HIPAA: Q-Compliance

REAL-TIME RISK MANAGEMENT & CON-MON COMPLIANCE FOR THE HEALTH CARE INDUSTRY

HIPAA compliance is often implemented 1 of 3 ways:

1) **Self-Assessments**
   Self-attestation requires copious amounts of supporting documentation, policies and procedures, and full-time resources dedicated to monitoring and reporting. We often see organizations jury-rig a system of datasheets and reports together to make compliance a checkbox exercise. This approach provides little if any long-term operational security value and proves grossly expensive Thus, other options must be exercised.

2) **Third Party Audits**
   If the first option sounds like an overhaul or inefficient use of internal resources, hiring a third party to manage your compliance posture may prove useful. While this may provide a robust approach to managing HIPAA compliance, it must be an ongoing contract to truly provide operational security benefits. And as one can imagine, the cost of having a third party on retainer can add up very quickly.

3) **GRC Tools or Relational Databases**
   If self-assessments are too risky or time consuming, and outsourcing is too expensive, buying software to store the appropriate data may be a great option. However, GRC tools do not report and monitor in real-time and therefore do not offer improved operational security. These products are also expensive, and often require maintenance or add-ons to improve the products.

The Health Insurance Portability and Accountability Act (HIPAA) went into effect as part of the Social Security Act of 1996 in order to protect health care coverage for individuals who have lost or changed their jobs, and to ensure security of electronic transfers of electronic protected health information (ePHI). Hospitals, private practices, dental offices, clinics, pharmacies, health plans, healthcare clearinghouses, and any other covered entity or person handling ePHI have all had to work earnestly to achieve and maintain compliance with the extensive set of strict requirements associated with HIPAA. In a time of increasingly costly and frequent data breaches, it is more important than ever to provide assurances when it comes to protecting vendor data and patient ePHI.

The 5 Main HIPAA Rules to Understand

1. Privacy Rule
The privacy rule protects the ePHI and medical records of individuals by setting limits and conditions on the various uses and disclosures that can and cannot be made without patient authorization.

2. Security Rule
The security rule defines and regulates the standards, methods, and procedures related to the protection of ePHI with regard to storage, accessibility, and transmission. The 3 safeguard levels of security are broken into administrative, technical, and physical.

3. Transaction Rule
HIPAA does not require physicians to conduct transactions electronically, but if a physician practice does conduct any the transactions named under HIPAA, the organization must submit the transactions according to the HIPAA standards. The transaction codes ensure safety, accuracy, and security of medical records or ePHI.

4. Identifiers Rule
HIPAA uses three unique identifiers for covered entities conducting HIPAA-regulated administrative and financial transactions. These identifiers are the National Provider Identifier (NPI), National Health Plan Identifier (NHI), and the Standard Unique Employer Identifier Number (EIN).

5. Enforcement Rule
The Enforcement Rule expands the rules and establishes criminal and civil penalties for any violations of privacy and security required by HIPAA. Covered entities and their business associates must enforce rules for the application of security and privacy requirements, accounting disclosure requirements, sales and marketing restrictions, accounting disclosure requirements, and the enforcement of all security requirements across business associates' contracts as well.

These rules are a lot to digest. HIPAA compliance is important and required for any covered organization, but with all the hustle and bustle of a modern health care organization, meeting these requirements frequently becomes a check-box exercise, leaving your organization and patient data vulnerable to breaches. Not only will this result in fines and legal consequences, but also lasting reputational damage if and when a vulnerability is exposed. The bottom line: making HIPAA compliance a priority is essential. The twist: HIPAA compliance does not have to cost you an arm and a leg.

splunk> POWERED

Administrative Safeguards

- Security Management Process
- Security Personnel
- Information Access Management
- Workforce Training and Management
- Evaluation

Physical Safeguards

- Facility Access and Control
- Workstation and Device Security

Technical Safeguards

- Access Controls
- Audit Controls
- Integrity Controls
- Transmission Security

Policies, Procedures, & Documentation Requirements

- Covered Entity Responsibilities
- Business Associate Contracts
- Risk Assessments

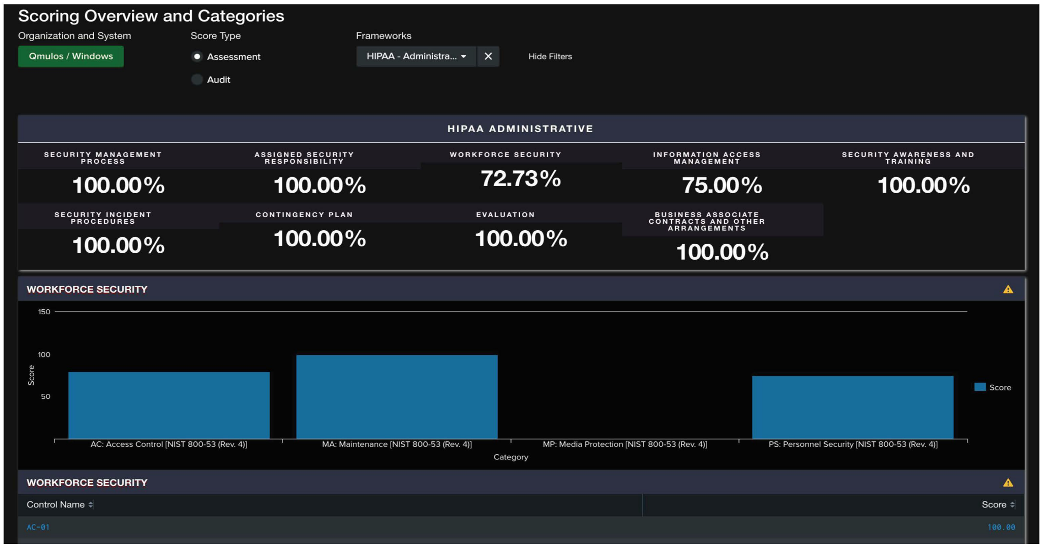
> **"Synonymous with quality health care, privacy of your clients and their protected health information should be your main concern."**

At Qmulos we Pride ourselves on that promise.

As a native Splunk powered solution, Q-Compliance solves this problem by applying a compliance lens to near real-time data being ingested across your enterprise and assessing it against the HIPAA security controls. Q-Compliance contextualizes the log data ingested through Splunk into a HIPAA compliance lens, making compliance easy for anyone to prove. No longer does a team need to manually collect technical evidence from various data sources, spend fortunes on audits, or spend hours sifting through static spreadsheets.

Q-Compliance is purpose-built to help you streamline and automate complex cybersecurity auditing and compliance requirements like HIPAA, NIST 800-53, SOX, PCI DSS, and many others. By selecting one of Qmulos' HIPAA dashboards (Administrative, Physical, Technical, or Policies and Procedures and Documentation Requirements) the user can track how an organization and its systems are scoring against each of the control categories, and where it needs to improve. The dashboards provide an ability to quickly drill into specific domains to view compliance against the capabilities, practices and processes set forth, and also drill into individual controls to see the specific systems, events, and assets that are non-compliant.

Q-Compliance gives the user the ability to upload policies, procedures and file evidence, as well as automatically log human activity. The software keeps evidence needed for audits all in one place, making things more organized and efficient. Q-Compliance also aligns specific security controls with the HIPAA policies and procedures to use real- time log and event data from Splunk to help you automate the assessment and scoring of your organization's practices against HIPAA. Qmulos codified industry best practices into the application workflows, enabling your organization to institutionalize and optimize the processes that improve your cyber posture and protect you and your client's ePHI.



Scoring Overview and Categories

Organization and System: Qmulos / Windows

Score Type: ● Assessment ○ Audit

Frameworks: HIPAA - Administra... ▾ ✕

Hide Filters

HIPAA ADMINISTRATIVE

SECURITY MANAGEMENT PROCESS	ASSIGNED SECURITY RESPONSIBILITY	WORKFORCE SECURITY	INFORMATION ACCESS MANAGEMENT	SECURITY AWARENESS AND TRAINING
100.00%	100.00%	72.73%	75.00%	100.00%
SECURITY INCIDENT PROCEDURES	**CONTINGENCY PLAN**	**EVALUATION**	**BUSINESS ASSOCIATE CONTRACTS AND OTHER ARRANGEMENTS**	
100.00%	100.00%	100.00%	100.00%	

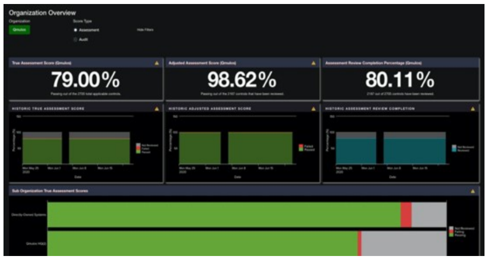
WORKFORCE SECURITY ⚠

150
100
50
Score
AC: Access Control [NIST 800-53 (Rev. 4)]
MA: Maintenance [NIST 800-53 (Rev. 4)]
MP: Media Protection [NIST 800-53 (Rev. 4)]
PS: Personnel Security [NIST 800-53 (Rev. 4)]
Category
Score

WORKFORCE SECURITY ⚠

Control Name	Score
AC-01	100.00

ExecutiveView



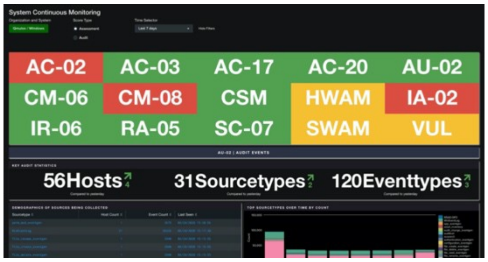
Organization Overview

True Assessment Score (Qmulos)	Adjusted Assessment Score (Qmulos)	Assessment Review Completion Percentage (Qmulos)
79.00%	98.62%	80.11%

HISTORIC TRUE ASSESSMENT SCORE
HISTORIC ADJUSTED ASSESSMENT SCORE
HISTORIC ASSESSMENT REVIEW COMPLETION
Sub Organization True Assessment Scores

- Compliance and risk postures
- Organization & system views
- View status across different compliance frameworks

Control Monitoring



System Continuous Monitoring

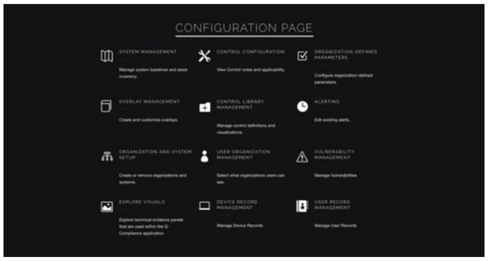
AC-02	AC-03	AC-17	AC-20	AU-02
CM-06	CM-08	CSM	HWAM	IA-02
IR-06	RA-05	SC-07	SWAM	VUL

AU-02 | AUDIT EVENTS

56Hosts 31Sourcetypes 120Eventtypes

- Realtime risk and compliance visibility
- Single pane of glass for all evidence and artifacts
- Workflows for time and event-based assessments

Native RMF Features



CONFIGURATION PAGE

- Support for all RMF steps
- Overlay management
- Organization, system, and asset management
- Control tailoring
- Assessment automation

qmulos

1560 Wilson Boulevard, Suite 900, Arlington, VA
22209 www.qmulos.com Copyright©2020 Qmulos