Araali Networks

HIPAA Compliance for Containers and VMs

Introduction

Modern cloud-native application architectures give developers the ability to test, iterate, and release applications and microservices at the speed of light. Also, companies are adopting hybrid and multi-cloud strategies to lower cost and keep vendors honest. This strategy helps companies build performance and resiliency as it allows for scaling and redundancy on one hand while mitigating cost and downtime risks on the other hand.

However, cloud-native and multi-cloud present its own set of challenges. The challenges, especially security and compliance, are more profound for companies in the regulated industry. Enterprises have to reevaluate and rethink their security processes and security solutions to remain compliant with regulatory controls.

What is HIPAA

HIPAA was enacted in 1996 and covered a wide range of topics. The privacy and security rules were added in 2003 and are set standards for protecting personal health information stored in digital format.

Definition provided by the US Department of Health and Human Services1

"*The HIPAA Privacy Rule establishes national standards to protect individuals' medical records and other personal health information and applies to health plans, healthcare clearinghouses, and those healthcare providers that conduct certain healthcare transactions electronically. The Rule requires appropriate safeguards to protect personal health information privacy and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The Rule also gives patients rights over their health information, including rights to examine and obtain a copy of their health records and request corrections*".

The HIPAA Privacy Rule regulates the use and disclosure of Protected Health Information (PHI) held by "covered entities", "Business Associates" and third-party service providers "Subcontractors" who may come into contact with patient healthcare data or payment information.

What are PHI and ePHI?

PHI, Protected Health Information is defined as “any information held by a covered entity that concerns health status, the provision of healthcare, or payment for healthcare that can be linked to an individual.” PHI consists of 18 different identifiers.

1. Names
2. All geographical data smaller than a state
3. Dates (other than year) directly related to an individual
4. Telephone numbers
5. Fax numbers
6. Email addresses
7. Social Security numbers
8. Medical record numbers
9. Health Insurance Plan Beneficiary number
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers including license plates
13. Device identifiers and serial numbers
14. Web URLs
15. Internet protocol (IP) addresses
16. Biometric identifiers (i.e., retinal scan, fingerprints, etc.)
17. Full face photos and comparable images
18. Any unique identifying number, characteristic or code

ePHI, ***electronic protected health information*** is defined as individually identifiable health information transmitted or stored electronically.

Based on the list above, if a company is providing a specific patient service on behalf of a hospital and sharing it back with the hospital, for example, reminding them of a prescription refill. If they ask for the patient's email id for login and email communication, then email id will fall under the ePHI category.

Who Has a Responsibility to Protect PHI?

There are three main categories of entity - "Covered Entities," "Business Associates," and "Subcontractors" that have the responsibility to comply with HIPAA.

Covered Entities - include Healthcare Providers, Health Plans, and Healthcare Clearing Houses closest to PHI data. These are organizations that maintain patient healthcare or payment information or come in contact with PHI in their daily duties like doctors and hospital staff.

Business Associates – are people or entities that are not employed by a covered entity, but perform or assist in achieving a function or activity regulated by HIPAA.

Contractors or subcontractors are independent employees or employees of a company likely to have access to PHI. They include labs and lab technicians, collection agencies, message and

confirmation services, IT and technical personnel, non-employed consultants, cleaning crews and staff providing unsupervised after-hours services

How Araali addresses HIPAA

Araali leverages the HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework published by NIST in February 2014 (link), as directed in executive order 13636 - Improving Critical Infrastructure Cybersecurity. The goal of this crosswalk was to provide a voluntary, risk-based approach—based on existing standards, guidelines, and practices.

Enterprises achieve HIPAA compliance by satisfying sub-categories specified in the NIST cybersecurity framework. An organization looking for HIPAA compliance should work with its auditors to fully understand and appreciate the subtle nuances around all control categories. The following table summarizes the specific sub-categories of controls that Araali can help achieve through its security solution. HIPAA Security Toolkit (link)

NIST - Function/ Category/ Subcategory	Description	HIPAA Security Rule	Araali
Identify /Asset Management /ID.AM-2	Software platforms and applications within the organization are inventoried	164.308(a)(1)(ii)(A), 164.308(a)(7)(ii)(E)	Inventory of containers and VMs. View of environments, applications, and services within containers and VMs.
Identify /Asset Management /ID.AM-3	View a visual representation of the network topology and associated connections of a service.	164.308(a)(1)(ii)(A), 164.308(a)(3)(ii)(A), 164.308(a)(8), 164.310(d)	Networks topology at the environment, application, containers/VM and process level including associated east-west connections
Protect /Access Control /PR.AC-5	Network integrity is protected, incorporating network segregation where appropriate.	164.312(a)(1), 164.312(b), 164.312(e)	Araali enables automated Container-level and VM-level network segmentation, preventing unauthorized network connections.
Protect /Data Security /PR.DS-2	Data in transit is protected.	164.312(e)(1)	Araali can encrypt communication between microservices running in containers or VMs.
Protect /Data Security /PR.DS-5	Protections against data leaks are implemented.	164.308(a)(1)(ii)(D), 164.310(b), 164.312(a)(1), 164.312(e)(1)	Araali whitelists application communications. Araali also monitors egress traffic and can apply rules to permit or drop the communication based on policies

Protect /Data Security /PR.DS-6	Integrity checking mechanisms are used to verify software, firmware, and information integrity.	164.312(b), 164.312(c)(1) 164.312(c)(2) 164.312(e)(2)(i)	Araali only allows binaries with known cryptographic identities to communicate. The app is fingerprinted during fortification and checked for deviations during runtime.
Protect /Data Security /PR.DS-7	The development and testing environment(s) are separate from the production environment.	164.308(a)(4) 164.502	Araali uses zone/environment setting to ensure integrity is maintained
Protect /Info Protection /PR.IP-1	A baseline configuration of information technology/industrial control systems is created and maintained.	164.308(a)(7)(i), 164.308(a)(7)(ii)(A), 164.308(a)(8)	Araali, out of the box, creates a policy baseline for your apps that can be enforced. It also comes with pre-canned policies for certain apps that could be implemented and enforced from day 1.
Protect /Info Protection /PR.IP-2	A System Development Life Cycle to manage systems is implemented.	164.308(a)(1)(i)	Araali fingerprints application binaries during CI and keeps track of it only to permit known binaries to run in production. Any tampering is automatically detected and not allowed to run.
Protect/Info Protection/PR.IP-4	Backups of information are conducted, maintained, and tested periodically.	164.308(a)(7)(ii)(A) 164.308(a)(7)(ii)(B)	Araali backs up all the policy, configuration, and other relevant information periodically. Customers can save and restore policies at will and share it with other teams
Protect/Info Protection/PR.IP-8	Effectiveness of protection technologies is shared with appropriate parties	164.308(a)(6)(ii)	Araali has integrations with Slack and SIEM to forward alerts to right teams
Protect/Protective Technology/PR.PT-1	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(C), 164.310(a)(2)(iv), 164.310(d)(2)(iii), 164.312(b)	Araali collects detailed process level logs for app communications. These are analyzed for policy creations, alerts, and zero-day vulnerability detection and are also shared with SIEM.
Protect/Protective Technology/PR.PT-3	Access to systems and assets is controlled, incorporating the principle of least functionality	164.312(a)(1), 164.312(a)(2)(iv)	Araali is based on a whitelisting model where an application can only talk to each other based on least-privileged policies.
Protect/Protective Technology/PR.PT-4	Communications and control networks are protected	164.312(a)(1) - access control, 164.312(b) - audit control,	Araali assigns an identity to each process and uses a whitelisted policy to control app communications. Inter-app

		164.312(e) - transmission sec, encrypt,	communication can be encrypted.
Detect/Anomalies and Events/DE.AE-1	A baseline of network operations and expected data flows for users and systems is established and managed	164.312(b)	Araali creates policies based on a baseline of Network activities. Any deviations are flagged as Alerts, and communication is dropped.
Detect/Anomalies and Events/DE.AE-3	Event data are aggregated and correlated from multiple sources and sensors.	164.308(a)(5)(ii)(B), 164.308(a)(8), 164.312(b),	Araali collects very detailed process-level information across the environments, VMs, and containers. Integration with SIEM for further analysis (SIEM integration being built)
Detect/Anomalies and Events/DE.AE-5	Incident alert thresholds are established	164.308(a)(6)(i)	Araali shows all alerts based on policy violations. Alerts are currently categorized based on the frequency of occurrence.
Detect/Security Continuous Monitoring/DE.CM-1	The network is monitored to detect potential cybersecurity events.	164.312(b)	Araali monitors and enforces egress and ingress traffic. It creates alerts when anomalies are detected and intelligently routes it to the right app team.
Detect/Security Continuous Monitoring/DE.CM-4	Malicious code is detected.	164.308(a)(5)(ii)(B)	Araali fingerprints apps during the fortification process or CI stage. This prevents any unknown or modified workload from running and communicating
Detect/Security Continuous Monitoring/DE.CM-6	External service provider activity is monitored to detect potential cybersecurity events	164.308(a)(1)(ii)(D)	Araali logs all network connections made by external service providers into the applications. It will prevent flows which were not whitelisted and raise an alert - thus detecting and stopping potential threats
Detect/Detection Processes/DE.DP-4	Event detection information is communicated to appropriate parties	164.308(a)(6)(ii), 164.314(a)(2)(i)(C), 164.314(a)(2)(iii)	Araali has integrations with Slack and SIEM to forward alerts to right teams.

About Araali

For CISOs and App teams, who care about security and compliance without loss in productivity, Araali Networks in a distributed firewall leveraging application identity and context. It covers any workload - BM, VM, container and serverless, and any app - customer or open-source without re-compile. Unlike traditional firewall and contemporary container security companies, Araali protects any workload and leverages its Infrastructure-Agnostic and Location-Transparent policies, which are not IP but app-id based. This makes cloud adoption simpler while lowering TCO and improving security posture.

Works Cited

1. HHS Office of the Secretary, Office for Civil Rights, and Ocr. “Privacy.” *HHS.gov*, US Department of Health and Human Services, 16 Apr. 2015, www.hhs.gov/hipaa/for-professionals/privacy/index.html.