



Protect the Privacy
of **Electronic Health Records**
with Netwrix Auditor



Table of Contents

Executive summary	3
1. Proactively detect incidents endangering health information	4
1.1 Avoid unnecessary risk by cleaning up user and computer accounts	5
1.2 Ensure legitimate access to eHR by controlling group membership	6
1.3 Avoid unwarranted privilege escalation and data exfiltration by controlling permissions	7
1.4 Safeguard patient data by promptly detecting abnormal user activity	8
1.5 Uncover potentially malicious intentions by reviewing logon activity	9
1.6 Identify access policy violations by looking at failed activity	10
2. Streamline investigations with enterprise-wide visibility	11
2.1 Simplify investigations of what actually happened in every part of your environment	12
2.2 Add more context to your investigations by pinpointing specific data	12
2.3 Establish accountability with intelligence about individual user activity	13
3. Demonstrate the effectiveness of your controls and excel at passing compliance audits	14
3.1 Prepare for internal and external assessments faster	15
3.2 Meet auditors' expectations	16
3.3 Minimize the complexity and stress of getting started with compliance	17
Conclusion	18
About Netwrix	19

Executive Summary

Healthcare is one of the most highly regulated industries in the world, and for good reason: The integrity of personal health information (PHI) can be critical to patient outcomes. Moreover, healthcare organizations collect and store not only PHI but large amounts of other personally identifiable information (PII). Both PHI and PII command a very high value on the shadow markets, which makes hospitals, medical centers and other healthcare facilities an attractive target for cyber attacks.

Accordingly, ensuring data security is the top priority for the IT departments in many of these healthcare organizations and their business associates. Unfortunately, the number of breaches occurring in the healthcare industry demonstrates an urgent need for better measures to ensure the confidentiality, integrity and availability of electronic health records (eHR).

Netwrix Auditor is a visibility and governance platform for hybrid cloud security that over 630 businesses in the healthcare sector worldwide already use to minimize risks to their sensitive information and successfully pass regulatory audits. You can, too.

This eBook details how Netwrix Auditor can help your healthcare organization become more resilient to the cyber threats that endanger your **highly sensitive PHI** — and also help you prepare for and successfully pass regulatory compliance audits. Read on for answers to all of the following important questions:

- How can your healthcare organization become more resilient to the cyber threats that endanger your highly sensitive PHI?
- How can you detect vulnerabilities in your security posture and spot attacks early?
- How can you ensure individual accountability and help prevent policy violations?
- How can you more effectively prepare for and pass compliance audits?

1. Proactively detect incidents endangering health information

A critical first step in reducing risk to patient data is controlling your user and computer accounts, user groups, and permissions in accordance with modern security best practices. A clean house with no mess reduces the possibility of unintentional unauthorized access to sensitive data, limits the scope of damage in case of intentional violations and facilitates the timely detection of attacks.

You also need to be vigilant for signs of improper or otherwise suspicious activity that could threaten your eHR. You need to be able to capture everything that happens in your IT infrastructure, quickly distill out important events, relate things into a coherent picture, and identify both threats in action and opportunities for an attack.

Netwrix Auditor makes it easy for you to stay current on the actual state of your accounts, groups and permissions, and monitor all changes to those entities, so you can keep them clean and in good condition. The product also provides comprehensive reporting that greatly simplifies the task of detecting existing and potential threats.



Because we deal with protected health information, confidentiality and integrity are vital issues for us. Prior to our decision to deploy Netwrix Auditor, visibility into changes to our SQL Server and touches to sensitive data was not nearly at the level we wanted it to be. Netwrix Auditor gave us full visibility into SQL Server changes, down to specific database columns and rows, instead of the “localized visibility” that we had with the previous system.



1.1 Avoid unnecessary risk by cleaning up user and computer accounts

Poor control over user and computer accounts is the first thing you need to tackle in order to reduce the exposure of your high-value health records to today's advanced threats. Netwrix Auditor facilitates the task of verifying account integrity and remediating issues with accounts for improved security. Predefined reports provide the total count of existing accounts with critical details like path, status, last logon time and more. Furthermore, you can check the state of user accounts at any particular moment in the past by choosing a historical snapshot.

User Accounts				
Shows user accounts, their paths, logon names, statuses (enabled or disabled), and last logon time.				
Total Enabled: 9				
Total Disabled: 23				
Total Count: 32				
Path	Name	Logon Name	Status	When
\com\enterprise \Inactive Users\Alex Terry	Alex Terry	A.Terry	Disabled	23/10/2016 7:56:44 AM
\com\enterprise \Users\Anna Watson	Anna Watson	A.Watson	Enabled	28/11/2016 10:12:32 AM
\com\enterprise \Users\Administrator	Administrator	Administrator	Disabled	30/09/2016 11:05:17 AM

Netwrix Auditor also enables you to quickly find and analyze all inactive, locked and expired accounts. Plus, it helps you spot potential account misuse and policy violations by providing reports like Temporary User Accounts, Temporary Users in Privileged Groups, Recently Enabled Accounts and others.

Inactive Users in Active Directory Report				
The following accounts are no longer active:				
Account Name	Account Type	E-Mail	Inactivity Time	Account Age
A.Kowalski	User	A.Kowalski@enterprise.com	33 day(s)	307 day(s)
S.Parker	User	S.Parker@enterprise.com	37 day(s)	311 day(s)
D.Lopez	User	D.Lopez@enterprise.com	40 day(s)	77 day(s)
R002312	User	None	21 day(s)	400 day(s)
T.Simpson	User	T.Simpson@enterprise.com	10 day(s)	255 day(s)

1.2 Ensure legitimate access to eHR by controlling group membership

Ensuring proper group membership is another “golden rule” that helps you safeguard your sensitive eHR. While there are legitimate reasons for changes to group membership, such as employees changing roles within the organization, other changes can signal an illicit attempt to escalate a user’s privileges. Netwrix Auditor makes routine review and validation of group membership much easier by providing reports like Effective Group Membership, Administrative Group Members and others.

Effective Group Membership

Lists user and computer accounts that belong to a specified group, the status (enabled, disabled) for each account, and whether the account was explicitly named as a member of the group or was included implicitly through group membership.

Name	Member Through	Type	Status
Administrator	Explicit	user	Disabled
Anna Kowalski	Explicit	user	Disabled
Anna Watson	Explicit	user	Enabled
Danny Johnson	Explicit	user	Enabled
Elena Anderson	Explicit	user	Enabled
Garry Brown	Explicit	user	Disabled
John Carter	Explicit	user	Enabled

Certain group membership changes signal a very likely threat to PHI safety. In particular, it is unusual for a user account to be deleted soon after it was created and added to privileged groups; this can indicate a rogue employee or an outsider trying to obtain extended privileges and cover their tracks. Netwrix Auditor enables you to spot such threats with the Temporary Users in Privileged Groups report.

Temporary Users in Privileged Groups

Shows user accounts deleted soon after they were created and added to privileged groups, such as Domain Admins, Enterprise Admins, Schema Admins, Account Operators, and other groups you specified. Use this report to detect intruders attempting to hide malicious activity.

Name	When Created	Who Created	When Removed	Who Removed
enterprise.com /Garry Smith	1/12/2016 1:27:58 AM	ENTERPRIS \J.Carter	1/12/2016 1:29:34 AM	ENTERPRIS \J.Carter
Group Name: \com\enterprise\Users\Domain Admins				
enterprise.com /Richard Smith	1/12/2016 1:30:13 AM	ENTERPRIS \J.Carter	1/12/2016 1:32:42 AM	ENTERPRIS \J.Carter
Group Name: \com\enterprise\Users\Domain Admins				

1.3 Avoid unwarranted privilege escalation and data exfiltration by controlling permissions

Excessive access permissions put patient data at increased risk of disclosure or destruction. Netwrix Auditor helps you enforce a least-privilege model with proper role separation and temporary permissions assignments by making it easy to find users with permissions that are not relevant to their roles or not appropriate for specific tasks.

Excessive Access Permissions

Shows accounts with permissions for infrequently accessed files and folders. Use this report for spotting unnecessary permissions and preventing data leaks. Track permissions assigned to accounts directly or by group membership.

Object: \\fs1\Patient History (Permissions: Different from parent)

Account	Permissions	Means Granted	Times Accessed
ENTERPRISE\N.Key	Full Control	Directly	0
ENTERPRISE\T.Simpson	Full Control	Group	0
ENTERPRISE\P.Anderson	Full Control	Group	0
ENTERPRISE\K.Miller	Write and list folder content	Directly	0
ENTERPRISE\T.Allen	Read (Execute, List folder content)	Group	0

Protecting assets containing sensitive medical records requires regular review of what level of permissions is granted to which account holders. Netwrix Auditor provides an easy way to see who can access specific sensitive shares and folders, what permissions those users have, and whether their access rights were inherited or explicitly assigned. Historic snapshots enable you to see permissions at a particular moment in the past and compare them with the current setup or your established baselines.

Object Permissions by Object

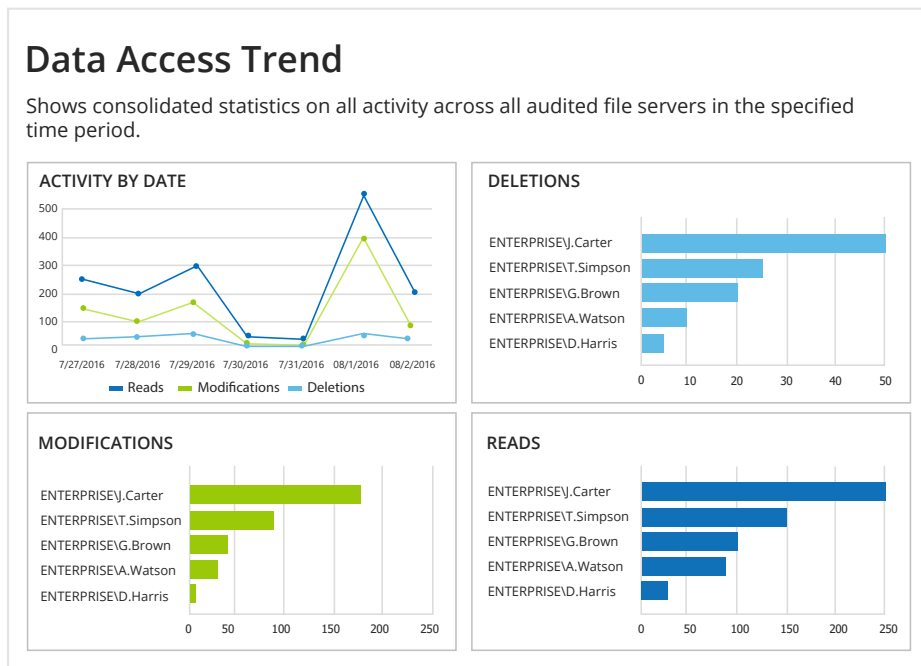
Shows file and folder permissions granted to accounts (either directly or via group membership), grouped by object path. Use this report to see who has access to files and folders, and determine whether the set of permissions on an object is the same or different from its parent.

Object: \\fs1\Shared (Permissions: Different from parent)

Account	Permissions	Means Granted
ENTERPRISE\A.Kowalski	Full Control	Group
ENTERPRISE\A.Watson	Full Control	Group
ENTERPRISE\Administrator	Full Control	Group
ENTERPRISE\G.Brown	Full Control	Group
ENTERPRISE\J.Carter	Read (Execute, List folder content)	Directly
ENTERPRISE\P.Anderson	Full Control	Group
ENTERPRISE\T.Simpson	Full Control	Directly
fs1\Administrator	Full Control	Group

1.4 Safeguard patient data by promptly detecting abnormal user activity

Any sudden burst of activity — like bulk file reads, modifications or deletions — can be a sign of an active threat to the safety of your PHI. The challenge is staying aware of these activity spikes. Netwrix Auditor’s Data Access Trend and File Servers Overview dashboards keep you informed so you can protect your data.



You also need to respond quickly to the deletion of data from your critical directories, SQL and Oracle databases, and SharePoint sites. To protect your PHI, use Netwrix Auditor’s predefined reports to promptly detect these threats and notify the affected employees or staff who are better acquainted with the situation. Other reports help you keep an eye on data modifications and additions and thereby ensure that personal health records are not processed outside of proper workflows.

Files and Folders Deleted

Shows removed files and folders with their attributes.

Action	Object Type	What	Who	When
Removed	File	\\fs1\Out-patient \ClinicalRecords2016\J.Smith.rtf	ENTERPRISE\J.Carter	7/18/2016 5:02:02 PM
Where:	fs1			
Removed	File	\\fs1\MaternityUnit\Births \T.Kelly.rtf	ENTERPRISE\J.Carter	7/18/2016 5:02:03 PM
Where:	fs1			
Removed	File	\\fs1\Traumatology\Statistics \Report_spring_03.01.2016.xlsx	ENTERPRISE\J.Carter	7/18/2016 5:02:04 PM
Where:	fs1			

1.5 Uncover potentially malicious intentions by reviewing logon activity

Thorough review of logon events can help reveal threats to sensitive PHI; however, capturing and analyzing this information can be a tedious process. Netwrix Auditor makes it easier by providing visibility into all logon activity across multiple IT systems in your environment. It tracks and reports all interactive and non-interactive logons, both successful and failed. Each logon record is packed with valuable details and can be referenced later if questionable activities are detected on your network.

All SQL Server Logons

Shows successful and failed attempts to connect to a SQL Server instance through Windows or SQL Server authentication. Use this report to analyze user activity on production databases and validate compliance.

Action	Logon Type	Who	When
Successful Logon Where: Workstation:	Windows logon sql1\sqldb1 172.17.34.21	ENTERPRISE\T.Simpson	9/10/2016 3:43:54 PM
Successful Logon Where: Workstation:	Windows logon sql1\sqldb1 172.17.44.31	ENTERPRISE\J.Carter	9/10/2016 5:32:15 PM
Failed Logon Where: Workstation:	SQL logon sql1\sqldb1 172.17.34.25	ENTERPRISE\A.Watson	9/10/2016 5:56:12 PM

Certain types of logon events require constant vigilance. In particular, logons at unusual times, multiple logons during a short time period, logons from non-typical endpoints and repeated failed logon attempts are red flags that can signal malicious insider activity, user impersonation or robotic intrusion attempts. Netwrix Auditor helps you detect those events by providing reports such as Logons by Single User from Multiple Endpoints, Logons by Multiple Users from Single Endpoint, Accounts with Most Logon Activity and others.

Logons by Single User from Multiple Endpoints

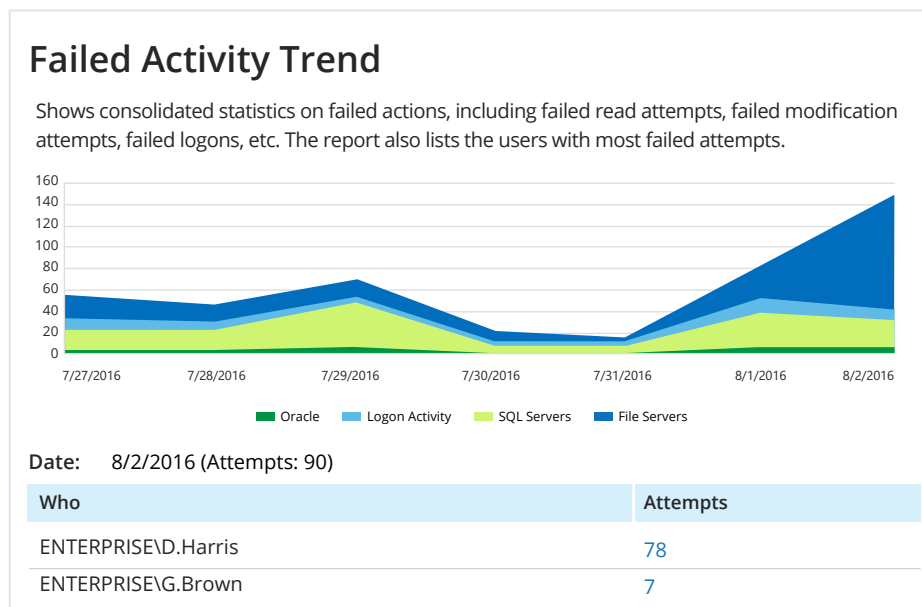
Shows users who logged on from several endpoints within a short period of time. Such occurrences may indicate that the account's password was stolen or compromised. Use this report to detect suspicious user activity and prevent data breaches.

User: [ENTERPRISE\J.Carter](#) (First Attempt: 7/27/2016 2:02:26 PM)

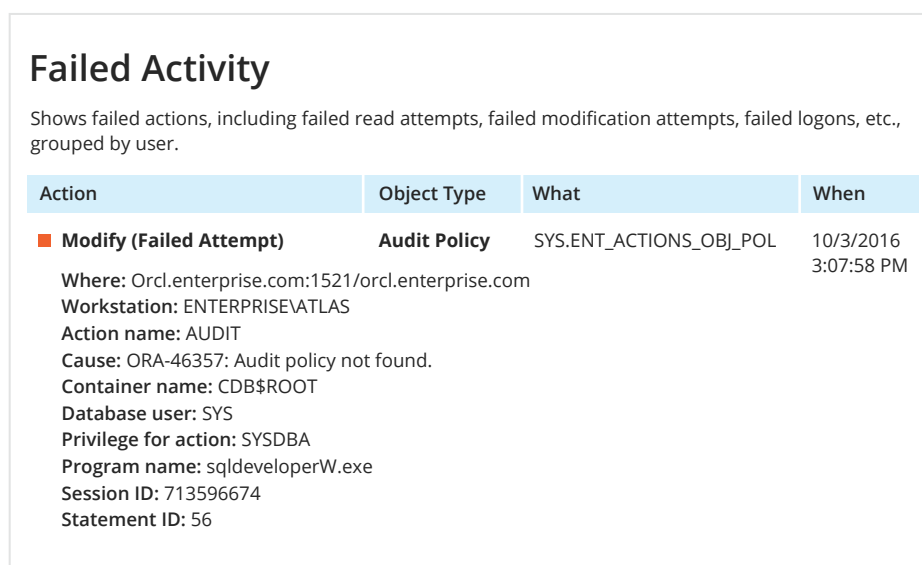
Endpoint	Logon Attempts
172.17.6.36	2
ENTWKS0376	6
WST055	12
192.168.1.1	1

1.6 Identify access policy violations by looking at failed activity

In any environment, ordinary user errors produce a certain level of failed reads, modifications, deletions, additions and so on. However, a sudden spike or a steady increase in failed activity can indicate malicious attempts to access sensitive PHI. Netwrix Auditor helps you determine the normal level of failed actions for your organization and detect suspicious trends. Plus, the Failed Activity Trend dashboard identifies the users with the most failed attempts and enables you to drill down and review their actions in detail.



It's especially important to promptly detect failed attempts to access, alter, copy or remove data on your protected databases and network drives, because that's where sensitive medical records and PII are typically stored. Netwrix Auditor facilitates the process of reviewing failed activity in your critical data repositories, such as Oracle Database and file servers, to help you safeguard your ePHI.



2. Streamline investigations with enterprise-wide visibility

As we've seen, Netwrix Auditor helps you protect your sensitive health information by identifying threats across your IT environment. But the solution doesn't stop there. Effective and timely response to a threat or an incident requires being able to quickly conduct a thorough investigation and establish user accountability. You need to be able to easily navigate through reams of audit data to find the specific information you require. This information must be credible and consistent, and you need to be able to tie all of the evidence together into a coherent whole.

Netwrix Auditor makes security investigations more efficient by providing meaningful intelligence based on the comprehensive data the product collects. It enables you to see exactly what actions have been taken throughout your IT environment, step by step, so you can reconstruct events with all the relevant context to determine whether a particular issue is a malicious attack or a simple mistake. With Netwrix Auditor, you are always ready to promptly address any incident, enforce your security policies and hold individuals accountable for their actions.



When a problem starts occurring, you can go through the event logs, but with so many entries to go through, that's like looking for a needle in a haystack. And oftentimes you don't even come up with the data that you really need. With Netwrix Auditor, it is much easier to do the investigation and single out a possible answer to the question of why something happened.



2.1 Simplify investigations of what actually happened in every part of your environment

All too often, blind zones and fragmented visibility leave investigators struggling to piece together the true history of a security incident. Netwrix Auditor transforms obscurity into a complete picture of who did what, when and where, with predefined reports that provide evidence enriched with valuable details. The reports can either make a particular user, system or activity the focus of attention, or detail everything that happened across multiple systems, simplifying investigations.

User Account Status Changes

Shows changes to user accounts status (enabled, disabled, locked, unlocked).

Total Count: 32

Who: ENTERPRISE\DC1\$

Action	What	When
■ Locked Domain Controller: dc1.enterprise.com Workstation: WIN-460JH7MQNFT	\\Enterprise\Users\Domain Admins	8/22/2016 1:13:26 PM
■ Locked Domain Controller: dc1.enterprise.com Workstation: WIN-74HTEGDHOYE	\\com\enterprise\Users\Guest	10/14/2016 3:36:00 PM

2.2 Add more context to your investigations by pinpointing specific data

When you find an unusual or alarming event that could threaten the safety of sensitive health records, you need to deeply investigate the issue and get as much relevant context as possible to make your incident response more effective. Netwrix Auditor provides a powerful search engine that makes it easier to quickly determine the true scope and severity of an issue.

← Search
WHO
ACTION
WHAT
WHEN
WHERE

⚙ Audited system "Oracle Database" x "SQL Server" x Admin

SEARCH

Who	Object type	Action	What	Where	When
ENTERPRISE\J.Carter	Login	■ Modified	Security\Logins\[Enterprise]J.Carter]	sql1.enterprise.com	11/7/2016 03:50:04 AM
Server Roles: - Added: "securityadmin;serveradmin;setupadmin;processadmin"					
ENTERPRISE\J.Carter	Server Role	■ Modified	Security\Server Roles\serveradmin	sql1.enterprise.com	11/7/2016 03:50:04 AM
Role Members: - Removed: "ENTERPRISE\T.Simpson"					

2.3 Establish accountability with intelligence about individual user activity

Securing patient data requires keeping physicians, contractors, business associates and highly privileged IT staff accountable for their actions. Netwrix Auditor can capture the screen activity of users in any applications, including those that do not generate logs. This capability helps you deter abusive insider activity, detect unauthorized actions and improve accountability.

Activity Records

Generate a summary of video records

Date 9/25/2016

Computer	User	Start Time	End Time	Duration
dc1.enterprise.com	ENTERPRISE\J.Smith	9/25/2016 4:12 PM	9/25/2016 4:17 PM	00:05:15
dc1.enterprise.com	ENTERPRISE\J.Smith	9/25/2016 5:12 PM	9/25/2016 5:13 PM	00:01:15

Netwrix Auditor user behavior and blind spot analysis reports, such as the Activity Outside Business Hours report, help you hold individuals accountable for any deviations from policy by providing evidence of their actions.

Activity Outside Business Hours

Shows users who performed any actions outside their business hours. Use this report to detect suspicious user activity.

User Name	Actions
ENTERPRISE\D.Harris	663
ENTERPRISE\J.Carter	44
ENTERPRISE\T.Simpson	21
ENTERPRISE\A.Watson	15
ENTERPRISE\G.Brown	8

3. Demonstrate the effectiveness of your controls and excel at passing compliance audits

Every organization that handles personally identifiable information or private healthcare information must comply with many laws and regulations. Failing official audits usually results in large fines and damage to the organization's reputation. Internal self-assessments are a wise first step, but proving compliance is never a piece of cake. Auditors are seldom satisfied to simply see what your policies state; they usually have established specific expectations and baselines that require response in action. In other words, to pass audits, you need to be able to demonstrate the effectiveness of your security measures in operation.

Netwrix Auditor helps healthcare organizations address many checkbox items in auditors' lists by enabling the vigilance required to manage risks to sensitive PHI. It provides extensive compliance reports out of the box, along with a variety of additional compliance features. As a result, Information Security staff work far more efficiently, both before and during assessments, which results in faster, less painful checks and improved grades with the regulators.



We are always busy trying to make things better and ensure simple yet safe procedures for our employees and patients. Netwrix Auditor enables us to see both the big picture of what is happening in our environment and what is going on in each specific application, which helps us achieve those goals and also helps in our compliance process.



3.1 Prepare for internal and external assessments faster

Preparing for approaching audits is usually a time-consuming and stressful process. Netwrix Auditor simplifies the task of pulling out and preparing data that is likely to be requested by auditors, reducing preparation time and effort. The Interactive Search feature can help you create custom reports that answer potential questions in your auditors' checklists, and you can save those reports for immediate access during actual assessments.

← Search
WHO
ACTION
WHAT
WHERE
WHEN

⚙️ Object type "Group" ×
🕒 When "Last 30 days" ×

SEARCH

Who	Object type	Action	What	Where	When
T.Simpson@enterprise.onmicrosoft.com	Group	■ Added	HR	https://enterprise.sharepoint.com/sites/PRportal	9/22/2016 4:55:47 PM
J.Carter@enterprise.onmicrosoft.com	Role Group	■ Modified	Organization Management	BL2PR19MB0835	9/21/2016 3:15:51 PM
Members: - Added: "T.Simpson@enterprise.onmicrosoft.com"					
A.Anderson@enterprise.onmicrosoft.com	Group	■ Removed	Guests	https://enterprise.sharepoint.com/sites/PRportal	9/21/2016 1:51:42 PM

3.2 Meet auditors' expectations

Netwrix Auditor offers preconfigured compliance reports designed to effectively tackle many specific compliance requirements that healthcare organizations are subject to. For instance, the HIPAA compliance report pack includes multiple security reports that help you demonstrate the adequacy of your internal controls in the IT domain to secure patients' medical records and other PII.

Reports ALL REPORTS COMPLIANCE

Search

- ▶ FERPA Compliance
- ▶ FISMA/NIST Compliance
- ▶ GDPR Compliance
- ▶ GLBA Compliance
- ▲ HIPAA Compliance
 - ▶ User Account Locks and Unlocks
 - ▶ **User Accounts - Last Logon Time**
- ▶ ISO/IEC 27001 Compliance
- ▶ NERC CIP Compliance
- ▶ PCI DSS Compliance
- ▶ SOX Compliance

Demonstrate to auditors that your Information Security team members and other appropriate staff stay updated with security intelligence on a regular basis through subscriptions to scheduled reports and email alerts.

Subscribe to the 'User Account Status Changes' report

Subscription name: 'User Account Status Changes' report

Delivery format: PDF

Send empty reports: No

Deliver report to: 2 recipient(s) every day [Attach report to email](#)

Filters

Managed Object: enterprise.com ▼

Who (Domain\User): %

What: \com\enterprise\Users\John Smith

Domain Controller: %

Workstation: %

Actions: Unlocked, Locked, Enable, Disable ▼

Sort By: When ▼

3.3 Minimize the complexity and stress of getting started with compliance

If your healthcare organization is just at stage one of building a security program to address the complex regulatory requirements you face, Netwrix Auditor can help you make it more solid. The product provides out-of-the-box compliance reports that help you ensure you implement the necessary controls, and Netwrix provides easy-to-understand information about best practices for meeting specific requirements.

Mapping of Processes and Report Categories to HIPAA Controls

§ 164.308 Administrative safeguards. (HIPAA Security Rule)

Control	How to Comply?	Processes and Report Categories
§ 164.308 (a)(1)(i) Security management process	In accordance with implemented policies, review activities in information systems to detect and investigate security violations.	AUDIT TRAIL All Changes CONFIGURATION MANAGEMENT Policy States Configuration States
§ 164.308 (a)(1)(ii)(A) Risk analysis	Utilize audit trail recorded by Netwrix Auditor, while performing assessment of risks to confidentiality, integrity, and availability of PHI.	ACCESS CONTROL All Changes INTEGRITY MONITORING System Integrity Data Integrity
§ 164.308 (a)(1)(ii)(B) Risk management	Validate that the implemented security measures are sufficient and appropriate relying on organization defined procedures and audit trail produced by Netwrix Auditor.	DATA GOVERNANCE Data Integrity User Activity CONFIGURATION MANAGEMENT Configuration Changes Configuration States
§ 164.308 (a)(1)(ii)(C) Sanction policy	To support this requirement please refer to the user activities trail for violations of security policies.	ACCESS CONTROL User Activity ACCOUNT MANAGEMENT Account States
§ 164.308 (a)(1)(ii)(D) Information system activity review	Utilize built-in capabilities for alerts and on-demand reports to regularly audit activities in organization-defined information systems.	AUDIT TRAIL All Changes User Activity

Conclusion

Ensuring the security of your healthcare organization's and your patients' data has never been more important — or more challenging. You face increasingly frequent and sophisticated cyber threats, and you regularly have to demonstrate your ongoing compliance with a wide range of complex regulations. It's time to invest in the right tools to ensure you can do the job right, and with far less effort.

Major healthcare organizations around the world already rely on Netwrix Auditor to minimize risks to their sensitive information and help them successfully pass regulatory audits. With Netwrix Auditor, you can easily collect and consolidate audit data from all the critical systems across your IT organization, both on-premises and in the cloud. You don't have to pore through multiple logs and try to piece together disparate and incomplete data: Netwrix Auditor provides actionable information in easy-to-understand dashboards and comprehensive reports, so you can easily detect both vulnerabilities in your environment and threats in progress, and respond quickly and effectively. It simplifies investigations with powerful capabilities of the Interactive Search. Moreover, Netwrix Auditor slashes the time and effort required to prepare for regulatory compliance audits and helps you pass them with flying colors.

We invite you to learn more — including how you can get Netwrix Auditor up and running in your environment in just 15 minutes — at www.netwrix.com




About Netwrix

Netwrix Corporation was first to introduce visibility and governance platform for on-premises, hybrid and cloud IT environments. More than 160,000 IT departments worldwide rely on Netwrix to detect insider threats on premises and in the cloud, pass compliance audits with less expense and increase productivity of IT security and operations teams. Founded in 2006, Netwrix has earned more than 100 industry awards and been named to both the Inc. 5000 and Deloitte Technology Fast 500 lists of the fastest growing companies in the U.S.

Netwrix Auditor is a visibility and governance platform that enables control over changes, configurations and access in hybrid cloud IT environments to protect data regardless of its location. The platform provides security analytics to detect anomalies in user behavior and investigate threat patterns before a data breach occurs.

Netwrix Auditor includes applications for Active Directory, Azure AD, Exchange, Office 365, Windows file servers, EMC storage devices, NetApp filer appliances, SharePoint, Oracle Database, SQL Server, VMware and Windows Server. Empowered with a RESTful API and user activity video recording, the platform delivers visibility and control across all of your on-premises or cloud-based IT systems in a unified way.

For more information, visit www.netwrix.com

 On-Premises Deployment Download a free 20-day trial netwrix.com/go/freetrial	 Virtual Appliance Download our virtual machine image netwrix.com/go/appliance	 Cloud Deployment Deploy NetwrixAuditor in the Cloud netwrix.com/go/cloud
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Corporate Headquarters:

300 Spectrum Center Drive, Suite 1100, Irvine, CA 92618

Phone: 1-949-407-5125 **Toll-free:** 888-638-9749 **EMEA:** +44 (0) 203-588-3023



netwrix.com/social