DeviceLock for HIPAA Compliance

Contents

Introduction

In keeping with the Health Insurance Portability and Accountability Act, Public Law 104-191 (HIPAA), which was adopted in 1996, all American organizations which use the personal medical data of citizens are required to guarantee the confidentiality of that information. HIPAA requirements are mandatory for medical institutions, medical insurance companies, government agencies and other organizations which have access to private medical records.

The privacy and security requirements set out in HIPAA have also been included in two additional statutory acts. First, there is the HIPAA Privacy Rule (Standards for Privacy of Individually Identifiable Health Information). This document requires that the confidentiality of absolutely all medical data be maintained, whether the data is in paper or electronic format or even if the information was pronounced out loud by a doctor. In general, the HIPAA Privacy Rule focuses on general issues of ensuring the protection of medical data, such as cases in which data is disclosed to third parties or organizations. Second, there is the HIPAA Security Rule (Health Insurance Reform: Security Standards). This document contains more detailed requirements for the protection of electronic medical records and describes the necessary policies and procedures.

Violation of HIPAA provisions is punishable with both civil and criminal liability. The US Department of Health and Human Services may fine violators USD 100 for one incident of noncompliance with HIPAA requirements. However, if a person knowingly receives or discloses someone else's medical data in violation of HIPAA requirements, they can be fined up to USD 50,000 and may be sentenced up to one year in jail. For those who intentionally violate and trade private individual health data and obstruct an investigation, punishment may be increased to USD 250,000 and up to 10 years in jail.

This white paper will review the requirements of the HIPAA Security Rule, which has an impact on a company's information infrastructure and the security means used therein. This paper will also address the features of DeviceLock, a product by DeviceLock, Inc., which can help organizations achieve compliance with HIPAA much more effectively.

HIPAA Requirements

First and foremost, we need a clear definition of which organizations must comply with the requirements of this law. According to the wording of the HIPAA, there are three types of organizations (i.e., covered entities). The first group is health plans, or companies which provide individual and group insurance policies for payment of a patient's medical expenses. The next group includes health care clearinghouses, which process transactions and transform medical

data from one format to another. Usually, these organizations serve as intermediaries between insurance companies (health plans) and health care providers. The third group of organizations affected by the HIPAA is health care providers, who must work with patients' personal medical data and pass it along via communication networks. If a company is still unsure of whether or not it must comply with HIPAA, it can check the covered entity charts.

Now let us address which categories of information fall under HIPAA requirements. The law protects all individually identifiable health information (**IIHI**) which is stored within an organization or transferred to its partners (contractors, business partners or outsourcers, etc.). HIPAA protects all IIHI, regardless of its format or the device on which it is stored. In other words, information may be in paper format, in electronic format, or even simply pronounced out loud. All of the data protected by HIPAA is called protected health information (**PHI**).

A more precise definition of IIHI is

- information relating to the past, present or future physical or mental health condition of an individual;
- information about medical aid provided to an individual;
- information relating to the past present or future payment for the provision of health care to an individual.

Furthermore, in order for this information to fall within the definition of IIHI, they must clearly identify an individual, or present reasonable grounds for associating the information with a specific individual. Overall, IIHI includes a great deal of common identifiers (such as a person's name, address, date of birth, insurance number, etc.).

Requirements of the HIPAA Security Rule

The HIPAA Security Rule is based on the concept of ePHI - protected health information in electronic format.

The key requirement of the HIPAA Security Rule can be summarized as follows: all institutions which store or transmit medical data in digital format (ePHI) must take the appropriate administrative, technical and physical security measures in order to:

- ensure the completeness and confidentiality of ePHI;
- reflect any potential dangers or threats to ePHI;
- prevent the unauthorized usage and disclosure of ePHI;
- ensure general control over the compliance of employees and officers with these rules.

One could draw the conclusion that the HIPAA Security Rule poses a relatively wide range of requirements for ensuring the security of ePHI. These include:

- **Protection against internal and external threats**. ePHI must be protected against both internal and external threats.
- **Risk analysis**. Companies must regularly conduct an extensive risk analysis.

Furthermore, organizations are obliged to formally express all of their security policies, processes and procedures in writing.

Requirement structure

The requirements of the HIPAA Security Rule are comprised of three different categories: administrative, physical and technical security measures. These three categories are set out in 18 standards, 12 of which are implementation specifications. For the sake of clarity, a *standard* defines exactly what an organization must do, and a *specification* outlines how it must be done.

The HIPAA Security Rule includes a total of 36 specifications which can be divided into two groups: required and addressable. The first category includes 14 specifications, and the second is comprised of 22 specifications. Required specifications are of a regulatory nature, and are mandatory for all organizations. Addressable specifications serve as recommendations, and organizations have three options in dealing with them.

1. If an organization finds that the requirements in a particular specification are reasonable and appropriate, then it must implement them.

2. If an organization finds that the requirements in a particular specification are not advisable or appropriate, but it cannot achieve compliance with all standards without implementing additional security measures, the organization must do the following:

    a. soundly document the reasons why the requirements of the specification in question are not advisable; and

    b. introduce and document alternative security mechanisms which will facilitate the effective execution of the task stipulated in the relevant specification.

3. If an organization finds that the requirements in a particular specification are not advisable or appropriate, and it is possible to achieve compliance with the standard without implementing additional security measures, the organization must do the following:

    a. make the decision against introducing this specification;

    b. document the reasons why this particular specification is not reasonable or appropriate, and

    c. document how the full compliance with the standard in question will be achieved.

Specifications may be introduced in any order when implementing the HIPAA Security Rule.

Administrative security measures

About one-half of all of the Security Rule's standards address administrative security measures. These standards require documented policies and procedures governing control over daily operations, managing employee access to ePHI, as well as the selection, development and usage of means of control. The table below summarizes the standards for administrative security measures.

Table. 1. HIPAA Security Rule Requirements for Administrative Security Measures

Requirement	Explanation
Security Management Process	Each organization must implement policies and procedures in order to prevent, identify, remedy and document security breaches.

Assigned Security Responsibility	Each organization must appoint a person who will be fully responsible for ePHI security.
Workforce Security	An organization must have developed and implemented policies, procedures and processes which will guarantee that access to ePHI will be given only to authorized personnel in line with established procedures.
Information Access Management	The organization must have developed and implemented policies, procedures and processes which govern the authorization and creation of and changes to ePHI access rights.
Security awareness and training	An organization must have developed and implemented a training program which informs employees of security issues.
Security Incident Procedures	Each organization must develop and introduce policies, procedures and processes for dealing with security incidents: a reporting system, taking actions in response to an incident, and incident management.
Contingency Plan	An organization must have implemented and incorporated policies, procedures and processes for taking action in response to catastrophes, natural disasters and other events which could cause technical difficulties with information systems storing ePHI.
Evaluation	Each organization must periodically conduct technical and other evaluations of security policies, procedures and processes in order to ensure compliance with the Security Rule.
Business Associate Contracts and Other Arrangements	When collaborating with partners which create, receive, store or transmit ePHI, organizations must develop and utilize contracts which will require the partner to implement effective ePHI security measures.

Physical security measures

Physical security measures comprise a collection of requirements dedicated to the protection of electronic information systems and ePHI against unauthorized physical access. Essentially, each organization which is covered by HIPAA must restrict physical access to ePHI and grant physical access only in line with established and authorized procedures. The table below summarizes the standards for physical security measures.

Table 2. HIPAA Security Rule Requirements for Physical Security Measures	
Requirement	Explanation
Facility Access Controls	Each organization must implement policies, procedures and processes restricting physical access to electronic information systems and guaranteeing access only in authorized cases.
Workstation Use	An organization must have developed and introduced policies and procedures setting out guidelines for the appropriate usage of workstations and the features of a physical workstation environment which may be used to gain access to ePHI.
Workstation Security	Organizations must implement physical security measures for all workstations with access to ePHI in order to restrict access to ePHI and ensure that it is accessed only by authorized users.

Device and media controls	Each organization must develop and introduce policies, procedures and processes which facilitate control over the connection and disconnection of hardware and electronic storage devices which contain ePHI. An organization must also ensure control over the movement of these devices within the organization and beyond its territory.

Technical security measures

The technical security measures are comprised of several requirements for using technology to protect ePHI. The table below summarizes the standards for technical security measures.

Table 3. HIPAA Security Rule Requirements for Technical Security Measures	
Requirement	Explanation
Access Control	Organizations must develop and introduce policies, procedures and processes which provide access to information systems that contain ePHI only to those persons and programs which have the appropriate rights to said access.
Audit Controls	Each organization must introduce mechanisms for introducing and analyzing action logs with information systems that contain or use ePHI.
Integrity	Organizations must develop and introduce policies, procedures and mechanisms which protect ePHI against distortion (inaccurate modifications) and destruction.
Person or Entity Authentication	Each organization must develop and introduce policies, processes and procedures which authenticate each person and each company which attempts to obtain access to ePHI.
Transmission Security	Organizations must develop and introduce policies, procedures and processes which prevent unauthorized access to ePHI during the transmission of said information via electronic communications, including the Internet.

Requirements for the storage of electronic documents

Each organization covered by HIPAA must store all documentation (for example, its policies, procedures, etc.) which must be drawn up in line with the Security Rule. All relevant documents are to be stored for a period of 6 years after they are created or come into force (whichever date comes latest). This documentation process is to be accessible to employees responsible for introducing policies and procedures. Moreover, an organization must periodically check and update these documents in order to guarantee confidentiality and integrity of the ePHI as well as the access to it. As a result, the storage process for developed documentation and ensuring the security of ePHI requires continuous efforts on the part of an organization.

Introducing the requirements of the HIPAA Security Rule is a complex process. First and foremost, organizations are required to identify and evaluate ePHI risks, and then introduce advanced practices as set out in the standards.

DeviceLock from DeviceLock, Inc.

DeviceLock is endpoint device security software developed by DeviceLock, Inc. for corporate users. With DeviceLock, a company of any size can protect itself from the theft, leakage and corruption of information secured on corporate networks. DeviceLock controls all uploading and downloading activity via workstation ports, wireless networks and external drives based on assigned policies. When configured for the purpose, it can also provide complete shadow copying of all outgoing data. In contrast to the great number of solutions for the storage of email correspondence, DeviceLock facilitates the collection and analysis of data leaving the corporate network via workstation ports.

The problem of data leakage through PC ports and drives is not unique to medical environments, though due to HIPAA regulation, the consequences of not checking the threat is greater here. There is an ever-increasing number of mobile devices maintained and, in some cases, purchased by employees connecting to corporate networks. Experts at Yankee Group and SCS Research studied this trend toward the '*consumerization of corporate IT networks*' and advised IT department managers and directors neither to ignore nor to attempt to completely prohibit the plethora of portable devices used by employees. They simply must provide support for employees' mobile computers and devices. Otherwise, the company risks losing its innovative and competitive edges by reducing the productivity of its employees. In a hospital context, for example, you wouldn't want to prohibit care givers from accessing or carrying medical records to the point of care via a device if that would improve the quality of care. But, such data movement does need to be controlled, as health data on mobile devices can lead to information leaks and HIPAA non-compliance. DeviceLock can help solve this dilemma.

DeviceLock protects companies against the leakage of ePHI and unwanted content, and serves as a tool for retrospective analysis of all data which company employees copy to external drives and take with them. It also affords a company the flexibility it needs in setting up information security policies when working with mobile devices.

DeviceLock can be used to control USB ports, disk drives, CD and DVD drives, as well as FireWire, IR ports, parallel and serial ports, WiFi and Bluetooth adapters, tape recordings, PDAs, and any internal and external removable drives and hard drives. DeviceLock conducts a thorough audit of user actions with these devices.

When it comes to PDAs, smartphones and other communicators, DeviceLock does more than just support the shadow copying of all of the data exchanged to a mobile device - it also allows a company to apply flexible security policies and then track the enforcement of these policies. For example, DeviceLock may permit a user to synchronize his contacts and calendar, but prohibit copying files or synchronizing email with attachments.

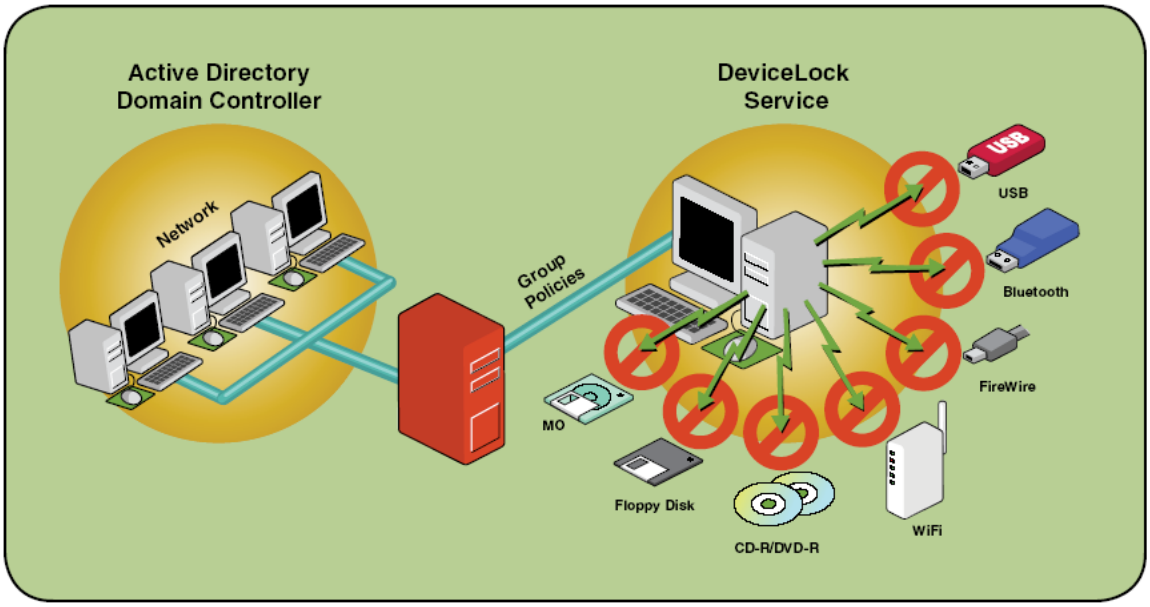
DeviceLock also provides protection against hardware keyloggers, which are connected between a computer's keyboard and the system unit and used to steal valuable data from employee workstations. A malicious user can connect a keylogger between an employee's computer and keyboard, thus tricking antivirus software and other means of security. Once DeviceLock detects the exchange of data from the computer to the keylogger, it will warn the user and create a record in the events log.

DeviceLock consists of three parts: the agent, the server and the management console:

1. DeviceLock Service (the agent) is the core of DeviceLock. DeviceLock Service is installed on each client system, runs automatically, and provides device protection on the client machine while remaining invisible to that computer's local users.

2. DeviceLock Enterprise Server (the server) is the optional component for centralized collection and storage of the shadow data and audit logs. DeviceLock Enterprise Server uses MS SQL Server to store its data.

3. The management console is the control interface that systems administrators use to remotely manage each system that has DeviceLock Service. DeviceLock ships with three different management consoles: DeviceLock Management Console (the MMC snap-in), DeviceLock Enterprise Manager and DeviceLock Group Policy Manager (integrates into the Windows Group Policy Editor).



DeviceLock can be controlled using group policies in Windows Active Directory, making it easy to integrate it into the infrastructure of an organization of any size.

How DeviceLock Supports HIPAA Compliance

DeviceLock controls data movement via local workstation ports, wireless networks and removable drives based on flexible policies. Each time, the decision to either permit or prohibit access to an external device is made automatically. That means DeviceLock's settings and policies are easily audited, and DeviceLock itself does not create any additional information security risks.

Using DeviceLock in a corporate environment helps ensure compliance with the two key requirements of the HIPAA Security Rule:

- **Device and Media Controls**. Each organization must develop and introduce policies, procedures and processes which facilitate control over the connections and disconnection of hardware and electronic storage devices which contain ePHI. DeviceLock helps fully resolve this problem.

- **Audit Controls**. Each organization must introduce mechanisms for introducing and analyzing action logs with information systems that contain or use ePHI. DeviceLock helps by shadow copying all data transferred to removable drives and mobile devices. By analyzing the collected data, it becomes easy to determine who copied what data, and when and how the transmission of ePHI took place - even in an external environment.

The table below summarizes the features of DeviceLock and how they help support compliance with the HIPAA Security Guideline.

Table 4. DeviceLock Features and Support for HIPAA Security Rule Compliance	
Administrative security measures	DeviceLock Features
Security Management and Assigned Security Responsibility	DeviceLock can help a company's management team effectively manage ePHI transmission processes in an external environment via local workstation communications. DeviceLock can also help guarantee that access to external devices will be granted only to employees who have received permission under the relevant security policy.
Workforce Security and Information Access Management	DeviceLock helps solve ePHI leakage issues by enforcing detailed control over communications that take place via local interfaces and the ports of corporate personal computers - even if attempts are made to steal data by an internal malicious user. Furthermore, shadow copying helps identify insiders after the fact and provide evidence of their actions.
Access Control and Audit Controls	Each organization must introduce mechanisms for introducing and analyzing action logs with information systems that contain or use ePHI. This is easy to achieve with DeviceLock. Shadow copying of data moved to and from removable drives and mobile devices makes it easy to identify who copied ePHI, and when and how it happened - even in an external environment.
Device and Media Controls	According to the HIPAA Security Rule, each organization must develop and introduce policies, procedures and processes which facilitate control over the connections and disconnection of hardware and electronic storage devices which contain ePHI. DeviceLock makes it easy to fully solve this problem by providing documented evidence of who has access to which devices.

About DeviceLock, Inc.

DeviceLock, Inc. (formerly SmartLine Inc) was established in 1996 to provide effective and economical network management solutions to small, medium and large-scale business. Early on, we made it our mission to design software that is robust and reliable when it comes to enforcing network policy, while being easy and intuitive for system administrators to use. Furthermore, we made it our job to deliver solutions that are well-integrated and cost-effective. Based on this formula, we've introduced and developed category-leading products like DeviceLock for enforcing security policy related to personal devices.

DeviceLock, Inc. is a worldwide leader in endpoint device control security. Our DeviceLock product is currently installed on more than 3 million computers in more than 55 000 organizations around the world.

The company's customers include BAE SYSTEMS, AEROTEC Engineering GmbH, HSBC Bank, Barclays Bank, Chase Manhattan Bank, and various state and federal government agencies and departments.

DeviceLock, Inc. is an international organization with offices in San Ramon (California), London (UK), Ratingen (Germany), Moscow (Russia) and Milan (Italy).

Contact Information

DeviceLock Germany:

Halskestr. 21, 40880 Ratingen, Germany

TEL: +49 (2102) 89211-0
FAX: +49 (2102) 89211-29

DeviceLock Italy:

Via Falcone 7, 20123 Milan, Italy

TEL: +39-02-86391432
FAX: +39-02-86391407

DeviceLock UK:

The 401 Centre, 302 Regent Street, London, W1B 3HH, UK

TEL (toll-free): +44-(0)-800-047-0969
FAX: +44-(0)-207-691-7978

DeviceLock USA:

2010 Crow Canyon Place, Suite 100, San Ramon, CA 94583, USA

TEL (toll-free): +1-866-668-5625
FAX: +1-646-349-2996

sales@devicelock.com

support@devicelock.com

www.devicelock.com