



AUTHOR

Kathleen Rosales
Likewise Software

Using Likewise Enterprise To Improve HIPAA Compliance

Abstract

The HIPAA Security Rule, created to protect electronic patient data, has many requirements for user access control, reporting, auditing, and security. This paper explains how Likewise Enterprise can help you comply with HIPAA.

Likewise integrates Linux, Unix, and Mac OS X workstations and servers into Active Directory, providing the basis to assign each user a unique ID for authentication, authorization, monitoring, and tracking. Likewise also supplies group policies for non-Windows computers so that their security settings and other configurations can be centrally managed in the same way as Windows computers.

The information contained in this document represents the current view of Likewise Software on the issues discussed as of the date of publication. Because Likewise Software must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Likewise, and Likewise Software cannot guarantee the accuracy of any information presented after the date of publication.

These documents are for informational purposes only. LIKewise SOFTWARE MAKES NO WARRANTIES, EXPRESS OR IMPLIED.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in, or introduced into a retrieval system, or transmitted in any form, by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Likewise Software.

Likewise may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Likewise, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2008 Likewise Software. All rights reserved.

Likewise and the Likewise logo are either registered trademarks or trademarks of Likewise Software in the United States and/or other countries. All other trademarks are property of their respective owners.

Likewise Software
15395 SE 30th Place, Suite #140
Bellevue, WA 98007
USA

Table of Contents

Introduction	4
Complying with HIPAA: A Common Problem	4
How Likewise Enterprise Can Help With HIPAA Compliance.....	5
Why Care About A Centralized Identity Management System?	6
How Likewise And AD Foster Compliance With HIPAA.....	7
Centrally Managed User Names, Passwords, and Access Rights	7
One User, One ID.....	10
Granular Access Control	11
Group Policies	12
Logging, Auditing, and Reporting	13
Summary.....	15

Introduction

You have a problem — you want to meet HIPAA requirements and still have the convenience of your computer network.¹ Your mixed network of computers is a never-ending problem because you are unable to secure your computer system. Your employees have multiple accounts and are having a difficult time keeping track of all the passwords, and your IT resources are constantly in use because of all the accounts they need to remove and add. In addition, your employees have unlimited access to patient files and information — but their access should be limited to “the minimum necessary information needed to perform job functions.”¹ Your system’s a mess and you don’t have the funds to keep pouring money into your computer security system. For the millionth time today, you curse HIPAA and wonder if there is an easier way to manage your network security.

Complying with HIPAA: A Common Problem

You are not alone. Small and large companies alike struggle with HIPAA compliance because of their need to quickly access patient files while maintaining a completely secure network. Current HIPAA regulations require that you protect against “any reasonably anticipated threats or hazards to the security or integrity of [health] information”² and “reasonably anticipated uses or disclosures of information that are not permitted or required,”³ but meeting these criteria is not easy.⁴

Hospitals and medical offices spend endlessly in their quest to comply with the HIPAA Security Rule’s technical safeguards. “The Security Rule [titled Security Standards for the Protection of Electronic Protected Health Information] defines technical safeguards in §164.304 as ‘the technology and the policy and procedures for its use that protect electronic protected health information and

¹ “Security Standards: Technical Safeguards.” HIPAA Security Series March 2007: 2-4. Centers for Medicare and Medicaid Services. 8 Oct. 2008. <<http://www.cms.hhs.gov/EducationMaterials/Downloads/SecurityStandardsTechnicalSafeguards.pdf>>.

² “Protecting the Privacy of Patients’ Health Information,” April 2003. US Department of Health and Human Services. 8 Oct. 2008 <<http://www.hhs.gov/news/facts/privacy.html>>

³ “Protecting the Privacy of Patients’ Health Information,” April 2003. US Department of Health and Human Services. 8 Oct. 2008 <<http://www.hhs.gov/news/facts/privacy.html>>

⁴ §164.306(a)(2) and §164.306(a)(3).

control access to it’.”⁵ You have a problem because, with your mixed network, you are unable to secure your computer system. In fact, compliance could be nearly impossible because, with so many passwords and user names to keep track of, you are never certain that your network is secure.

How Likewise Enterprise Can Help With HIPAA Compliance

For many businesses, compliance is difficult because they use different identity management systems for different operating systems: Windows users might authenticate through Active Directory, Linux and Unix users might authenticate through NIS, and Mac OS X users might authenticate through an ad hoc Kerberos key distribution center. Different identity management systems for different operating systems can create confusion when a user leaves or joins the company because you have to update your identity management systems separately—leading to security holes. Security holes can create problems for healthcare corporations because of the sensitive information their servers protect. You don’t want to be the hospital whose employee leaked Britney Spears’ or Maria Shriver’s health information to the press, as has happened in California. Thus, you have to find a solution to your multi-platform identity management system problem.

Likewise can help you with your network problem. Likewise integrates Linux, Unix, and Mac OS X computers with Microsoft Active Directory (AD), enabling you to securely authenticate Linux and Unix users, control their access to customer data, and apply group policies to manage password policies and root access. Altogether, the centralization of your identity management system creates a streamlined user account management system and improved security.

⁵ “Security Standards: Technical Safeguards.” HIPAA Security Series March 2007: 2-4. Centers for Medicare and Medicaid Services. 8 Oct. 2008. <<http://www.cms.hhs.gov/EducationMaterials/Downloads/SecurityStandardsTechnicalSafeguards.pdf>>.

Why Care About A Centralized Identity Management System?

HIPAA contains security technical safeguards to protect electronic information. The security technical safeguards generally “apply only to PHI”⁶—protected health information.

Protected health information (PHI) is the HIPAA term for health information in any form (i.e., paper, electronic or verbal) that *personally identifies* a patient. This includes individually identifiable health information in paper records that have never been electronically stored or transmitted. It does not include data that have been ‘dis-identified’ by removal of identifying information, such as name, address, ZIP code, etc.⁷

Based on this definition, PHI could be patient records that contain social security numbers, date of birth, and a spouse’s name — information that could be valuable in the hands of a person who invades your computer system. Because of your multi-platform identity management system, your computer system is probably not as secure as HIPAA requires it to be. But how do you know if your system complies with HIPAA? You should be able to answer the following questions:

- How can we tell if an unauthorized user accessed PHI through the practice's computers or networks? What safeguards are in place to prevent unauthorized access?
- What activities need to be monitored and logged, and what level of detail is reasonable and appropriate?
- What technology is in place to assure the true identity of (i.e., to "authenticate") users? What about passwords and IDs? Digital signatures? Telephone callback?
- How often does the system issue prompts to change passwords? Has staff been trained to create hard-to-break passwords?
- How much risk of message interception or unauthorized access to PHI is posed by the practice's use of wide-area networks or the Internet?

⁶ Kibbe M.D., David C. “A problem Oriented Approach to the HIPAA Security Standards.” Family Practice Management. July/August 2001. 8 Oct. 2008. <<http://www.aafp.org/fpm/20010700/37apro.html>>

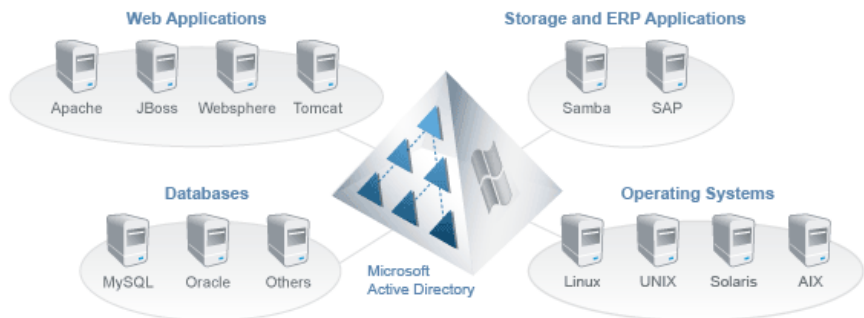
⁷ Ibid.

⁸ Ibid.

If you cannot answer these questions, it is time to consider improving your security by installing Likewise Enterprise and creating a centralized identity management system. Likewise lets you to answer most of these questions affirmatively because you can control access to computers, assign unique user identifications on a cross-platform system, log access to files based on user identification, restrict access based on group membership, centralize authentication, restrict facility access from unauthorized remote access users, and manage passwords — elements needed for HIPAA compliance.

How Likewise And AD Foster Compliance With HIPAA

The cornerstone of Likewise is that it joins Linux, Unix, and Mac OS X computers to Microsoft Active Directory – a secure, scalable, stable, and proven identity management system.



Joining non-Windows computers to Active Directory gives you the power to manage all your users' identities in one place, use the highly secure Kerberos 5 protocol to authenticate users in the same way on all your systems, apply granular access controls to sensitive resources, and centrally administer Linux, Unix, Mac, and Windows computers with group policies. You can seamlessly manage both Windows and non-Windows computers within Active Directory.

Centrally Managed User Names, Passwords, and Access Rights

Central management of unique user accounts is important. HIPAA has specific requirements for managing your information and data systems.

According to SystemsExperts' consultants Jonathan Gossels and Landon Curt Noll:

Healthcare organizations will need to establish and maintain the following security services:

- Healthcare information and data access controls based on “need to know”
- System and network activity and access audits. . .
- Healthcare data integrity validation
- Authentication and validation of identity of an entity accessing healthcare data⁹

Likewise Enterprise helps you meet these expectations. It lets you create unique user accounts, manage and log accounts' access to PHI, create system reports for auditing needs, review healthcare data integrity validation, and securely authenticates users for single sign-on.

HIPAA Requirement	Likewise Support
Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident-tracking reports	Likewise enables you to track which users log on systems that contain protected data, create detailed reports for auditing, and review password attempts by account.
Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information . . . and to prevent those workforce members who do not have access ... from obtaining access to electronic protected health information.	Implementing Likewise Enterprise with Active Directory creates a centralized identity management system, providing the technology to put in place a variety to access control mechanisms.

⁹ Gossels, Jonathan and Landon Curt Noll, “HIPAA Compliance.” A Perspective on Practical Security 2004. SystemsExperts Corporation. 9 Oct. 2008 <<http://www.systemexperts.com/tutors/HIPAA%20Overview.pdf>>.

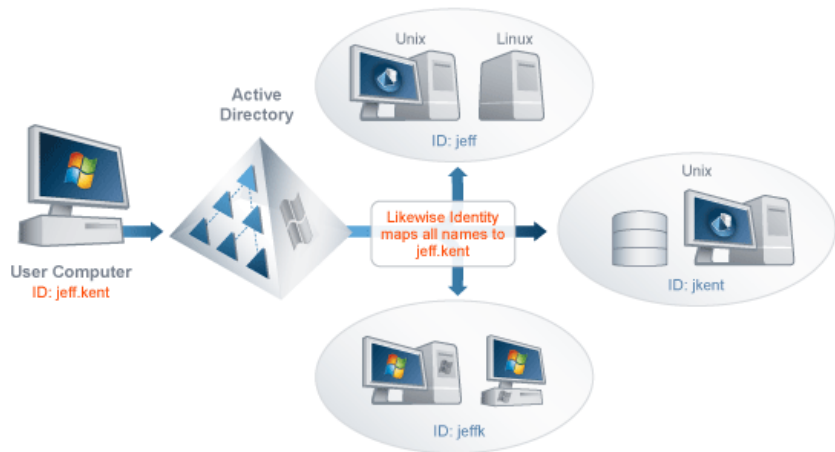
HIPAA Requirement	Likewise Support
<p>Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends. . .</p>	<p>The Likewise Console generates reports that identify disabled accounts. You can then simply delete the account from Active Directory.</p>
<p>Implement policies and procedures for granting access to electronic protected health information, for example through access to a workstation, transaction, program process or other mechanism.</p>	<p>Likewise and Active Directory give you not only secure authentication for applications and users but also single sign-on: Users authenticate once against the Active Directory database and receive a Kerberos ticket-granting ticket. Users can then seamlessly obtain authenticated access to other resources, including databases, for which they are authorized.</p>
<p>Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.</p>	<p>Likewise gives you the ability to establish, document, review, and modify a user's right of access through its centralized identity management system.</p> <p>Judicious use of Likewise cells provides a convenient way of controlling or changing access to different classes of Unix, Linux and Mac OS X computers.</p> <p>Likewise includes additional methods for controlling or modifying access: setting an allow logon rights group policy, specifying logon hours, using logon lists, and disallowing logons</p>

HIPAA Requirement	Likewise Support
	<p>by individual users.</p> <p>Likewise can generate a variety of access reports to show which users and groups have access to which computers. The reports can be output in several formats to help document users' access rights.</p> <p>Likewise also includes a category of reports geared specifically for compliance efforts.</p>

One User, One ID

One main requirement of HIPAA is that every user has a unique name or number with which to access patient data. By using Likewise with Active Directory, you can easily do just that –for both Windows users and Linux and Unix users. Active Directory makes ID assignment simple: one ID, one user. Likewise extends that functionality to Linux, Unix, and Mac OS X users. With one unique ID stipulated and centrally managed through Active Directory, a user can log on Windows, Unix, Linux, and Mac OS X computers with an encrypted password that is securely authenticated against the Active Directory database.

More: You can assign each user a unique ID in Active Directory while maintaining your NIS domain user information. When you migrate Linux and Unix users from NIS domains to Active Directory, Likewise uses *cells* to preserve the user information in your NIS domains. A cell provides a custom mapping of a unique and identifiable Active Directory user to that user's UIDs and GIDs, as illustrated by the following diagram:



HIPAA Requirements	Likewise Feature Support
Implement electronic mechanisms to collaborate that electronic protected health information has not been altered or destroyed in an unauthorized manner	Likewise allows you control user access to PHI— a capability that allows you to eliminate unauthorized destruction of PHI before it happens.
Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed	Active Directory can control access to all system components at the level of the user. Individual users can be authorized for access to system components at a granular level.
Assign a unique name and/or number for identifying and tracking user identity.	Active Directory assigns a unique user name to each user. The user name can then be used on all the computers that are joined to Active Directory. In addition, Likewise lets you assign multiple UIDs to a single user to maintain NIS domain information.

Granular Access Control

HIPAA Security Standards require that user access be controlled based on necessity. With Likewise and Active Directory, you can use your pre-existing

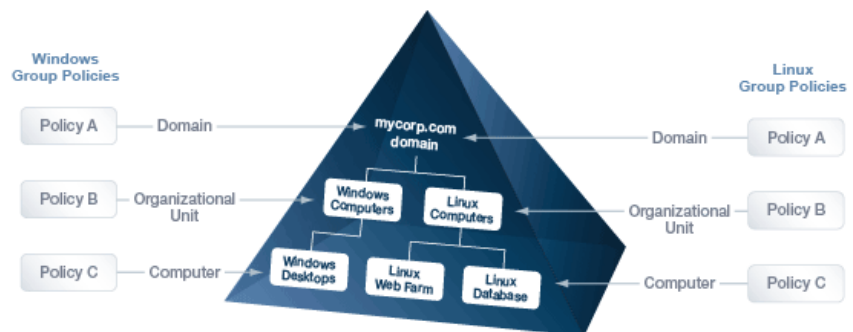
UIDs and GIDs to control access to patient data at a granular level. By mapping SIDs to UIDs and GIDs, Likewise makes Active Directory's granular access control available to Unix, Linux, and Mac OS X computers, users, and groups.

In addition, Likewise cells can provide a convenient way of controlling access to different classes of Unix, Linux and Mac OS X computers.

Likewise Enterprise includes additional methods for controlling access: specifying logon hours, using logon lists, and disallowing logons by individual users.

Group Policies

To meet HIPAA compliance standards, you must guard your patients' information against unauthorized access. With Likewise, you can centrally manage the security settings on non-Windows systems by using the Group Policy Object Editor and the Group Policy Management Console to create group policies and then apply them to computers running Linux, Unix, and Mac OS X. Likewise comes with more than 100 group policies for Linux, Unix, and Mac OS X computers, including policies for setting security parameters. Likewise applies group policies to Linux and Unix systems in the same way that Active Directory applies group policies to Windows systems:



Likewise group policies can also be used to help comply with HIPAA's requirement that you "allow access only to those persons or software programs that have been granted access rights . . ." ¹⁰ Likewise can help you with this requirement by allowing you to control access to computer resources with a group policy that allows or disallows logon rights by user or group.

¹⁰ §164.308(a)(4)

HIPAA Requirements	Likewise and AD Feature Support
Protect against any reasonably anticipated threats or hazards to the security or integrity of [protected health information]	Likewise provides group policies to manage files, directories, symbolic links, file system mounts, cron jobs, and scripts which allow for advanced access control settings. Likewise includes a group policy for applying sudoers configuration files to all the computers in your network.
Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights . . .	A Likewise group policy can control access by allowing or disallowing logon rights.
Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity	Likewise provides a number of group policies for controlling the screen saver, including policies that lock the system after a set number of idle minutes.

Logging, Auditing, and Reporting

HIPAA requires audit controls. “The Audit Controls [require] a covered entity to: ‘Implement hardware, software, and or procedural mechanisms that record and examine activity in information systems that contain or use electronic health information.’”¹¹ Likewise can help you comply with HIPAA-required

¹¹ “Security Standards: Technical Safeguards.” HIPAA Security Series March 2007: 2-4. Centers for Medicare and Medicaid Services. 8 Oct. 2008. <<http://www.cms.hhs.gov/EducationMaterials/Downloads/SecurityStandardsTechnicalSafeguards.pdf>>.

audit controls by providing you with the ability to log individual access to your information system — enabling you to examine access activity of an individual user.

In addition to its logging capabilities, Likewise enables you to create custom reports about Linux and Unix users, groups, computers, forests, and domains within Active Directory. You can choose the information you want to include in a report by selecting from a variety of report options. Depending on the type of report, you can select different columns for users, groups, computers, and cells. When you generate a User Access report, for example, you can select from such report options as Login Name, Unix Login Name, User Status, UID, Primary GID, Gecos, Login Shell, and Home Directory.

Each type of report includes filters and options. All the reports let you filter by domain. Depending on the type of report that you create, you can choose whether to show disabled users or disabled computers. For some reports you can limit the number of objects by specifying a maximum number of computers per group.

After you generate a report, you can view, save, preview, and print it. Likewise outputs the report data in a variety of formats.

HIPAA Requirement	Likewise Feature Support
Implement hardware, software, and or procedural mechanisms that record and examine activity in information systems that contain or use electronic health information	Event logs can record individual access to your information system. In turn, this allows you to examine access activity of an individual user.
Implement policies and procedures to protect electronic protected health information from improper alteration or destruction	Event logs that record access to your information system can help you protect health information from improper alteration or destruction because you can review activity by user.
Log-in monitoring (Addressable). Procedures for monitoring log-in attempts and reporting discrepancies	The Active Directory event log can track individual user access to patient data. Also, you may decide to create a group policy that can enforce password history on computers that are joined to Active Directory.
Password management (Addressable)	By using Likewise with Active

Procedures for creating, changing, and safeguarding passwords	Directory, you can enforce security settings for passwords, including password change intervals.
Implementation specification: Response and Reporting (Required). 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.	With Active Directory, a group policy can specify the account lockout threshold — the number of invalid logon attempts before the account is locked.

Summary

To foster compliance with HIPAA, Likewise integrates Linux, Unix, and Mac computers into Active Directory – a stable, secure, and scalable identity management system.

Likewise lets you not only join non-Windows computers to Active Directory but also migrate Linux, Unix, and Mac users to Active Directory while maintaining their identities and permissions.

Once you have joined non-Windows computers to Active Directory and migrated your users, Likewise and Active Directory can help you comply with a number of key HIPAA requirements, including the following:

- Track every user with a unique name or number: Assign a single ID and password to each user and then use that ID to monitor and track the user.
- Authenticate the encrypted passwords of users and groups with the highly secure Kerberos authentication protocol.
- Authorize and control access to resources, including those that contain protected health information.
- Monitor user logons by tracking individual user access to patient data.

- Apply group policies, such as for sudo configuration files and for password settings, to help bring Linux, Unix, and Mac computers into compliance with HIPAA requirements.

The combination of Likewise and Active Directory can help you comply with many of the HIPAA requirements by providing you with a proven identity management system, central management of your heterogeneous network, improved security, and advanced reporting capabilities.

ABOUT LIKewise

Likewise Software is an open source company that provides audit and authentication solutions designed to improve security, reduce operational costs and help demonstrate regulatory compliance in mixed network environments. Likewise Open allows large organizations to securely authenticate Linux, UNIX and Mac systems with a unified directory such as Microsoft Active Directory. Additionally, Likewise Enterprise includes world-class group policy, audit and reporting modules.

Likewise Software is a Bellevue, WA-based software company funded by leading venture capital firms Ignition Partners, Intel Capital, and Trinity Ventures. Likewise has experienced management and engineering teams in place and is led by senior executives from leading technology companies such as Microsoft, F5 Networks, EMC and Mercury.