# secRMM

## Security Removable Media Manager

## *Whitepaper- Healthcare*

**OVERVIEW.** HIPAA Security Rule requires health plan administrators, health information clearinghouses, and healthcare providers who transmit information electronically to implement policies and procedures to prevent, detect, contain, and correct security breaches.[1] In addition when these covered entities contract with others (business associates) to perform business functions, arrangements must be made to ensure the privacy of protected health information accessible by the business associates.[2] secRMM provides covered entities and business associates with a tool that helps ensure compliance with the HIPAA Security Rule by monitoring and collecting data about removable write activities and providing simple authorization modules.

**The following is a list of compliance rules under HIPAA that the deployment of secRMM will satisfy (with respect to removable media);**

1) Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.[3]
2) Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.[4]
3) Implement procedures to regularly review records of information system activity such as audit logs, access reports, and security incident tracking reports.[5]
4) Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.[6]

[1] See HIPAA Security Rule, 45 C.F.R. §164.308(a)(1)(i).
[2] See definitions of "business associate" and covered entity" at 45 C.F.R. §160.103.
[3] See HIPAA Security Rule, 45 C.F.R. §164.308(a)(1)(ii)(a).
[4] See HIPAA Security Rule, 45 C.F.R. §164.308(a)(1)(ii)(b).
[5] See HIPAA Security Rule, 45 C.F.R. §164.308(a)(1)(ii)(D).
[6] See HIPAA Security Rule, 45 C.F.R. §164.308(a)(3)(ii)(A).

5) Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in §164.308(a)(3)(ii)(B).[7]
6) Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes.[8]
7) Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.[9]

Regardless of the type of electronic device (USB, tablet or smartphone) connected to a network with electronic protected health information ("ePHI"), users must abide by HIPAA Security Rule guidelines when handling both information at rest and that which is being transferred onto a removable media device. As required by section 13402(e)(4) of the Health Information Technology for Economic & Clinical Health ("HITECH") Act and HIPAA Security Rule 408(a), a covered entity must report breaches of unsecured protected information.

However, the reporting requirements are significantly enhanced if the breach affected more than 500 individual's ePHI. If a breach of unsecured protected health information affects 500 or more individuals, a covered entity must notify the Secretary of the Department of Health & Human Services of the breach without unreasonable delay and in no case later than 60 calendar days from the discovery of the breach.[10] Whereas, if the breach affected fewer than 500 individuals, a covered entity must notify the Secretary of the breach within 60 days of the end of the calendar year in which the breach was discovered.[11] By providing the exact files that have been breached secRMM allows the covered entity to determine the appropriate timeline and action for reporting the breach.

**In addition to the increased reporting requirements HITECH established more stringent federal guidelines associated with the loss of ePHI, including more severe fines, penalties, and procedures for data breaches.[12]** All of which has created a demand for solutions that seal off potential liability risks due to breaches in an organizations network. There are some other solutions on the market that try to tackle this problem, however they are costly to implement and/or require downloading the software on the individual's device. Whereas, if your organization deploys secRMM across its network it will have the capability of logging all activities with respect to removable media without the necessity of downloading the software on each device. This allows organizations the continued benefit of permitting employee's the use of their own devices thereby increasing efficiencies and limiting cost expenditures while maintaining network security of ePHI.

**LIMIT LIABILITY THROUGH DATA LOSS PROTECTION WITH secRMM.** secRMM provides a solution within a healthcare organizations security suite that solves the Issue ("Pain") of Data Loss through removable media mounting to the network. If left unmanaged, the introduction of removable media storage devices can lead to loss of control and ultimately a breach of sensitive data that can subject an organization to financial liability (failing to adhere to HIPAA Security Rule) and/or damage to your reputation. secRMM allows for the management of growing workforce expectations around the mobility of data without simply relying on an honor system.

[7] See HIPAA Security Rule Administrative Safeguards, 45 C.F.R. §164.308(a)(3)(ii)(C).
[8] See HIPAA Security Rule, 45 C.F.R. §164.308(a)(6)(ii).
[9] See HIPAA Security Rule, 45 C.F.R. §164.312(b).
[10] U.S. Department of Health & Human Services. Health Information Privacy: Breaches Affecting 500 or More Individuals. Retrieved on February 5, 2015 from http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html.
[11] U.S. Department of Health & Human Services. Health Information Privacy: Breaches Affecting Fewer than 500 Individuals. Retrieved on February 5, 2015 from http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html
[12] See Amount of Civil Money Penalty, 45 C.F.R 160.404(b)(2).

## secRMM ADDITIONAL BENEFITS TO HEALTHCARE ORGANIZATIONS…

**SIMPLE AUTHORIZATION MODULES.** secRMM provides simple authorization modules for organizations to control the who/what/where/when/how of data being written from their network to removable media. Unlike other competing solutions, secRMM lets organizations control what files the end-user can copy from both the local computer and the network. Additional functions allow for organizations to control removable media write activity based on userid, removable media serial number, and removable media internal IDs (i.e. VIDs and/or PIDs) and the program that is being used to perform the write operations. The solution can also prevent unauthorized devices from mounting to the Windows Operating System. When an individual attempts to perform an unauthorized copy or mount secRMM logs the event. This enables firms to further investigate why the user was attempting to perform that activity and helps stop future potential breaches.

**CONTINUED USE OF "BRING YOUR OWN DEVICES" ("BYODs") WITH SECURITY.** With the increasing use of BYODs organizational networks cannot be adequately secure without procedures in place to limit/prevent write activity or monitor the who/what/where/when/how of files being written. secRMM is the only solution capable of providing source file names for write operations to virtually all removable media- smart phones (iPhone, Blackberry, Windows, Android, etc.), tablets, USBs, and CD/DVDs. This allows firms to easily and centrally evaluate activity being performed on endpoint terminals. secRMM provides for effective assessment of potential risks by monitoring and collecting detailed forensic data about removable media write activity or even attempted write activity.

**ADDED PROTECTION TO ENCRYPTION TECHNOLOGY.** secRMM works seamlessly with hardware/software encryption technologies to generate security events which informs a system administrator when an encrypted device has been mounted, and whether authorization was granted.

**INTEGRATED WITH MICROSOFT SYSTEM CENTER SUITE OF PRODUCTS.** secRMM is tightly integrated with the Microsoft System Center suite of products; including System Center Configuration Manager ("SCCM"), System Center Operations Manager ("SCOM"), SCOM Audit and Collection Services ("ACS"), and System Center Orchestrator. This allows the system administrator to set up alerts, notifications, tasks, reports, and can optionally generate SNMP traps, among other desirable capabilities.

**COMPLETE SOURCE PATH.** secRMM is the only Data Loss Prevention ("DLP") software capable of capturing the complete source path of a file being copied to a removable media storage device.

**secRMM DOES NOT REQUIRE ITS' OWN FRAMEWORK.** secRMM easily integrates into the enterprise management framework organizations are currently using. This makes secRMM particularly cost effective compared to other solutions. secRMM accomplishes this by utilizing the base Windows Operating System components. Furthermore, secRMM is completely functional within the Windows Event Log and the base Microsoft Management Console ("MMC"). Given these efficiencies Squadra is able to provide the software at *affordable pricing*.

**Squadra Technologies**
**7575 West Washington Ave.**
**Suite 127-252**
**Las Vegas, NV 89128**
**+1 (760) 846-6844**

**For More Information Contact:**
**info@squadratechnologies.com**

**Free Trial Download Visit:**
**www.squadratechnologies.com**