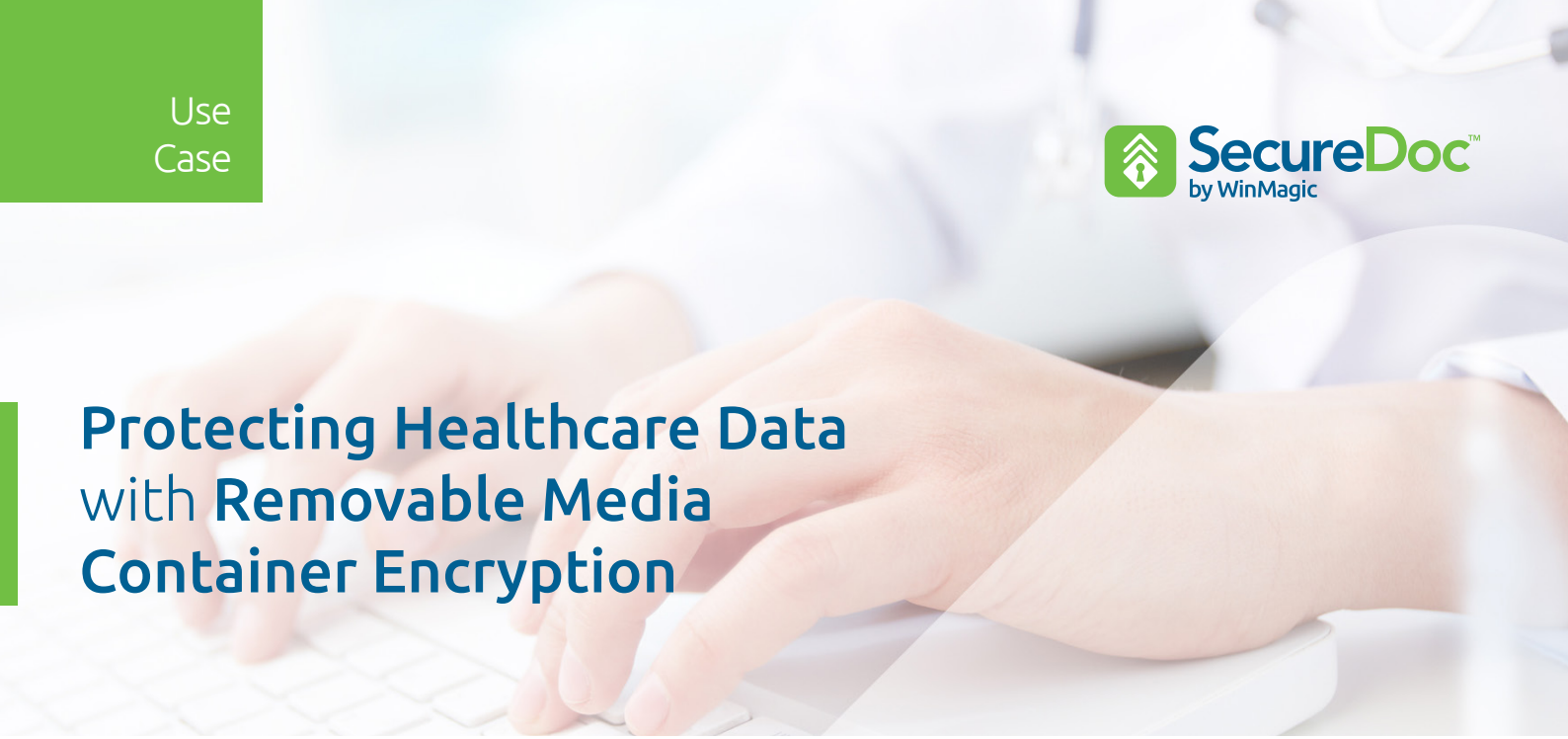
Use Case

SecureDoc™ by WinMagic



Protecting Healthcare Data with Removable Media Container Encryption

Healthcare professionals need to have access to patient information wherever they are in the building. That access needs to be fast, simple, transparent, and most of all highly secure.

Business Challenge

Healthcare Providers are the stewards of significant volumes of sensitive data including the names, healthcare numbers, address, gender, race, date of birth, x-rays and other medical history of patients. With the ease in which data flows across networks of healthcare centers, and the risk inherent in allowing such a large audience of personnel to have access to highly sensitive data, organizations need to be confident that a patient's record is secure whenever it is being transported or stored. And, with increasing data privacy compliance requirements and the fines attached with a compliance failure, there is no justifiable reason not to encrypt data at every point within the business it's simply a healthy data security practice.

Portable Media

Unfortunately, for some healthcare providers, trying to cohesively manage data security and access across a large hospital can be particularly trialing, often leaving gaping holes in protection – especially when it comes to use of portable storage devices by its employees. Most if not all healthcare providers restrict their use, prohibiting personally-owned removable media in systems owned or operated by the organization.

In some organizations, USBs or removable media containers (RMCs) are used for both short term file transfers and more importantly, as a means of authentication on shared devices. Many of these USB devices rely on password protection, which comes with an inevitable volume of costly password resets due to forgotten passwords, password loss, or breach. Organizations need a simpler and more secure way to manage removable media containers, and rights management to ensure that users have seamless and secure access to data critical to performing their highly-sensitive work.

Compliance Challenge

Data security has become especially critical to the healthcare industry as the frequency of breaches continues to rise. Patient privacy hinges on data security regulations, like the Health Insurance Portability and Accountability Act (HiPAA) to drive compliance. However, compliance is not a one-time project – rather, it's an ongoing effort requiring regular risk assessments, compliance monitoring and workforce training. Unfortunately, not having a simple and secure means to encrypt removable media containers, and therefore relying on less secure means of protecting data, could result in a very costly breach, or regulatory compliance failure.

SecureDoc by WinMagic

USE CASE SCENARIO

Industry
Healthcare

Common Pain Points

- Complexity in managing data security across device portfolios
- Shared devices left accessible in open public spaces
- Shared devices have multiple users sharing PINs
- Improper file access
- Password resets are inconvenient and costly
- Fear of failing compliance if devices or passwords are breached or lost
- No plan/assurance of persistent encryption during data movement

Challenges

- No current continuity in encryption solutions (where existing) across the organization
- Customer needs better rights management
- Customer had no good solution for password passthrough to RMCE

WinMagic Solution

• SecureDoc Enterprise (FDE)

SecureDoc Features

Industry-leading Drive Encryption: Protect all data and the OS with FIPS 140-2 validated SecureDoc Full Drive Encryption (FDE)

Robust RME & Device Controls: Enable automatic, enforced encryption of removable media devices – including portable drives, USB, CD/DVD, SD Cards

Pre-Boot Network Authentication: Keep data safe by ensuring devices are booted only when on your network

Enterprise Manageability: Operation, management and recovery of encrypted devices possible within a single console

Technical Solution

Comprehensive Encryption

Compatible with Microsoft Windows, Mac and Linux platforms, SecureDoc's enterprise-class 'always-on' full-disk encryption protects all data stored on servers, desktops, laptops and removable media, such as USB thumb drives and CD/DVDs, and virtual and cloud environments. SecureDoc offers healthcare providers a single, unified console to manage data and device protection – combining industry-leading endpoint encryption with robust device and port controls to significantly reduce the threat of data loss of ePHI.

SecureDoc simplifies any combination of sector-based full-disk encryption, file-and-folder encryption, container encryption and self-extractor encryption deployment, not only making it easy to customize data protection to meet specific security protocols, but also 'future-proofs' their investment in encryption.

Simple and Transparent

SecureDoc makes encryption easy. Users can simply insert the encrypted ISB on any approved device and immediately have access to the encrypted data available to them. As an example, File Explorer will open and show their files immediately without needing to wait for a password prompt, etc.

User-Specific Key Management

For shared devices, like mobile laptop carts and USBs, SecureDoc provides the required methods to partition access across its user base, well beyond a simple password or PIN. And, if those devices are found, dropped or removed from premises, they will ultimately be unreadable to unauthorized users.

SecureDoc's Intelligent Key Management provides secure, centralized management of encryption keys, shared key access, or password-protected access policies via application or web-based console with role-based access to ensure separation of duties. SES manages individual user credentials and keys for authorized users and processes linked to AD or LDAP.

How RMCE Works

- Healthcare professionals' key profiles are loaded to the device, including any approved group key profiles
- Upon log-in via pre-boot to any device, the key file is transferred transparently, and access is granted only to authorized files and folders – which are all encrypted
- The user's identity is validated automatically, and keys are only valid for the session
- Upon removal of the RMC device, all keys are removed from the system, ensuring no other users can access non-approved data

Business Results

With SecureDoc FDE for RMCE, healthcare providers gain a more secure means of encryption and user authentication to protect their highly-sensitive personally identifiable information (PII) of its patients against breach, following the user wherever they go. SecureDoc's ease-of-use means that users don't need to constantly log-in by remembering many passwords or PINs, and by eliminating or reducing costly password recovery and reset processes, healthcare providers can save valuable time and money.

Interested in learning more about WinMagic's encryption solutions for healthcare? Visit winmagic.com, or email info@winmagic.com

WINMAGIC

US & Canada +1 888 879 5879 | United Kingdom +44 0148 334 3020 | Germany +49 69 175 370 530 | Japan +03 5403 6950 | APAC +65 9634 5197