

**WHITEPAPER**

# Removable Media Security for Healthcare Organizations

Practical Advice for Enabling Healthcare IT and Security Professionals



## Removable Media



### Introduction

Security professionals in the healthcare industry find themselves facing unprecedented challenges protecting sensitive information. While the threats to information have grown ever more complex, so has the computing environment in which they must work. The need to support access to ever-increasing quantities of healthcare data by an increasingly mobile and distributed workforce coincides with greater-than-ever regulatory oversight and pressure to keep that same information secure.

Although attacks targeting sensitive information may grab the headlines, it is the day-to-day challenges of ensuring the right people have access to critical information when they need it, and that potentially highly sensitive, protected information is secure, that remains among the top concerns of security professionals.

As the workforce has become more mobile, utilizing newer, high-powered smartphones, as well as the latest generation of high-capacity USB storage devices, the problem of deperimeterization has grown with it. Traditional security controls and processes are often ill-suited to a world in which a user can copy gigabytes or terabytes of data in a few seconds to a device small enough to fit in their pocket. A single device worth only a few dollars could be the source of a breach costing millions of dollars in fines, legal fees, remediation and business loss.

Most concerning for security professionals is the constant and growing stream of such breaches now visible to the public. Independent organizations such as the Open Security Forum and the US Department of Health and Human Services provide publicly available tracking information for breaches as they occur. In the case of the US Department of Health and Human Services, the breaches are tracked when they affect 500 or more patients. Between January of 2010 and June of the same year, HHS reported 62 breaches, several of which compromised more than 10,000 records. In two cases, over 100,000 records were lost. Of the breaches reported, 42% involved a laptop or portable electronic device.

While removable media security may be one of the more difficult challenges facing security teams in the healthcare industry, there are strategies that can be adopted to reduce the risk of a breach of sensitive information through these devices. These strategies will help you not only prevent data loss, but also help ensure that your end-users can continue to have access to the information they need, wherever it is stored. Before addressing these strategies, it is important to understand why removable media security has become such a significant problem.

## Removable Media



### THE REMOVABLE MEDIA CHALLENGE

There are a number of reasons why removable media, such as the ubiquitous USB flash drive, have proven to be such a thorn in the side of IT security policies. Among them are the number and variety of device types, the way in which they are used, and user expectations when it comes to freedom to copy and transfer information on and off systems. We'll look at:

- › Shared systems
- › User expectations
- › Management costs
- › Recovery of lost information and keys
- › Reporting and auditing

While there are certainly other challenges, these are the most pressing. For a more complete discussion on the challenges of removable media security, also review CREDANT's whitepaper series "Removable Media Security Best Practices," available at [www.credant.com](http://www.credant.com).

### SHARED SYSTEMS

The need to share systems and yet apply appropriate security controls is especially acute in the health-care industry, where a single system may be shared by many users. As a result, the removable media security strategy must also enable multiple users to seamlessly, and securely, move and copy data.

### USER RESISTANCE

End-user expectations often present a significant roadblock to the implementation of controls around protecting information on removable media. Devices are simple to use, copying data requires nothing more than dragging icons on to the device, and no special software or skills are needed to transfer or back-up very large volumes of data. Any security

policy or control that affects this user experience is likely to be perceived as onerous. Solutions that require the entire storage device to be encrypted when first inserted can impose significant delays in the use of the device, and therefore cause the perception that security is acting as a barrier to operational effectiveness. This may cause the end-user to abruptly abort the encryption process by simply removing the USB device partway through the initial encryption process. (In the case of large-volume storage devices, this process can take many minutes or even hours.) In some cases, this could result in the corruption of the device and the loss of any data already on it—further compounding user perception that the security process is a barrier to overcome, not an enabler to better data protection.

### MANAGEMENT COSTS

The cost of managing encryption of removable media has also been a cause for concern. While the number of hard drives in any organization changes relatively slowly and in a controlled manner, removable media is difficult to track and may represent many times the number of end points. The very large number of devices, with new devices being constantly added, imposes significant burdens for reporting and key management.

### RECOVERY OF INFORMATION AND KEYS

Without the ability to easily recover a lost (forgotten) key in order to access a flash drive, access to potentially valuable and even life-saving information could be delayed and, at the very least, the productivity of the end-user is reduced and the workload for the helpdesk increased. Good key recovery strategies are especially important when the device is to be used outside of the central network, where access to a stored key or helpdesk function may be more difficult or simply not accessible at all.

## Removable Media



### REPORTING AND AUDITING

As one of the most heavily regulated of industries, healthcare IT professionals are already familiar with the requirements to provide detailed auditing information for compliance purposes. However, the addition of removable media, with the associated increase in the speed, ease and volume of data now stored on mobile resources will stretch reporting and auditing capabilities to their breaking point. As the penalties (both legal and commercial) associated with a significant breach continue to mount, the ability to ensure, and prove, that sensitive information on a removable media device was encrypted and therefore protected, is greater than ever.

### SOLUTIONS THAT WORK FOR HEALTHCARE

The challenges of protecting data on removable media are significant, however the good news is that a well-integrated and centrally managed encryption strategy will enable healthcare IT and security professionals to not only protect sensitive information, but to do so in a way that has minimal impact on end-users, enables enforcement of policies across the enterprise, and actually reduces the workload for auditing and reporting.

A number of different factors will affect how you define and implement a removable media strategy, what policies to enforce, and which solution you select to implement them.

We will look at:

- › Encryption strength
- › Device policy decisions
- › Key management
- › Reporting and auditing
- › Integration

How each of these areas is addressed—and their relative importance to your organization and security approach—will help define what controls to put in place and how to ensure a successful deployment.

### ENCRYPTION STRENGTH

Ensuring the security of data is the primary purpose of encryption, however, the actual strength of the encryption algorithm is unlikely to be an area where solutions will differ significantly. You should expect to see standard, military-strength algorithms such as AES (either 128 or 256 bit keys) or DES in any solution you evaluate. Lost USB media is unlikely to be subjected to the kind of sophisticated attack that would cause any concern, although poor key choices may enable brute-force, dictionary-based attacks to be successful. One policy option to consider would be to force a cool-down period after a certain number of failed attempts to enter the key. In the case of highly sensitive information, automatically destroying the key on the device under those circumstances would also help prevent any access by an attacker. (However, if this option is desired, it would be essential to warn end-users well in advance, and to ensure that a recovered device would be accessible once it was brought back into the corporate network. For more information on this approach, see CREDANT Technologies “Removable Media Best Practices” whitepaper series at [www.credant.com](http://www.credant.com)).

### DEVICE POLICY DECISIONS

Deciding what policies are to put in place is essential to ensuring the appropriate balance of risk management and business enablement. There are a number of choices regarding how to deal with devices and what level of control needs to be put in place.

The main considerations are discussed here, and include deciding what types of media to allow, who policies will apply to, and dealing with access outside of the corporate network.

## Removable Media



### **Preventing the use of any removable media**

Disallowing any removable media is always an option, but for many organizations it is unlikely to be successful. End-users have become accustomed to using removable media freely, and preventing all use is likely to cause significant business impact. However, for certain systems that either house highly sensitive information or are in public locations such as a kiosk, this may be a necessary step.

### **Using only self-encrypting flash drives**

Some organizations have taken the decision to allow only company-issued encrypted devices to be utilized. These devices can be effective at protecting the information on them; however certain management problems must still be overcome. These include how to prevent end-users from bringing their own, non-encrypted devices into the corporate environment and using them, as well as the risk that a user will disable encryption on the company-issued flash drive itself, thus negating any security benefits. For the above reasons, while these devices are a useful addition to your security strategy, they are unlikely to be the only solution you will need in place.

### **Allowing all external storage media and choosing what data to encrypt**

Many users will freely mix both corporate, protected information and non-sensitive or personal data on the same device. This approach is the most common, and the one you are most likely to implement with the bulk of the user community. However, deciding whether to encrypt some or all of the data on a device is an important point. It may be appropriate to only enforce encryption for new data as it is copied from a corporate system onto the removable media. Alternatively, you may wish to simply enforce encryption for everything, as this may reduce reporting and management challenges and help protect any legacy data in place.

### **Providing different controls for different groups of users**

Different users will access different types of data, and as a result, may also need different policies in place. As the appropriate policies will typically be defined by the role of the user, it is generally best to enforce a policy based on an authoritative identity source, such as Microsoft<sup>®</sup> Active Directory. Tying a security policy in to Active Directory users and groups helps simplify management and reporting, as well as ensuring that more comprehensive coverage is applied.

### **Allowing access on third-party systems**

Many users will copy data onto a removable media device in order to transfer it to another system. Often, that system will be outside your corporate network. An important decision that must be made is whether to allow the use of removable media that contains potentially sensitive information outside the corporate network. There are three basic choices:

1. Prevent any use of a device containing corporate information outside of the network perimeter
2. Allow data to be copied onto another system, but only if it is also encrypted (and therefore protected)
3. Allow free access to the data from another system

In reality, it is likely that you will want to enforce a mix of these policies, depending on who the user is and what type of information they may have access to. While the third option is the least restrictive, it also presents the greatest risk of a breach. However, much of the concern associated with removable media is accidental disclosure (that is, that the device is simply lost) and in this case, even choosing the third and least restrictive approach would still protect data on a lost USB stick that is accidentally lost.

## Removable Media



### KEY MANAGEMENT

Key management, and the ease with which it can be carried out, often defines the success of an encryption approach. Centralized escrow of keys for removable media enables a number of important benefits:

- › It enables a user to simply insert a removable media device into a corporate system without having to remember the key in order to access the data. The encryption software should automatically authenticate the user based on their login credentials, authorize access to the key and, therefore, the data on the device in a way that is completely transparent to the end-user.
- › Should a device become lost (and as a security measure the key is disabled on the device as described earlier), centralized key management will re-enable access to the information on the device if it is recovered. In the same way, if the end user accidentally causes the local, on-device key to be deleted then again, simply bringing the device into the network will re-enable access.
- › It simplifies remote support for a user who has forgotten the key to access a device.
- › It enables access to a device that has been recovered from an employee who has left the organization, when the key is no longer known or available.

By providing centralized key management, a good removable media encryption solution will reduce the workload of managing security, as well as ensure that users can continue to access information when they need it, regardless of what happens.

### REPORTING AND AUDITING

In the highly regulated healthcare industry, reporting and auditing are essential elements of any security approach, and this is every bit as true for removable media security. In fact, as data moves ever more rapidly from device to device and as the storage capacity of removable media devices continues to grow,

the ability to audit and report on security for these devices is vital. Important considerations for reporting and auditing will be:

- › The ability to report on removable media encryption events (such as a device being encrypted)
- › Providing an inventory of devices that have been encrypted
- › The ability to show that no unencrypted devices have been used
- › Centralizing encryption reporting for removable media and integration into the broader encryption reporting to ensure that stakeholders have access to a full view of data security events

In those instances when end-users are allowed to decide whether to encrypt information on a removable media device it is also important to be able to show what decisions were taken, and by whom. This is especially important in the event that a device is lost, or there is concern that a breach may have occurred. The ability to quickly produce a report proving that information on removable media was encrypted at the time of the breach could prevent extremely expensive and unnecessary forensic activity and even ultimately avoid the need for a formal breach notification.

### INTEGRATION

As referenced earlier, integration between the removable media encryption solution and the rest of the security solutions in place helps reduce the workload of managing multiple solutions, and will also have the added benefit of providing a more complete view of organizational risk. As organizations utilize an increasingly broad array of computing platforms, and as the consumerization of enterprise IT (in which employees use their own devices for business purposes) continues, the number of variety of security solutions that must be managed will continue to grow. This is true of encryption, where everything from self-encrypting

## Removable Media



drives, policy-based encryption, OS-level and even hardware-level encryption must be managed. The ability to integrate removable media encryption into broader encryption management will reduce the work on security teams and help provide more complete and integrated protection for sensitive health data.

### CONCLUSION

All organizations must be vigilant and show due care when protecting sensitive information. However, the healthcare industry is under particular pressure to do so, as the information stored is both potentially valuable and highly personal. As a result, the rapid growth of high capacity and low cost storage media, such as USB flash drives and USB hard drives, has places extra pressure on security and IT organizations. Nevertheless, with the right controls in place and with a well integrated and automated solution, protecting information on removable media can be accomplished without creating unreasonable amounts of additional work or interfering with the very important day-to-day requirements of healthcare workers to access information how and where they need it.