Realtime publishers

The Essentials Series:
Fulfilling Compliance by Eliminating Administrator Rights

Fulfilling HIPAA Compliance by Eliminating Administrator Rights

sponsored by

by Greg Shields

Copyright Statement

Fulfilling HIPAA Compliance by Eliminating Administrator Rights

There's a problem with the widespread distribution of administrator rights in your organization, and it has nothing to do with security.

That problem is compliance: Compliance with the industry, governmental, and regulatory statutes that define certain configurations within your IT infrastructure. Although many of those configurations are mandated to enforce a greater level of security control, your job as IT professional is to ensure their fulfillment.

However, similar to the tradeoffs we endure between strong security and total usability, the solid implementation of a compliant configuration often requires a reduction in user flexibility, administrative capability, and merely getting the job of IT done. Nowhere is this more prevalent than in compliance's role in reducing the power and spread of administrative rights.

Understanding HIPAA

The Heath Insurance Portability and Accountability Act (HIPAA) of 1996 was enacted for dual purposes. Its first purpose was to establish a mechanism for employees to retain their health insurance coverage during a job loss or job change. The second arrives through what is known as Title II. In this section, HIPAA enacts national standards for the creation, use, and protection of electronic personal health information (ePHI).

HIPAA requires the creation and management of documented evidence that security policies exist and are being followed. This document should include elements such as network and server configuration, backup and restore procedures and audits, operational procedures, as well as the auditing of user and administrator actions within IT systems.

The majority of HIPAA's requirements that relate to IT systems are contained within section 45 CFR 164, commonly known as "the final rule." This final rule outlines HIPAA's guidance associated with the integrity, availability, and privacy of ePHI. It also outlines guidance associated with authentication to and access control within systems that contain ePHI data, as well as the requirements for auditing such systems. The following list highlights Information about that guidance:

- **Integrity of ePHI Data—45 CFR 164.312(c)(1), (2), & (e)(2)(i).** Technical controls must be implemented that protect ePHI from improper alteration or destruction until it is disposed.
- **Availability of ePHI Data—45 CFR 164.308(a)(7)(ii).** Procedures must be established and implemented that create and maintain retrievable and exact copies of ePHI data. Also, procedures must be established and implemented to restore any lost data.
- **Authentication to ePHI Data Systems—45 CFR 164.312(d).** Systems and/or procedures must be established that verify the person or entity seeking access to ePHI data is the one claimed.
- **Access Control in ePHI Data Systems—45 CFR 164.312(a)(1), (2), & (3).** Systems that contain ePHI data must allow access only to those persons or software programs that have been granted access rights. Unique IDs must be assigned for identifying and tracking users. Sessions must be terminated when they have become inactive.
- **Audit of ePHI Data Systems—45 CFR 164.308(a)(5)(ii)(c) & 164.312(b).** Technical controls must be implemented that record and examine the activity in ePHI data systems as well as procedures that monitor logins and report discrepancies.

The widespread distribution of administrator rights in an organization is at direct odds with these requirements. Such is the case because administrator rights enable complete and unrestricted access to an entire system for the specified user. Additionally, with administrator rights, users can alter system records and generally subvert the requirements for tracking users who access information.

HIPAA, Admin Rights, and the Goal of Least Privilege

As with other compliance regulations, HIPAA's guidance revolves around the protection of personal data through the implementation of technical controls. The controls also protect that data from corruption or change through established systems that enforce data integrity.

IT organizations are also charged with implementing a set of "controls" that restrict the actions of users to just those tasks required by their job roles. Further, when users actually work with business systems, their activities must be monitored and logged into a verifiable database. This task would be easy if it were natively supported by the Windows operating system (OS).

Although not explicitly stated, it is generally accepted that a central goal of HIPAA as well as every other industry, governmental, and regulatory compliance statute is the implementation of Least Privilege. The Principle of Least Privilege was developed more than 30 years ago by the United States Department of Defense (DoD). This principle "requires that each subject in a system be granted the most restrictive set of privileges…needed for the performance of authorized tasks. The application of this principle limits the damage that can result from accident, error, or unauthorized use."

By eliminating administrator privileges from your environment, you are moving that environment towards one that fulfills this principle's goals. You are at the same time going far towards fulfilling the requirements of regulations such as HIPAA.

Yet Least Privilege is more than simply eliminating administrator rights. Least Privilege can more broadly be described as the intersection of the user's role in the organization, the overarching corporate security policy of that organization, and the tasks that are available to be accomplished within the IT infrastructure. In effect, an environment that fulfills the requirements of Least Privilege will be very granularly capable of providing access to each person based on their needs.

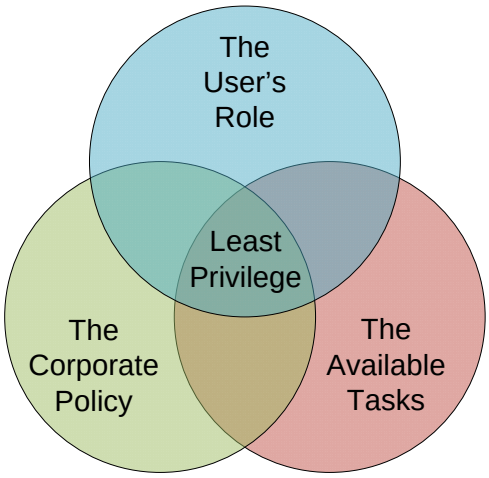

Figure 1: Least Privilege's elimination of administrator rights is really the combination of three factors.

For a comprehensive look at Least Principle's three overlapping requirements as well as how the effective elimination of administrator rights requires the involvement of each, check out *Essentials Series: Eliminating Administrator Rights*, found at http://www.beyondtrust.com/wp_ElimAdminRights_download.aspx?source=Realtime.

Unfortunately, the Microsoft Windows OS alone does not natively provide the architecture to enable this granular control. Using the Microsoft Windows OS, it is possible to eliminate the privileges assigned to an individual. However, these person-based privileges are far too coarse in their application. For example, with poorly-coded applications, simply removing administrator rights from a user may actually prevent needed applications from functioning. Other system configuration changes, like connecting to a local printer, can also require administrative rights, making their removal a problem for the user.

Summary

Organizations that fall under the scope of HIPAA should consider the use of external solutions that extend the granularity of privileges assigned. Such tools enable privileges to be assigned to applications based on user roles, adding that necessary granularity while still fulfilling the requirements of governmental mandates. These tools also provide the right level of audit-friendly logging that tracks user and administrator actions across systems, ensuring you meet your compliance regulations' requirements for activity tracking.