

HIPAA Compliance and Varonis

About HIPAA

Overview

This document provides an overview of the Health Insurance Portability and Accountability Act (HIPAA), its scope and purpose as well as a description of the way in which Varonis Systems enables entities to follow guidelines for regulation compliance. Varonis personnel and value added partners may distribute this document as an informational overview.

Background

The Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, the US Department of Health and Human Services (DHHS) published on November 3, 1999 proposes regulations establishing national standards for privacy of health information.

The Security Rule

The Final Rule on HIPAA Security Standards was issued on February 20, 2003. It took effect on April 21, 2003 with a compliance date of April 21, 2005 for most covered entities and April 21, 2006 for “small plans.” The Security Rule complements the Privacy Rule. While the Privacy Rule pertains to all Protected Health Information (PHI) including paper and electronic, the Security Rule deals specifically with Electronic Protected Health Information (EPHI). It lays out three types of security safeguards required for compliance: administrative, physical, and technical.

Who Needs To Comply

The following entities are covered by the proposed regulations:

- All health care providers who choose to store and/or transmit health information electronically
- All health plans
- All health care clearinghouses

The proposed regulations protect health information that 1) identifies an individual and 2) is maintained or exchanged electronically.

What Are the Costs/Risks of Non-Compliance

On February 16, 2006, the department of Health and Human Services (HHS) issued the Final Rule regarding HIPAA enforcement. It became effective on March 16, 2006. The Final Rule covers the enforcement process from its beginning, which will usually be a complaint or a compliance review, through its conclusion. A complaint or compliance review may result in informal resolution, a finding of no violation, or a finding of violation. If a finding of violation is made, a civil money penalty will be sought for the violation, which can be challenged by the covered entity through a formal hearing and appellate review process. These rules apply to covered entities that violate any of the rules implementing the Administrative Simplification provisions of HIPAA.

Security Rule Requirements

The security rules outline general requirements. They do not outline specific technologies. This is meant to provide flexibility so that adherence to HIPAA can take advantage of technological advancements. Organizations are expected to establish a prudent level of security based on community practices.

However, healthcare organizations may be affected by two regulations that do provide specific guidance. Organizations that deal with Medicare patients be aware of the specific requirements of the Health Care Financing. The Graham-Leach-Bliley act outlines specific requirements for organizations dealing with financial information, such as insurance companies or hospitals that provide financing for procedures.

How Can Varonis Help with HIPAA Compliance Efforts

The data governance solutions from Varonis help “Covered Entities” meet key requirements put forth in sections 164.308 (Administrative), 164.312 (Technical) and 164.316 (Documentation) of the Security Rule as they apply to data (research documents, patient records, spreadsheets, etc), stored on Windows and UNIX file server and Network Attached Storage (NAS) devices. The chart below identifies the applicable sections of the HIPAA Security Rule and provides a brief description of the Varonis products and functions that help meet these requirements.

HIPAA Requirement	Description	Varonis Product/Feature
Administrative		
Security Management Process 164.308(a)(1)	<i>Prevent, detect, contain, and correct security violations</i>	Varonis DatAdvantage maintains a detailed history of all objects managed by the Varonis application including users, user groups and by extension administrative accounts within user directories. At any given time users of DatAdvantage can generate reports that show which administrators changed security settings and access permissions to file servers and their contents. The same level of detail is provided for users of data, showing their access history as well as any changes made to security and access control setting of files and folders. Further, alerts and reports are automatically generated for anomalous or overly rigorous activity on important data sets. All of this ensures that access to data is continuously monitored for appropriate use and that organizations have all of the information they need to conduct forensic analysis and process improvement.

<p>Workforce Security 164.308(a)(3))</p>	<p><i>Prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.</i></p>	<p>Varonis helps meet the objectives of these requirements in a number of ways. 1) Varonis recommends the revocation of permissions to data for those users who do not have a business need to the data – this ensures that user access to data is always warranted and driven by least privilege. 2) Varonis generates reports showing the history of permission revocations and the percentages by which overly permissive access was reduced 3) Varonis DataPrivilege provides a mechanism via a web-based application by which to monitor, administer (allow/deny) all access requests to unstructured data. Requestors, data owners, technical controllers, financial controllers are all united in communication and action through this system. With regard to requests to access unstructured data on file shares, all actions taken and rationale for them are recorded. Further, a workflow is enforced (i.e. requests to financial folders go straight to the business owner). Via these capabilities, entities can demonstrate a historical and sustained enforcement of least privilege access and its effects.</p>
<p>Information Access Management 164.308(a)(4))</p>	<p><i>Implement policies and procedures for authorizing access to electronic protected health information</i></p>	<p>Varonis DataPrivilege helps organizations not only define the policies that govern who can access, and who can grant access to unstructured data, but it also enforces the workflow and the desired action to be taken (i.e. allow, deny, allow for a certain time period). This has a two-fold effect on the consistent and broad communication of the access policy: 1) it unites all of the parties responsible including data owners, HIPAA compliance officers, auditors, data users AND IT around the same set of information and 2) it allows organizations to continually monitor the access framework in order to make changes and optimize both for HIPAA compliance and for continuous enforcement of warranted access.</p>
<p>Technical</p>		
<p>Access Control 164.312(a)(1))</p>	<p><i>Allow access only to those persons or software programs that have been granted access rights as specified in 164.308(a)(4)</i></p>	<p>Varonis addresses these requirements in two key ways:</p> <ol style="list-style-type: none"> 1) Varonis recommends the revocation of permissions to file share data by explicitly and automatically identifying those persons who have no business need to the data for which they have privilege. Varonis system administrators can “commit” the Varonis recommendations through the application 2) Varonis DataPrivilege shifts accountability for data access control from IT to data business owners

		(which Varonis DatAdvantage will help identify). By administering access control through this application business owners record their rationale and the right parties stay informed of actions taken on data.
Audit Controls 164.312(b)	<i>Record and examine activity in information systems that contain or use electronic protected health information.</i>	Varonis provides highly detailed reports including: data use (i.e. every user's every file-touch), user activity on sensitive data, changes including security and permissions changes which affect the access privileges to a given file or folder, a detailed record of permissions revocations including the names of users and the data sets for which permissions were revoked. In fact, because DatAdvantage allows any query or complex query of data use within the application to be saved and generated as a report, the amount and types of information that can be furnished for HIPAA compliance documentation are nearly infinite.
Documentation		
Documentation 164.316(b)(1))	<i>Maintain a written (which may be electronic) record of the action, activity, or assessment.</i>	As stated above Varonis maintains detailed activity records for all user objects including administrators within active directory and all data objects within file systems. Reports on changes are automatically generated and sent to those parties who have chosen to subscribe for receiving this information via email, to PDA etc. These reports can be generated and sent at user defined frequencies so that the appropriate parties become aware of changes in access controls in a timely fashion that is commensurate with the organization's communication policies.

Overview of Varonis Products

Varonis DatAdvantage

The Varonis DatAdvantage software solution aggregates user, data and access event information from directories and file servers. Sophisticated analytics applied to the collected information show detailed data use and determine rightful access based on business need. Specifically, and in a non-intrusive way, Varonis:

- Protects data by recommending removal of overly permissive access controls
- Restricts unstructured data access to those with a business need for that data
- Tracks and monitors every user's every file touch
- Re-computes access controls to account for changes in roles and file server contents

Varonis DataPrivilege

Varonis DataPrivilege makes it possible to transition the responsibility of data entitlement management from IT to business owners without any infrastructure changes or business disruption. Varonis DataPrivilege brings together data owners and data users in a forum for communicating, authorizing and activating entitlements.

DataPrivilege allows you to implement a cohesive data entitlement environment, thereby raising accountability and reducing risk. Upon implementation, Varonis DataPrivilege provides:

- Data protection by reducing errors in entitlement management
- Business need-to-know access control by enabling data owners to make the call
- Access approval rationale capture for refinement and improvement
- Policy and workflow enforcement for consistency and greater security

Sources

<http://www.cms.hhs.gov/SecurityStandard/>

<http://www.wpc-edi.com/hipaa/>

<http://www.ncpdp.org>

<http://www.wedi.org/snip/public/articles/hipaasolution.pdf>

For More Information

sales@varonis.com

877-292-8767

www.varonis.com