers.

**Sarbanes-Oxley Section 404** requires attestation of documented controls for all financial systems, applicable to publicly traded health care companies.

## Solution Highlights

- Manages the complete lifecycle of company issued USB drives
- Protects against unauthorized use of sensitive company data
- Avoids the regulatory and market repercussions caused by data breaches due to lost or stolen USB drives
- Adheres to regulatory compliance by tracking and auditing activity, as well as demonstrating that strict encryption measures are in place

## How to Contact Us

**SanDisk Corporation**  
Corporate Headquarters  
601 McCarthy Blvd.  
Milpitas, CA 95035

For more information, please go to  
[www.sandisk.com/enterprise](http://www.sandisk.com/enterprise)  
or e-mail [enterprise@sandisk.com](mailto:enterprise@sandisk.com)

<sup>1</sup> The Star-Ledger, "Health insurer says stolen laptop had customers' data," Ted Sherman, Jan 29, 2008

<sup>2</sup> Price Waterhouse Coopers, "Quarterly in law," Feb 2008, p. 3, [http://www.pwc.co.uk/pdf/quarter\\_in\\_law.pdf](http://www.pwc.co.uk/pdf/quarter_in_law.pdf)

SanDisk and the SanDisk logo are trademarks of SanDisk Corporation, registered in the United States and other countries. TrustedFlash is a trademark of SanDisk Corporation. microSD and SD are trademarks. Other brand names mentioned herein are for identification purposes only and may be trademarks of their respective holder(s).