

AXONIUS CYBERSECURITY ASSET MANAGEMENT

HIPAA Compliance Review



TABLE OF CONTENTS

Disclaimer (Tevora).....	3
EXECUTIVE SUMMARY	4
Overview	4
CURRENT ASSET MANAGEMENT Practices.....	5
Potential Challenges	5
Outdated forms of Asset Management	5
Cloud Asset Management	6
Lack of Process Controls and Policies	6
Redundant Asset Collection	6
Lack of Established Scopes.....	7
HIPAA Compliance Challenges	7
Large Scale Organizations	7
Gaps in ePHI Scope	7
BEYOND ASSET MANAGEMENT	9
AXONIUS FOR HIPAA COMPLIANCE	10
Overview	10
Key Features	10
Asset Management	10
Visibility.....	11
Access Management	12
Compliance Management.....	12
Incident Management	12
Policy Management.....	13
Third Party Integrations	13
Reporting and Analytics	14
COMPLIANCE REQUIREMENTS	15

TECHNICAL ANALYSIS METHODOLOGY..... 19

CONCLUSION 20

APPENDIX..... 21

ABOUT AXONIUS 22

ABOUT TEVORA 23

DISCLAIMER (TEVORA)

The opinions stated in this guide concerning the applicability of Axonius® products to the HIPAA Security Rule are the opinions of Tevora. All readers are advised to perform individual product evaluations based on organizational needs.

EXECUTIVE SUMMARY

OVERVIEW

Axonius engaged Tevora, a security and risk management consulting firm, and an accredited PCI Qualified Security Assessor (QSA) and HITRUST Assessor, to conduct an independent, in-depth evaluation of Axonius against the applicable Health Insurance Portability and Accountability Act (HIPAA) Security Rule Requirements.

This paper describes the observations and conclusions drawn by Tevora through their partnered review of Axonius. This review included an assessment of key features via an initial demonstration of Axonius, and several testing sessions with Axonius to validate capabilities.

Furthermore, this whitepaper outlines the specific ways the Axonius Cybersecurity Asset Management platform can help organizations fulfill the mandates of HIPAA.

CURRENT ASSET MANAGEMENT PRACTICES

Information technology asset management (ITAM) is one of the most critical components of IT organization, but ITAM programs often don't incorporate the data security teams need to secure assets. Cybersecurity asset management (or modern asset management) allows IT and security teams to gather rich data about all assets and understand whether assets meet security policies and frameworks.

From an operational perspective, it is crucial to ensure IT assets are effectively managed, controlled, and protected. In addition, it is important to resolve any risk associated with the deployment and use of these assets. An increase in work from home environments has introduced new challenges to IT and security management, where the visibility of assets has declined significantly due to connections with unmanaged and personal networks. It is difficult to enforce the proper use of assets when organizations lack standardized policies and have inadequate visibility to asset environments.

POTENTIAL CHALLENGES

Outdated forms of Asset Management

It is vital for asset management to be strategized in order to benefit businesses. Previous asset management practices have proven to be inefficient and wasteful. One of the most common methods includes manually tracking assets in a spreadsheet or similar document. This poses multiple challenges. For instance, it is very difficult to track all installed software on every device, as well as trace every valid or expired software license. Tracking with a spreadsheet does not allow administrators to record any real-time changes or data. Another

challenge of manual tracking is an increased chance for errors. When evaluating the accuracy of a tracking document, human error must be accounted for, bringing the integrity of the data into question. In addition, manually tracking assets is time consuming and interrupts important tasks.

Cloud Asset Management

As cloud computing has rapidly increased, it is crucial that all applications, platforms, and infrastructure are managed correctly. When relying on a cloud-based application, IT managers and administrators tend to lean on the services of the provider, at times neglecting any responsibility for the asset. Leaving a gap between what IT administrators think they know, versus the actual current state of assets.

Lack of Process Controls and Policies

Many users in an enterprise may view IT asset management as an optional function rather than an organizational discipline. Therefore, it is critical that administrators create process controls and enforce valid policies. Asset policies are typically at the enterprise level and do not reflect the current state of IT assets. Enforcing policies can become a difficult task for administrators with minimal visibility to assets. Additionally, it is common for administrators and regular users to be unaware that there are proper controls and policies in place. As a consequence, many of these policies are ignored or bypassed.

Redundant Asset Collection

It is common for department managers, users, and IT management to hold onto assets that are no longer needed or used. This includes software applications, laptops, desktops, and mobile devices. This can lead to continued purchasing of IT

assets, while current unutilized assets go unseen. Assets that are not used also introduce increased security and audit risks.

A lack of proper asset acquisition processes can lead to the purchase of unnecessary assets. Even if processes are in place, being unaware of these asset acquisition processes can promote uninformed purchases and introduce uncontrolled assets to the environment, which also increases security and compliance risks, and amplifies costs.

Lack of Established Scopes

There are times when organizations do not have predefined scopes defining what constitutes an IT asset. Users then purchase assets or install software that has not been approved, presenting more security and compliance risks. The lack of predefined scopes dismisses any type of enforcement or regulations for users to follow.

HIPAA COMPLIANCE CHALLENGES

Large Scale Organizations

Many enterprises attempting to comply with HIPAA Security Rule requirements have a large number of assets. The larger the scope of assets, the more challenging it becomes for administrators to view and manage every asset properly. Tools should be in place to facilitate mitigating any type of disruption or, at the very least, help identify potential assets at risk.

Gaps in ePHI Scope

Often times, healthcare providers do not know where all electronic protected health information (ePHI) is located, creating gaps in compliance with risk analysis requirements listed under HIPAA. The lack of an asset inventory tool can potentially disrupt the development

of a comprehensive, enterprise-wide risk analysis strategy. Overlooked assets in an environment can greatly disrupt the overall security of an enterprise. Without full visibility into every asset, administrators can be left unaware of rogue assets or of users misusing assets.

BEYOND ASSET MANAGEMENT

The Axonius platform was built to go beyond taking inventory of assets. Axonius can discover and evaluate how each of asset is operating, verify settings and configurations, and enforce specific policies. The following are some of the features that demonstrates how Axonius is more than an IT asset management tool.

- 1. Agentless Tool - Axonius connects via API to the management consoles already in use by organizations to collect assets.*
- 2. Data Collection – Axonius is designed to discover, aggregate, normalize, and deduplicate all data about devices, users, and cloud instances by connecting to multiple tools that have detected an asset.*
- 3. Access Control – Axonius was built to identify both on-prem and cloud-based devices.*
- 4. Configuration Management – Axonius integrates with over 300 solutions, including Configuration Management Database tools to ingest and push changes to configurations.*
- 5. Risk Controls - Axonius queries help administrators identify risks and implement risk controls.*
- 6. Compliance Frameworks – Axonius can be used to automate compliance checks and compile in-scope environments.*

AXONIUS FOR HIPAA COMPLIANCE

OVERVIEW

Axonius allows organizations to manage and track assets connected to their networks. This product currently offers integrations with more than 300 of the most powerful business management and security tools to accurately collect data on all assets, users, vulnerabilities, and more. Once this data is aggregated, Axonius provides an asset inventory, uncovers security gaps, and validates security policies. It allows administrators to have a centralized management location for full visibility and control of assets and their data.

Axonius offers a variety of deployments like on-premise and private cloud deployments. In addition, Axonius-as-a-Service (a SaaS deployment) is also available. During an on-premise deployment, Axonius is deployed on a virtual appliance that becomes part of the organization's internal network. If an organization prefers Axonius-as-a-Service, the solution is deployed on an AWS EC2 instance.

KEY FEATURES

Asset Management

The main component of the Axonius Cybersecurity Asset Management tool is to maintain an updated asset inventory, while validating asset security and configurations. This platform actively discovers assets as they appear in other data sources integrated with Axonius. It automatically updates the inventory from connected data sources at customer-defined time intervals..

Axonius offers to the capability to identify unmanaged devices that are known only through network connections. This is done

by identifying any device that has gone rogue with specific queries. A rogue device includes any asset with unwanted software or any non-restricted device connected to restricted network segments. Axonius can discover and manage any cloud asset, as it integrates with all major cloud providers. Axonius integrates with other network tools, including firewalls, routers, and switches, enabling administrators to easily find any IoT device – managed or unmanaged - connected to the network.

As cloud computing continues to grow, Axonius wants to ensure full security on all assets hosted by any cloud instance. This is accomplished by mapping the state of currently connected cloud instances against industry standards and benchmarks. The platform reports on how assets adhere to or deviate from common security best practices for Amazon Web Services, Microsoft Azure, Google Cloud Platform, and Oracle Cloud.

Visibility

Axonius Cybersecurity Asset Management connects with key security and management solutions used by the organization to discover any asset on the network. It then collects and correlates information about devices, cloud instances, and users. This allows administrators to have full visibility of all assets as they report back to Axonius through multiple connections. In addition, administrators can discover any security gap and enforce security policies. The Axonius Dashboard is a customizable page for organizations to track any relevant metrics and show any insights based on saved queries. It offers full visibility to critical events in the current environment.

Access Management

Access management focuses on validating that secure exchange of credential operations are conducted, as well as ensuring authorization and provisioning functions are secure. Policies based around access are also contained within access management functions.

Axonius has the ability to automate queries that benefit access management. This platform enables administrator and privileged access to be validated by creating queries with specific tool connections. There is also a big focus on finding unauthorized wireless access, queries to search for unknown, unmanaged, and rogue devices on network interfaces across connected network infrastructure.

Compliance Management

Axonius is designed to integrate into the dynamic, agile, and scaling cloud architectures deployed by organizations at the forefront of modern technology. Primarily focused on cloud asset compliance, Axonius is set to comply with specific industry benchmarks and frameworks. Some of those compliances include CIS Amazon Web Services Foundations, CIS Microsoft Azure Foundations, CIS Oracle Cloud Infrastructure Foundations, and CIS Google Cloud Platform Foundations benchmark.

Incident Management

Axonius can help accelerate incident response investigations by providing clear asset inventories. This is accomplished by connecting adapters to critical sources that will provide detailed information on devices, users, and cloud assets. Administrators can then correlate any incident alert to data Axonius has provided.

By providing a full asset inventory, Axonius will indicate which devices and users were associated with the alerts, where the devices were located, all software running on those devices, and which users are associated with the device. In addition, Axonius data can be sent to different security information and event management (SIEM) and security orchestration, automation, and response (SOAR) systems to provide rich asset data that can contextualize log data.

Policy Management

Security policies can be validated by Axonius on a continuous basis using queries that look for specific conditions. Using any query or select assets, actions can be designed to alert or create incident response tickets during an event. Axonius can be integrated with Slack, ServiceNow, Zendesk and other ticketing systems to notify users and create tickets. Other actions include enriching device and user data with third party sources, updating vulnerability assessments, creating, and updating CMDB records, or isolating devices from the network.

Third Party Integrations

In addition, Axonius can integrate with more than 300 pre-built solutions. For a list of available solutions, please visit [Adapters List](#). These tools include IT, Security, and business solutions that can securely send Axonius asset data. This is accomplished by configuring supported adapters with the necessary credentials to fetch asset data. For more information on how to configure an adapter, go to [Adapters Page](#).

Reporting and Analytics

Axonius can also generate reports based on the information being displayed on the Dashboard. Dashboard spaces can be customized to show specific spaces, saved queries, users, or a combination of all. Additionally, administrators may configure email notifications when reports are generated. The report PDF file contains a cover page, contents, discovery summary, dashboard charts, and saved queries for both devices and users.

COMPLIANCE REQUIREMENTS

Here is how Axonius addresses each applicable HIPAA Security Rule requirement:

HIPAA SECURITY RULE REQUIREMENT	AXONIUS FEATURES	SUPPORTS COMPLIANCE
---------------------------------	------------------	---------------------

Security Management Process: Risk Management		
--	--	--

164.308(a)(1)(ii)(B) – Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level	Axonius allows administrators to create queries based on the configurations that need to be validated. This includes any configuration on a network device like a router or firewall. The following is an example of a query that can be used to validate firewall rules: <i>Show ALL Axonius assets with INGRESS traffic in Firewall Rules AND targets all possible IPs (0.0.0.0) OR ALL Axonius assets with EGRESS traffic in Firewall Rules AND targets all possible IPs (0.0.0.0)</i> The query will depend on the client's environment and how networks are segmented.	Yes
---	---	-----

Security Awareness and Training: Security Reminders		
---	--	--

164.308(a)(5)(ii)(A) – Provide periodic security updates.

Axonius automated queries can check for updates at any given time and can be configured to run as often as desired or required. When creating a new query for software or security updates, administrators can specify the version of the update that needs to be verified. Queries can confirm that the most recent security update is currently running or installed on all assets.

Yes

Security Awareness and Training: Protection from Malicious Software

164.308(a)(5)(ii)(B) – Procedures for guarding against, detecting, and reporting malicious software.

Axonius queries can be configured to automatically run and verify detection tools are running. In addition, data can be logged by connecting Axonius to a SIEM. The following is an example of a query that can be used to ensure that anti-virus is actively running:

Yes

Show ALL assets that have a McAfee ID AND have reported back to Axonius in the last three days AND have NOT been seen in the last three days by McAfee

A similar query may be run continuously to ensure that data is being returned to the anti-virus software and to Axonius.

Security Awareness and Training: Password Management

164.308(a)(5)(ii)(D) – Procedures for creating, changing, and safeguarding passwords.

Axonius can integrate with Microsoft Active Directory (AD) to ensure that users are signing in through an identity solution. Additionally, Axonius can enforce specific password policies through Microsoft Active Directory (AD).

Partial

Evaluation

164.308(a)(8) - Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operations changes affecting the security of electronic protected health information, that establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart [the Security Rule].

Through Axonius queries, administrators can evaluate environmental and operational changes related to systems containing health information. The scope of these evaluations will vary depending on the organization's environment.

This can be accomplished by creating queries that continuously monitor and evaluate assets.

Once queries are saved, they will automatically validate any environmental change.

Yes

Access Control: Unique User Identification

164.312(a)(2)(i) - Assign a unique name and/or number for identifying and tracking user identity.

Axonius allows administrators to keep a detailed inventory of all assets and identities. In the main Dashboard page, administrators have full visibility of each asset with device details and current installed software.

Yes

Audit Controls

164.312(b) - Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.

Axonius queries can help validate configuration settings for systems carrying electronic protected health information. Creating groups of crucial environments needed to comply with HIPAA can be saved and evaluated together continuously. Additionally, Axonius can push a number of configuration settings to designated groups of assets. The following is an example of a query that can be used to verify which assets are missing anti-virus software:

Show ALL Axonius assets that do NOT contain Adapter Properties that equal Endpoint_Protection

Yes

TECHNICAL ANALYSIS METHODOLOGY

Tevora reviewed the Axonius solution to observe effectiveness for the following HIPAA compliance requirements:

- *Security Management Process:*
 - *164.308(a)(1)(ii)(B) – Risk Management*
 - *164.308(a)(5)(ii)(A) – Security Reminders*
 - *164.308(a)(5)(ii)(B) – Protection from Malicious Software*
 - *164.308(a)(5)(ii)(D) – Password Management*
- *Evaluation*
 - *164.308(a)(8)*
- *Access Control*
 - *164.312(a)(2)(i) – Unique User Identification*
- *Audit Controls*
 - *164.312(b)*

CONCLUSION

Axonius Cybersecurity Asset Management Platform provides the necessary tools to enable and successfully comply with multiple HIPAA Security Rule requirements. As an asset management solution, it provides full visibility into complex environments and their assets. Additionally, it provides a wide variety of query options to discover security gaps and subsequently enforce security policies by pushing action configurations into specified assets.

With over 300 available integrations, Axonius should ideally be integrated with any data source that knows about assets, if possible. This will provide the most accurate data results for all assets. Axonius provides a full view into assets and helps control asset, compliance, incident, policy, and access management.

The Axonius Cybersecurity Asset Management Platform will enable enterprises to effectively fulfill some of the most important HIPAA Security Rule requirements.

APPENDIX

Definitions – compliance standards

HIPAA Security Rule

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 requires that Covered Entities must take strong measures to protect the privacy and security of health information. At the endpoint, this translates to ensuring the host is protected from malware. Specifically, the HIPAA Security Rule requires Covered Entities and Business Associates to comply with general security requirements. More specifically, the Administrative Safeguards in §164.308(a)(1), §164.308(a)(5)(ii)(B) and §164.308(a)(6)(ii), require Covered Entities and Business Associates to implement and maintain procedures to protect, detect, contain, respond, correct, and report on malicious software throughout the environment.

ABOUT AXONIUS

Axonius was founded in June 2017 to answer a simple question. Despite all of the high-tech, sci-fi tools we have in cybersecurity, why is it so difficult to answer simple questions about the devices, users, and cloud instances we're tasked with securing? Asset management is so foundational, yet it's a nagging problem that is only getting worse. Co-Founders Dean Sysman, Ofri Shur, and Avidor Bartov, veterans of an elite intelligence unit of the Israeli Defense Force built Axonius to solve the asset management challenge for cybersecurity. Axonius is headquartered in New York, NY and our R&D team is based in Tel Aviv, Israel.

It's 2021, and security teams are still spending time and manual effort trying to understand the assets they have, whether those assets are secure, and whether they adhere to or deviate from their security policies. Our mission is to give customers a comprehensive and always up-to-date asset inventory, uncover security gaps, and automate as much of the manual remediation work as our customers want. When organizations stop spending time on manual asset management tasks, they're able to take on the high-value cybersecurity initiatives that highly trained and skilled cybersecurity professionals love doing.

ABOUT TEVORA

Tevora is a leading management consulting firm specializing in enterprise risk, compliance, information security solutions, and threat research. We offer a comprehensive portfolio of information security solutions and services to clients in virtually all industries and also serve institutional and government clients.

Tevora's leaders are professionals with years of experience and records of accomplishments in technology as well as business. This dual background means that we understand the importance of growth and profitability and our solutions are designed to enhance both.

As a consulting firm that has the ability to fully implement whatever it recommends, Tevora works with all of the industry's top vendors, yet is beholden to none. We are completely vendor-independent and select best-of-breed products tailored exclusively to our clients' needs. Security is our only business and our single-minded focus on anticipating and solving client problems has been described as "obsessive." We consider this a fair assessment.

Our hard work and dedication has established us as a reliable partner CTOs CIOs, and CISOs can depend on to help protect against threats, both internal and external. With Tevora as a partner, business leaders can devote their energies to enhancing the overall value of information technology to their enterprise.

Tevora is a Qualified Security Assessor (QSA) and Payment Application Qualified Security Assessor (PA-QSA) in good standing with the PCI Security Standards Council. Tevora is also a DVBE (Disabled Veteran Business Enterprise) certified by the California General Services Department (Cert REF# 32786).

For more information please visit www.tevora.com.