Roxio Security for Medical Offices

Helping Medical Offices Comply with HIPAA and HITECH Rules

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) required the U.S. Department of Health and Human Services to develop regulations protecting the privacy and security of Protected Health Information (PHI). As part of this requirement, the HHS established a set of rules and national standards for the protection of certain health information. These rules apply to 'covered entities' including health plans, health care clearinghouses, such as billing services, and community health information systems and health care providers that transmit health care data in a way that is regulated by HIPAA.

HIPAA includes a set of administrative simplification provisions that, among other things, include rules to help protect the privacy of PHI:

- The Privacy Rule requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization.

- The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity and security of electronic protected health information.

- The Breach Notification Rule, issued as part of the Health Information Technology for Economic and Clinical Health Act (HITECH), requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information.

The HHS has issued guidance on how to secure protected health information appropriately. According to the HHS, PHI stored on data at rest (such as data stored on CD, DVD or USB flash memory devices) "…may be secured using one or more methods for rendering PHI unusable, unreadable or indecipherable to unauthorized individuals: encryption and destruction."[1]

Data breach has become a major problem for businesses and organizations. The media's almost daily reports of these incidents shows just how common and costly data breaches are for both organizations and individuals. According to a recent study by Poneman Institute, a leading research firm in privacy and data protection, the costs of data breach exceed $200 per customer record lost and continues to grow year by year.[2]

Health organizations have both ethical and legal responsibilities to protect confidential patient data. Furthermore, organizations must protect internal data such as employee records. Of particular concern is the need to protect personally identifiable information (PII) about individuals. Encryption is a key tool to prevent unwanted access to data.

The Challenge of Protecting Data

In the simplest terms, encryption of data on portable media can prevent unauthorized users from accessing it. The encryption needs to be strong enough to prevent circumvention and some organizations must also comply with specific encryption standards such as US government approved standards.

One of the biggest challenges in protecting data on removable media is that it is so easy for workers to write unprotected files to an optical disc or to a USB stick. Even if encryption is available, employees may simply choose not to use it because it requires extra time and effort.

Roxio Secure Burn Enterprise is specifically designed to make it extremely easy to secure data on removable media. Furthermore, Secure Burn Enterprise is designed to be scalable, depending on the needs of the organization. Encryption can be controlled by the user, or by the system administrator at the user, group or organizational level based on policy.

With Secure Burn Enterprise, business decision makers as well as employees responsible for transporting data can be confident that the data they carry is encrypted and secure.

Roxio Secure Burn Enterprise

With user-friendly design and powerful tools for system administrators, Roxio Secure Burn Enterprise helps protect your organization against data breach. Employees can quickly secure data on CD, DVD, Blu-ray Disc and USB devices using powerful data encryption that safeguards the content from being accessed by unauthorized persons. Secure Burn Enterprise goes beyond simple encryption on standalone machines to provide advanced end-point security features for network of computers in small workgroups to multi-departmental global enterprises. Secure Burn Enterprise arms organizations with the tools to not only meet internal security policies, but also comply with industry and government-mandated privacy measures and regulations.

Roxio Secure Burn Enterprise:

- Burns data on CDs, DVDs, Blu-ray Discs and USB drives using an easy drag and drop interface
- Copies discs and disc image files
- Encrypts data using a FIPS 140-2 encryption module*
- Secures files with powerful 256-bit AES encryption
- Spans files too big to fit across multiple discs
- Reads and writes disc image files
- Allows discs to be read on PCs within permitted departmental groups
- Restricts permission to read discs on PCs outside permitted departmental groups
- Supports read/write permissions set by system administrators
- Enables logging to keep track of data, computer name, user name, files, folders and other information

Secure Burn Enterprise enables encryption of data on removable media, including optical discs and USB flash memory devices. Ideal for firms of all sizes, Secure Burn Enterprise makes it easy for employees to automatically encrypt data per organizational policies and helps to protect medical offices and clients from the expense of data breach and non-compliance with mandated regulations.

Secure Burn Enterprise is an inexpensive and convenient way for medical offices to ensure that confidential records stored on optical and USB flash media are only viewable by authorized personnel, and can help ensure compliance with mandated regulations.

*Roxio secure disc burning uses a FIPS 140-2 certified encryption module from Microsoft.

[1] Department of Health and Human Services, O.o. (n.d.) Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals for Purposes of the Breach Notification Requirements under Section 13402 of Title XIII (Hea. Retrieved from www.hhs.gov: http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/hitechrfi.pdf)

[2] 2014 Cost of Data Breach Study: Global Analysis by Poneman Institute: http://www.ponemon.org/blog/ponemon-institute-releases-2014-cost-of-data-breach-global-analysis

Contact

To request a quote, contact the Volume Licensing Sales team at:

North America:

Brian Hanlon
North American Licensing Manager
Corel, Roxio & Pinnacle
1-888-267-3548 ext. 1246
C. 613-299-4129
Brian.Hanlon@Corel.com

Europe:

Email: vlp.emea@roxio.com