Technical White Paper

HIPAA Compliant Containers

Improving Secure Healthcare Information Workflow

ClearDATA
SECURE • HEALTHCARE • CLOUD

amazon web services | Partner Network
ADVANCED CONSULTING PARTNER
HEALTHCARE COMPETENCY
AUTHORIZED PUBLIC SECTOR PARTNER

HIPAA Compliant Containers

Improving Secure Healthcare Information Workflow

Table of Contents

Executive Summary

The HIPAA Privacy and Security Rules state that entities who create, receive, manage, store or process protected health information (PHI) must ensure the PHI is secure throughout the data lifecycle. Failing to protect PHI at any point from creation through use, distribution, maintenance, storage and destruction leaves an entity vulnerable to security incidents and subject to enforcement actions, including hefty fines, as determined by the Office for Civil Rights. Historically, protecting PHI was more straightforward as healthcare data resided within an organization. However, as the healthcare industry increasingly adopts the cloud, data and the associated compliance requirements are migrating beyond each entity's walls.

Though cloud adoption increases the scope of compliance activities, it also introduces technologies supporting rapid advancements in innovation. One such technology is containers. Containers allow deployment of single-purpose virtual compute instances for processing workloads in the cloud regardless of the operating system used. Care must be taken, however, to ensure that your container strategy, deployment methodology, monitoring protocols, and vulnerability management practices are harmonized in a manner that complies with the HIPAA Security Rule, as well as industry recognized security frameworks such as NIST, ISO, CSF and PCI DSS.

What are Containers?

Containers are single-purpose virtual compute instances that support workloads in the cloud. A container is similar to a virtual machine (VM) with a few important distinctions. Whereas virtual machines leverage hardware virtualization to carve a physical host into multiple VMs, containers virtualize the operating system,

allowing it to be carved into multiple lightweight slices called containers. These slices share the kernel and binaries of the host OS allowing an application to bring its own data and libraries.

What They Do Well

As mentioned, containers are extremely fast – they can be created and boot in mere seconds. One notable example of how quickly containers can launch can be seen when Alexa is asked for the latest weather. Once Alexa recognizes the request, containers from Amazon's Alexa Voice Service boot instantly in the cloud – in the correct order - to fulfill the request. The result may seem simple – "it's about to rain" – but the prediction is based on hundreds or thousands of data points in real time.

Containers are great at delivering specific applications quickly, efficiently and without introducing errors based on operating system inconsistencies when leveraging multiple systems. They can also be sequenced in an order that resembles a traditional application boot order, making application delivery appear as if it were done through traditional means, but occurring in a fraction of the time.

Containers solve the problem of how to get software to run reliably when moved from one computing environment to another and can allow the use of the same tools and workflows regardless of target operating system. At the same time, containers can move applications through networks in the same manner as traditional VMs AND can move an application wherever a copy of that OS is available.

This dramatically improves speed, reliability and, to the great benefit of healthcare, interoperability, as discussed below.

What They Don't Do Well

In spite of their strengths, containers have drawbacks in several areas. For instance, containers should not be used to store data. Because containers can easily be stopped, replaced or destroyed, storing data on containers can lead to data loss. Instead, containers

should be designed to write to a shared data store in a separate volume. In addition, if two containers write data on the same volume at the same time, the data can be corrupted.

Individual containers are also not meant to run multiple processes. Running more than one process on a single container becomes problematic when managing processes, retrieving logs, and updating the processes individually.

Because containers are ideally stateless, they require development teams to alter their mindsets and function differently than when developing legacy applications. This can be challenging for teams not yet trained on, and immersed in, container technology. Like development teams, many classic IT monitoring and management tools require updates to properly utilize and take advantage of containerized applications. Even with newer toolsets, IT professionals will require education and practice.

The fact that containers are easily deployed is a major benefit to using them. However, without proper DevOps processes and governance, the ease of deployment can result in unwanted, and undetected, container sprawl.

Like any other tool in the technology toolbox, containers have their strengths, but being mindful of their weaknesses and understanding the strategies to overcome those weaknesses, will aid in the architecture and deployment phases of implementation.

Problems Solved by Containers in the Healthcare Life Cycle

From the moment of injury or illness, a patient must encounter a complex series of information workflows. Part of the information journey begins when the caregiver retrieves the patient record to learn about the patient's conditions in an attempt to provide the most appropriate treatment. The care-giving process generates massive amounts of data that follows the patient throughout

the process. Data is not only generated by the EMR, but also by ancillary applications, including monitoring, care collaboration, patient management and consent, medication management, home monitoring, and telemedicine.

The infrastructure and software needed for information management throughout the healthcare lifecycle can be complex. Information can flow from an ambulance to an emergency room and possibly through other systems that may be located in on-premise data rooms, local Health Information Exchanges located in a collocation facility, and even in a public cloud environment.

There are many points of possible failure along that journey.

Breakdowns occur when software environments are not identical across multiple systems. Similar challenges happen at the network layers where topologies can vary, security policies differ and storage may be configured differently from system to system. Despite the numerous potential points of variability, the same software is expected to run smoothly, quickly and without error even with these differences.

Enter containers.

Envision the information journey from one system to the next in a manner devoid of the challenges associated with systems that may not always be identical, communicate the same, be secured consistently, or even speak the same language.

Containers enable information to flow in a way that is nearly instantaneous, secure and compliant, and transparent and effective, whether from a doctor's laptop to a production environment or perhaps from a physical machine in a data center to a virtual machine in a private or public cloud.

How Can Containers Help Improve Healthcare Delivery?

Interoperability encompasses the exchange of data between any number of systems, for any number of purposes. However, data exchange between systems is often hindered by a lack of common communication standards. In the end, this is but a technical barrier—and one that is slowly being overcome, albeit with different workarounds. ONC's 2014 survey of hospitals, for example, found that most do electronically report and exchange data of some sort, e.g., lab results and clinical care summaries, with outside providers and hospitals.

By containerizing the application platform and its dependencies, and by isolating data flows to microservices, differences in OS distributions and underlying infrastructure are abstracted away[1]. This allows for more efficient information flow. The remaining efforts can then be spent ensuring data standards are compatible, whether using FHIR (XML), HL7 (pick a flavor), or even JSON. Removing the barriers of how the application and data is delivered can yield significant benefits to the healthcare data lifecycle by putting the right data, in the right place, at the right time, ultimately resulting in improved patient experience and care.

Container Security Review

The "Out of the Box" Security Anatomy of a Container

While containers of the past may have been configured out of the box for convenience, that is no longer true. Today, Docker default settings incorporate most of the Center for Information Security (CIS) guidelines that indicate which defaults which should, and which should not, be changed.

Within Docker, containers rely on the kernel, as well as the Docker daemon, for a range of services accessed via system calls. Many

1 Rubens, Paul. "What are containers and why do you need them?" May 20, 2015. Accessed January 28, 2017. http://www.cio.com/article/2924995/enterprise-software/what-are-containers-and-why-do-you-need-them.html.

of these calls are essential for simple things like ordinary file and network tasks. Some system calls should be disabled, while others have no real impact on security. The key is to understand the difference.

In another example, the Docker daemon can be bound to the Unix Docker access group or the TCP port that allows containers to speak to each other. While reasonable for certain security processes, security and compliance stakeholders frown upon providing all users root access.[2]

Because containers share the physical server's memory, CPU and disk (requiring block-level I/O), as well as the host operating system, the security posture of a container can vary depending on how it is architected. Just as applications can be coded poorly, physical hosts can be neglected, the host operating system can remain unmaintained, and containers can be insecurely architected and deployed. This can result in containers loaded with malicious code, that could, for example, seek decryption keys or compromise a container designed to write data to a database.

Additionally, containers communicate through standard network channels outside the host. This requires security group configuration, sound identity and access management configuration, and the integration of appropriate monitoring and management processes and tools.

Hardening remains a challenge for those who may not understand defense in depth principles on public clouds and in particular, how those defenses should accommodate the nuances of container clusters.

ClearDATA Container Security

ClearDATA secures container deployment by managing PHI-capable container clusters in a HIPAA-compliant infrastructure. Based on the ClearDATA Dynamic PHI Platform – a fully responsive platform for Amazon Web Services (AWS) that allows PHI to be run in the cloud with ClearDATA's enhanced Business Associate Agreement coverage – security is applied by automating proven defense in depth principles.

2 Jerbi, Amir. "5 keys to conquering container security." August 4, 2016. Accessed January 2, 2017. http://www.infoworld.com/article/3104030/security/5-keys-to-docker-container-security.html.

Stateless Container Applications

Containers should never store important state information inside their local filesystem because:

1. If the container is recreated, any changes to its filesystem are lost. Relying on container storage for important data will lead to data loss.
2. Requests may be routed to any healthy container providing a given service. Imagine that a client makes a request and the container records some state data on its local filesystem. Subsequent requests from that client may be routed to other containers, which will not have the state data.
3. If an application has no local state, it can be easily scaled up by deploying more copies. Those new copies will be ready to serve requests without syncing any data. Similarly, scaling down is simple, as there is no local data to be saved.

In order to avoid storing local state, applications that you intend to run on a PHI Container Cluster should store all of their sensitive data in an external storage system such as S3, RDS, and DynamoDB.

In standard ClearDATA deployments, a PHI Container Cluster can access AWS services. Because of this, no special handling is required. A containerized application can use the standard SDKs and APIs to access AWS storage systems like those above. Of course, that requires AWS credentials to be configured. Since Identity and Access Management (IAM) users have static keys, ClearDATA strongly discourages their use in this setting.

Isolation

Container isolation can further the goal of securing sensitive information. Isolation is achieved primarily through control groups and namespaces. Control groups are a kernel feature that limits, accounts for, and isolates the resource usage (CPU, memory, disk I/O, network, etc.) of a collection of processes.[3] Namespaces, on the other hand, define what a container is authorized to access. Namespaces are complicated and if misconfigured, can

3 Cgroups. January 24, 2017. Accessed February 4, 2017. https://en.wikipedia.org/wiki/Cgroups.

have negative security consequences. Secure isolation between containers really comes from the same isolation tools used in non-containerized applications; file access permissions, mandatory access controls, scamp, etc.

ClearDATA configures control groups, namespaces, and infrastructure isolation consistently with HIPAA-compliant security policies. Automated configuration is critical, as containers can be easily misconfigured, or can be attacked via namespace manipulation.

Access Control

One of the most common tools in information security is limiting user access to only what is authorized for that particular user.

Access controls should be designed using principles of least privilege, which leads to the creation of role-based access permissions across hosts. ClearDATA enforces a centralized container access approach to ensure that each container has constraints on what changes or commands a user can execute based on their role. These constraints are designed to be appropriate and consistent with the user's or application's functional role. Separation of duties is one of the inherent strengths of containers from a security perspective.

Vulnerability Management

To stay ahead of vulnerabilities, and to keep containers up to date, ClearDATA scans both images and containers on a regular basis. ClearDATA also insists that vulnerability scanning be automated and included in its integration pipeline to ensure that secure images are created and maintained.

Patching

In tandem with vulnerability management is the need to patch. For containers, this is done a little differently than with a traditional IAAS/VM environment. In a traditional environment, security patches are installed independently of application code. Typically, a change window is coordinated, a server is patched, and if the patch

breaks an application, downtime can occur while the latest "fix" is rolled back.

Instead, containers are not patched, they are re-created and re-deployed from the base container image. Due to the degree to which containerized application dependencies are coupled with the application itself, there exists the potential to patch the system more frequently and potentially, less painfully.

For example, in the case of a vulnerability like Heartbleed, to ensure that the new version of SSL is deployed on every container, the base image must be updated and the container recreated in line with your typical deployment procedures. A deployment automation process makes this fairly simple.

The common image formats for container distribution provide additional benefits for patch management. Unlike a VM's disk image, the files in a container image are convenient to access and analyze offline. This includes access to the container's package information. Specialized software has emerged that reads this information and correlates it with a database of known vulnerabilities and patches, providing powerful possibilities, such as identifying missing patches before an application is deployed and more simply tracking vulnerabilities across many applications. In some cases, the software can be configured to take action in response to vulnerable containers. Taking the example of Heartbleed above, an operator could write a policy to immediately shut down any container with a known-vulnerable version of OpenSSL, while permitting containers with the required fixes to continue as normal.

Automating the container security process

In security circles, nirvana is the idea of integrating security into operational processes. Using its Entourage model and incorporating security into containers during configuration of the container image, ClearDATA has bridged the division between DevOps and security that exists in some organizations. This has led to more secure applications by marrying the role of DevOps with the responsibilities of security.

Reducing Attack Surfaces

Another basic security practice is reducing attack surfaces. For containers, just like any other process, this means preventing code with vulnerabilities from entering the environment, eliminating unnecessary service calls, and applying controls to file system access, network sockets and outbound/inbound connections. In many ways, containers are just like normal software. Containers can be created and deployed at lightning speed; thus, controlling least privilege for each container can be a daunting task.

System Activity

To reduce that attack surface, one must have visibility into container activity. Extracting meaningful activity metrics, such as activity or security information, can be difficult with existing tools (e.g. application firewalls, or host-based intrusion prevention systems [HIPS]), because these tools are not natively aware of sub-virtual machine components. Most monitoring tools on the market are just beginning to have a view of transient instances in public clouds, but have much work ahead to be able to monitor sub-virtual machine entities. Yet understanding the activity within the environment is critical to maintaining a secure environment. Specialized container security applications have some automated capabilities to monitor, model, report, and enforce container behavior.

Monitoring, vulnerability management and IDS tools installed on the virtual instances that host the containers will allow you to better address container security. However, logs will need to be organized by instance, not by container, task, or cluster.

Audit and Compliance

Visibility is also critical for creating logs and assessing compliance. If logs cannot be generated, those charged with ensuring compliance with regulatory requirements or security frameworks may not be able to properly audit a system. To overcome this challenge, ClearDATA ensures that central event logging is enabled and provides a full audit trail for container deployment and management, using state-of-the-art tools to facilitate both real-time monitoring as well as asynchronous analysis of container activity.

Using Containers to Comply with HIPAA

Containers do not present fundamentally new compliance challenges or require an overhaul of existing compliance strategies. In fact, containers can actually make compliance easier. For example, containers make it easy to package an application inside a container and deploy that application on a managed hosting platform that is designed specifically for HIPAA compliance, resulting in a wholly compliant production environment. On the flip side, making an environment compliant using virtual machines is complicated because the entire virtual machine image, including the OS, must be addressed.

HIPAA compliance using containers should primarily consider encryption of all data, including PHI, in motion, and at rest, as well as solid isolation of decrypted data from other programs running in AWS's cloud.

On AWS, treat PHI within and outside of a Virtual Private Cloud (VPC) as though it were being transferred and stored in a publicly accessible network. ClearDATA uses container-to-container network encryption, traffic isolation, and segmentation to ensure the highest levels of data protection using container clusters.

Encryption in Motion

To enable encryption in motion, a VPC should be used to create logical isolation from the internal network. Both public and private zones can be used, however, PHI should only be stored in private zones. VPCs should include access control lists, security policies, and default tenancy requirements. Use automation tools such as CloudFormation to define the VPC and update it as necessary.

A VPC creates a logical isolation of your resources, but it does not encrypt traffic as it travels the physical wires that connect real hosts. Therefore, both traffic internal to your VPC and traffic going to and from the public internet must be encrypted.

Private EC2 instances can create connections to the outside world via a NAT instance in the public zone of your network. Private EC2 instances may then be connected to using a Bastion server in your public zone.

Network traffic should be encrypted using HTTP over TLS as well as SSH Tunneling.

Encryption at Rest

To encrypt PHI at rest, both application and infrastructure layer encryption should be used. Application layer encryption varies depending on the application and is typically the data owner's responsibility. But infrastructure layer encryption is handled using Amazon's Encrypted Elastic Block Storage (EBS).

While Docker containers do not support persistent data, storage can be mounted as a "Docker volume" from containers. Docker volumes that store data may do so at the root volume of an EC2 instance, which should be architected to ensure that Docker volumes end up on an encrypted EBS rather than the unencrypted root EBS.

Breach Prevention using Containers and Microservices

Containers can effectively implement microservices because every containerized microservice has a unique role. Additionally, container orchestration composes the entire application by putting all relevant containers into communication with each other.

There are several advantages to this approach from a breach prevention perspective. First, preventing functions from having access to unauthorized services can force one container for one role, with one permission level, using one set of credentials. This strategy can kill privilege escalation exploits and resource traversal loopholes when sound access management rules are in place. Second, microservices can be quickly and easily swapped out for more efficient equivalents, or rolled back in case of a possible compromise without bringing down the rest of the system.

Incident Response

During an incident, the nature of an environment residing in Docker containers requires more focus on container access and interaction with data, and less focus on the host. Incident responders cannot approach incident investigation by tracking inter-container traffic, or leaving a machine online to see what is in memory (there is no running memory in Docker). This could potentially make it more difficult to see the source of an alert and the potential data accessed.[4]

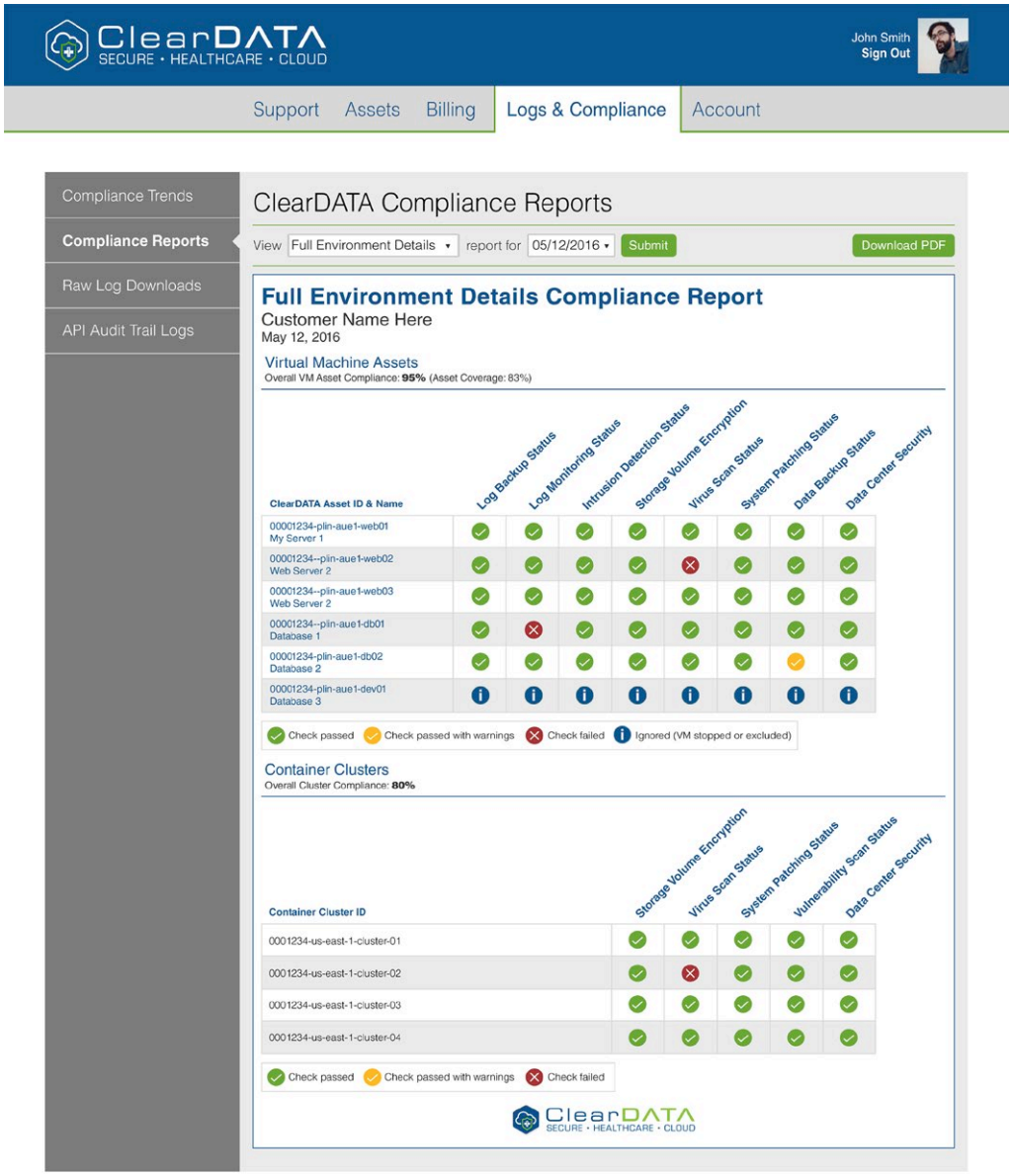
As security monitoring and alerting tools continue to mature, incident response for anything container-related should involve the Governance, Risk and Compliance (GRC), Security, and DevOps teams to ensure that the response is technically accurate. Runbooks should be updated to reflect the technology and the nuances of container environments.

Organizations should also invest in training teams on issues specific to containers so that incident investigation follow defined, repeatable, efficient processes.

4 McKay, Jason. "Docker Security: How to Monitor and Patch Containers in the Cloud." April 20, 2016. Accessed February 6, 2017. http://www.logicworks.net/blog/2016/04/docker-security-monitor-patch-containers-aws/.

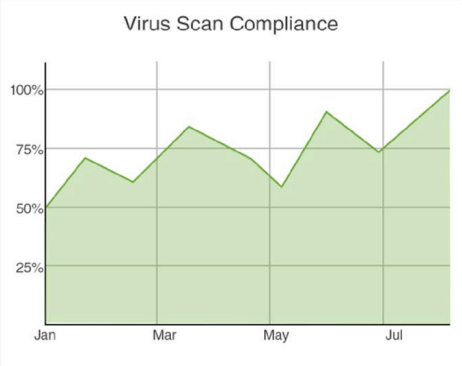
How to Validate Container Security & Compliance

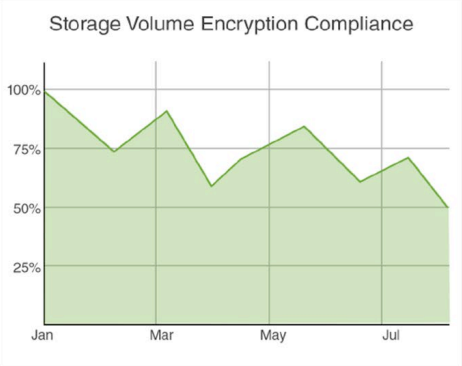
Visualization of compliance controls is vital to addressing deficiencies. ClearDATA helps to visualize trends through a dashboard that dynamically updates a container clusters' compliance state. This enables transparency and aids in demonstrating to security and compliance teams, as well as to auditors, that system activity is under constant review and issues are proactively addressed. If compliance issues are holding you back from embracing containers, it's time to rethink your strategy.

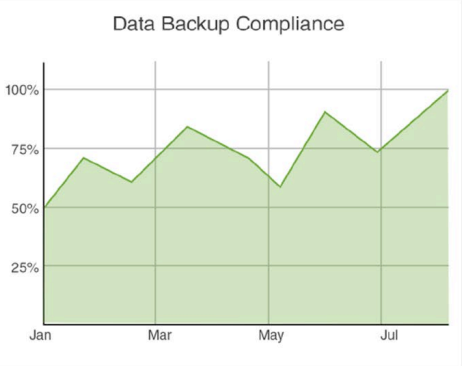


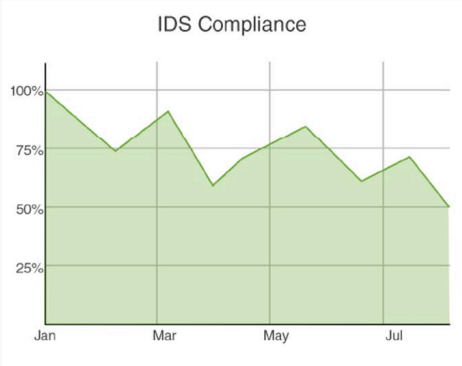
Virtual Machine Assets

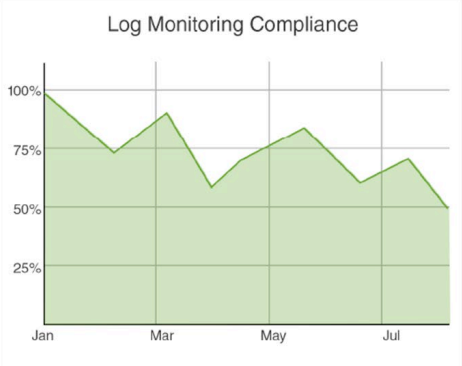
Overall VM Asset Compliance: **95%** (Asset Coverage: 83%)

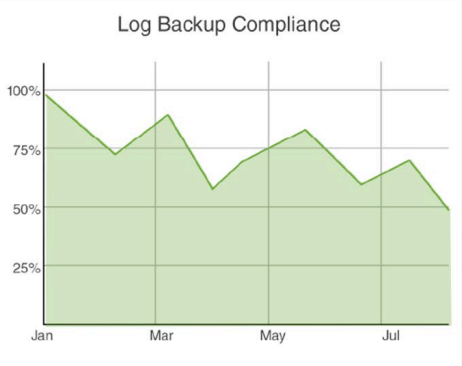






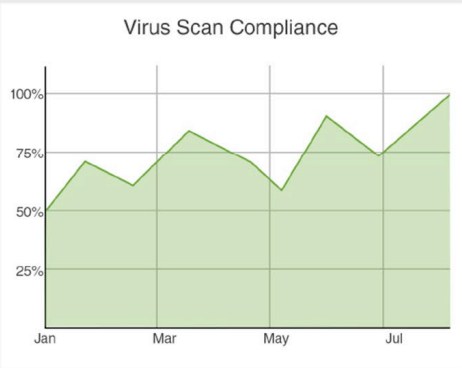


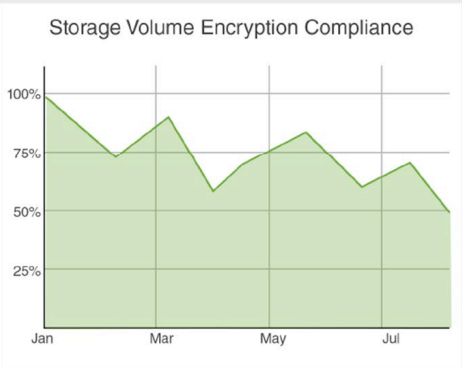


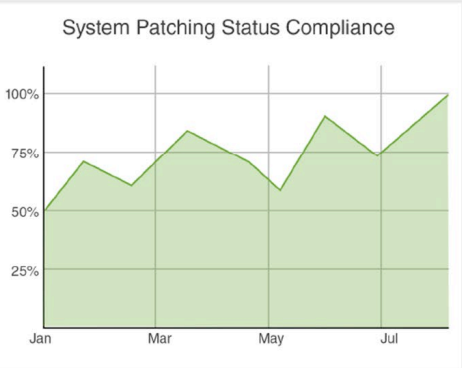


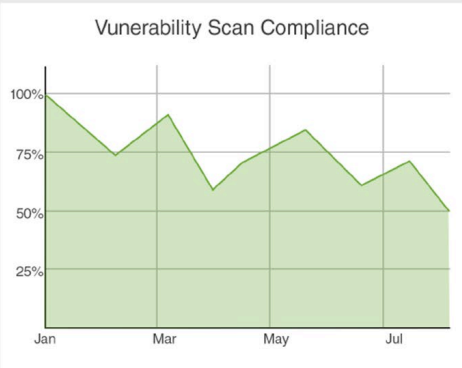
Container Clusters

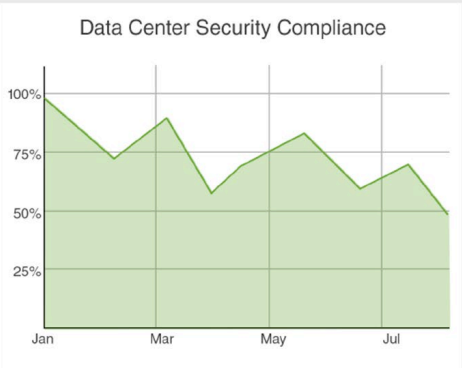
Overall Cluster Compliance: **95%**











Container Provider Vendor Diligence

The HITECH Act holds covered entities and business associates accountable to the Department of Health and Human Services (HHS) and to individuals for proper safeguarding of their private information.

HIPAA classifies a Business Associate as "a person who performs functions or activities on behalf of, or certain services for, a covered entity that involved the use or disclosure of individually identifiable health information."[5] This includes legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation or financial services entities. The Omnibus Rule in 2013, as well as official HHS guidance in October, 2016, has clarified that Cloud Providers are considered Business Associates, even if the cloud provider has no access to a customer's decryption keys.[6]

While diligence questionnaires seek information on many topics, including physical, administrative and technical controls, NIST Special Publication 800-30 [7] describes effective methods for assessing risks associated with federal systems, but aptly applies to private organizations and vendors as well. Other risk frameworks are used in the industry to attempt to measure risk. ClearDATA manages risk according the HITRUST Common Security Framework and requires that critical vendors undergo detailed reviews of physical, administrative and technical controls. In many cases, vendors are able to provide assurance from a third party, such as an independent audit report in the form of a SOC 2 Type II or a HITRUST certification.

Whatever framework is used to perform diligence, there are three basic questions affiliated with HIPAA and the HITECH Act's reasonable diligence in risk assessments:

- Have you identified the ePHI within your organization? This includes ePHI that you create, receive, maintain or transmit.
- What are the external sources of ePHI? For example, do vendors or consultants create, receive, maintain or transmit ePHI?

5 HHS-OCR Privacy Brief, Summary of the HIPAA Privacy Rule, p. 3 (2003)

6 Secretary, HHS Office of the. "Guidance on HIPAA & Cloud Computing." HHS.gov. October 06, 2016. Accessed February 13, 2017. https://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html.

7 "Guide for Conducting Risk Assessments." September 15, 2012. Accessed February 13, 2017. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf.

- What are the human, natural and environmental threats to information systems that contain ePHI?

Of course, ClearDATA recommends that organizations choose a container provider that has undergone the rigorous, independent examination of the HITRUST Alliance.

Security & Compliance Mapping

HIPAA compliance using containers is similar to HIPAA compliance using traditional virtual machines. An organization should continue to primarily consider encryption of all data, including PHI, in motion, and at rest, as well as solid isolation of decrypted data from other programs running in AWS's cloud.

Other requirements for HIPAA compliance still apply. Listed below are statutory mappings to the controls used for a compliance environment that utilizes ClearDATA's container products in an AWS environment. Descriptions below incorporate AWS control descriptions[8] assuming a ClearDATA managed environment.

8 HIPAA Compliance on AWS. February 10, 201. Accessed February 13, 2017. https://aws.amazon.com/quickstart/architecture/accelerator-hipaa/.

#	Statute	Rule	Description
1	164.308(a)(1)(i)	Security management process: Implement policies and procedures to prevent, detect, contain, and correct security violations.	ClearDATA ensures that Amazon CloudTrail and AWS Config (in regions where available) are employed to provide a configuration history, resource inventory, and review mechanisms for system changes. ClearDATA also implements policies and procedures to prevent, detect, contain, and correct security violations for the operating systems and assists your organization where need with security violations at the application layer where they may impact sensitive information.
2	164.308(a)(1)(ii)(D)	Implement procedures to regularly review records of IS activity such as audit logs, access reports, and security incident tracking.	ClearDATA provides a security and compliance dashboard for your environment. This dashboard aggregates information from AWS CloudTrail, AWS CloudWatch and CloudWatch Events, as well as status of specific components of a service, such as encryption, in order to support the capability for review of system activity by logging all security-relevant user/API activities, data access activities, and status. Log records are stored in an S3 bucket for access by auditors and/or log analysis tools and retained for 6 years.
3	164.308(a)(3)(i)	Workforce security: Implement policies and procedures to ensure that all members of workforce have appropriate access to ePHI, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information (ePHI).	ClearDATA and AWS tightly control physical access to data centers to prevent against unauthorized access to system hardware that contains PHI. ClearDATA configures your environment to use the appropriate database in RDS, and storage on EC2 using secondary EBS volumes. S3 buckets utilize policies that require encryption and IAM is configured with baseline access control policies for groups and roles to which authorized users may be assigned by your organization ClearDATA is responsible for ensuring the security of its workforce, under the shared responsibility model. If the exact details are needed a SOC2 report can be requested once a NDA is in place.

#	Statute	Rule	Description
4	164.308(a)(5)(ii)(C)	Implement procedures for monitoring log-in attempts and reporting discrepancies.	ClearDATA logs login attempts from the OS. Depending on your organization's requirements ClearDATA can also enable AWS CloudTrail, which provides the audit trail capability to monitor the use of AWS Identity and Access Management (IAM) accounts. ClearDATA also recommends that logs be aggregated to an S3 bucket centrally to store the CloudTrail audit logs. Using the ClearDATA compliance dashboard, your organization can regularly review AWS logs and respond to events.
5	164.308(a)(5)(ii)(D)	Implement procedures for creating, changing, and safeguarding passwords.	AWS Identity and Access Management (IAM) built-in features include the mechanisms for creating, changing, and protecting passwords for the AWS account. IAM enforces AWS account password policies such as minimum complexity, password expiration, re-use of old passwords, requirement for a new password to be entered upon login, etc. AWS IAM provides the capability for uniquely identifying and authenticating users, providing privileges based on the credentials, group memberships, and access policies assigned to them.
6	§164.308(a)(7)	Contingency plan: Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, or natural disaster) that damages systems that contain ePHI.	ClearDATA can configure your environment to incorporate multiple AWS Regions and Availability Zones, as well as S3 that is a highly durable and redundant storage service. This will enable your organization to transfer processing and storage to alternate sites. This approach constitutes a built-in alternate storage and processing capability that dynamically provides transfer and resumption of system operations in the event of failures due to fire, vandalism, hardware malfunctions, network/power outages, or a small area natural disaster. Availability Zones consist of one or more discrete data centers, each with redundant power, networking and connectivity, housed in separate facilities. These Availability Zones offer the ability to operate production applications and databases which are more highly available, fault tolerant and scalable than would be possible from a single data center. To address organizational requirements related to major regional disasters, ClearDATA and AWS support the ability to place data in multiple geographic regions. ClearDATA can assist your organization with modifying this architecture to employ additional AWS regions and cross-region data synchronization, load balancing, etc.
	164.308(a)(7)(ii)(A)	Establish and implemented procedures to create and maintain retrievable exact copies of ePHI	ClearDATA architects your organization's environment to limit ePHI storage to an Amazon RDS database, Amazon S3 buckets, and potentially secondary EBS volumes attached to EC2 instances that reside in a private subnet. AWS built-in features provide a full back up of RDS using a full daily snapshot as well as through transaction logging at approximately five-minute intervals. This architecture is configured to retain RDS backups for the default of 1 day, which can be increased to 35 days by the customer. AWS also employs live storage redundancy for Amazon S3, which provides 99.999999999% durability of objects over a given year. This architecture employs multiple AWS Availability Zones, which constitutes an inherent alternate storage site capability for data stored in Amazon S3 and Amazon RDS databases. S3 uses multiple Availability Zones by default, and the RDS databases.

#	Statute	Rule	Description
7	164.308(a)(7)(ii)(B)	Established (and implemented as needed) procedures to restore any loss of ePHI data stored electronically.	ClearDATA configures the environment to limit the storage of ePHI Amazon RDS database, Amazon S3 buckets and potentially secondary EBS volumes attached to the application/web server EC2 instances. Full database recovery from snapshot or point-in-time can be initiated from the RDS console/API. The Amazon S3 managed service features inherent redundancy, so that no customer-initiated data recovery operation is required. ClearDATA also configures all EBS volumes to be backed up through the use of EBS snapshots, with all backups retained for 30 days. ClearDATA configures all backups of data to address any requirements related to the recovery of individual S3 objects, RDS database objects, or EBS files, filesystems that are destroyed, modified, overwritten by logical actions and to mitigate any residual risk of data loss caused by AWS hardware failures. Using the ClearDATA Security and Compliance Dashboard your organization may monitor the success or failure of all backups in the environment.
8	164.308(a)(7)(ii)(C)	Established (and implemented as needed) procedures to enable continuation of critical business processes and for protection of ePHI while operating in the emergency mode.	ClearDATA uses multiple AWS Availability Zones, Amazon S3 storage, and a replicated RDS database to enable a live alternate storage and processing capability that dynamically provides transfer and resumption of all system operations. Multiple AWS Availability Zones and redundant storage and processing provide identical security safeguards for the protection of ePHI.
9	164.308(b)(1)	Business associate contracts and other arrangements: A covered entity, in accordance with Sec. 164.306, may permit a business associate to create, receive, maintain, or transmit ePHI on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with Sec. 164.314(a) that the business associate appropriately safeguards the information.	ClearDATA uses the services of AWS. ClearDATA has a Business Associate Agreement in place with AWS that extend ClearDATA's obligations to that relationship. ClearDATA also negotiates "purpose-built" Business Associate Agreements with our customers that includes duties to mitigate harm, address incident response and breach notification procedures, as well as outline liability in the case of an incident that leads to reportable events.
10	164.310(a)(1)	Facility access controls: Implement policies and procedures to limit physical access to electronic information systems and the facility or facilities in which they are housed, while ensuring properly authorized access is allowed.	Physical Environment controls associated with AWS data center facilities and the hardware components within them is generally inherited from AWS as part of the shared responsibility model. Your organization is responsible for any part of the requirement that is applicable to your physical property and the applications. ClearDATA is responsible for the logical infrastructure with the AWS account, including the Operating systems on EC2 instances.
11	164.310(a)(2)(i)	Establish (and implemented as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan.	Procedures associated with AWS access to its data center facilities and the hardware components within them as part of a recovery operation is generally inherited from AWS as part of the shared responsibility model. Your organization is responsible for any part of the requirement that is applicable to your physical property and your organization's applications. ClearDATA remains responsible for the configurable portion of the logical infrastructure with the AWS account, including the Operating systems on EC2 instances.
12	164.310(a)(2)(ii)	Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.	Safeguarding the physical environment of AWS data center facilities and the hardware components within them is generally inherited from AWS as part of the shared responsibility model. Your organization is responsible for any part of the requirement that is applicable to your physical property and your organization's applications. ClearDATA remains responsible for the configurable portion of the logical infrastructure with the AWS account, including the Operating systems on EC2 instances.

#	Statute	Rule	Description
13	164.310(a)(2)(iii)	Implement procedures to control and validate a person's access to facilities based on his/her role or function, including visitor control, and control of access to software programs for testing and revision.	Procedures associated with controlling access to AWS data center facilities and the hardware components within them as part of a recovery operation is generally inherited from AWS as part of the shared responsibility model. Your organization is responsible for any part of the requirement that is applicable to your physical property and your organization's applications. ClearDATA remains responsible for the configurable portion of the logical infrastructure with the AWS account, including the Operating systems on EC2 instances.
14	164.310(a)(2)(iv)	Implement policies and procedures to document repairs and modifications to the physical components of a facility that are related to security (for example, hardware, walls, doors, and locks).	Maintenance controls associated with AWS facilities and hardware components is generally inherited from AWS as part of the shared responsibility model. Your organization is responsible for any part of the control that is applicable to your organization's configurable portion of the logical infrastructure. ClearDATA maintains responsibility for the Operating systems on EC2 instances while your organization assumes the responsibility for its applications.
15	164.310(d)(1)	Device and media controls: Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain ePHI into and out of a facility, and the movement of these items within the facility.	Media protection and control associated with storage devices and media within AWS is generally inherited from AWS as part of the shared responsibility model. AWS has a strict policy that prohibits the removal of ANY storage device or media, unless it has been properly degaussed and destroyed. ClearDATA and your organization share responsibility for any part of the control that is applicable to your organization's configurable portion of the logical infrastructure, including the Operating systems on EC2 instances. Your organization maintains responsibility for its applications and on-premise storage media and devices.
16	164.310(d)(2)(i)	Implement policies and procedures to address final disposition of ePHI, and/or hardware or electronic media on which it is stored.	Media protection and control associated with storage devices and media within AWS is generally inherited from AWS as part of the shared responsibility model. AWS has a strict policy that prohibits the removal of ANY storage device or media, unless it has been properly degaussed and destroyed. ClearDATA and your organization share responsibility for any part of the control that is applicable to your organization's configurable portion of the logical infrastructure, including the Operating systems on EC2 instances. Your organization maintains responsibility for its applications and on-premise storage media and devices.
17	164.310(d)(2)(ii)	Implement procedures for removal of ePHI from electronic media before the media are available for reuse.	AWS Built-in features erase all data stored or processed on shared resources (storage, memory, CPU) before those resources are re-provisioned to other AWS users or AWS accounts.
18	164.310(d)(2)(iii)	Maintain a record of the movements of hardware and electronic media and the person responsible for its movement.	Maintenance controls associated with AWS facilities and hardware components is generally either inherited from AWS as part of the shared responsibility model. ClearDATA maintains responsibility for the Operating systems on EC2 instances while your organization assumes the responsibility for its applications.
19	164.310(d)(2)(iv)	Create a retrievable, exact copy of ePHI, when needed, before moving equipment.	ClearDATA configures your environment to limit the storage of ePHI storage to Amazon RDS database, Amazon S3 buckets, and potentially secondary EBS volumes attached to the application/web server EC2 instances, which employ AWS built-in hardware storage redundancy to maintain exact copies of ePHI at all times. In this virtual environment, there is no movement of equipment. AWS is responsible for hardware maintenance activities that involve movement of physical equipment, and maintains storage redundancy to ensure that your organization's data is not impacted by any infrastructure maintenance /hardware moves. AWS built-in features provide a full back up of RDS using a full daily snapshot as well as through transaction logging at approximately five-minute intervals. This architecture is configured to retain RDS backups for the default of 1 day, which can be increased to 35 days. AWS also employs live storage redundancy for Amazon S3, which provides 99.999999999% durability of objects over a given year. Amazon EBS is replicated across multiple volumes within a single availability zone. ClearDATA also configures all EBS volumes to be backed up through the use of EBS snapshots, with all backups retained for 30 days.

#	Statute	Rule	Description
			Continued This architecture employs multiple AWS Availability Zones, which constitutes an inherent alternate storage site capability for data stored in Amazon S3 and Amazon RDS databases. S3 uses multiple Availability Zones by default, and the RDS databases deployed within this architecture are configured to be replicated across multiple Availability Zones, which instantiates a retrievable exact copy of ePHI.
20	164.312(a)(1)	Implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights as specified in Sec. 164.308(a)(4).	Access controls should always be defaulted to no access unless overridden manually, and then only according to compliant policies, procedures and periodic reviews ClearDATA creates an architecture that employs a baseline set of AWS Identity and Access Management (IAM) groups and roles to support alignment of user accounts to personnel roles at various levels of privilege related to infrastructure/platform management (e.g. Billing, EC2/VPC/ RDS systems administration, I.T. auditing, etc.) IAM enforces access to the AWS infrastructure. Login/API access is restricted to those users for whom the organization has authorized and created or federated IAM user accounts, and provided IAM group and/or role membership (which specify access policies). S3 buckets in should have specific policies to restrict access to appropriate roles/groups, based on various criteria and under various conditions. Your organization is responsible for 1) authorizing users before granting system permissions, and 2) ensuring that only authorized persons are assigned permissions within AWS IAM. ClearDATA can assist your organization with configuring access control mechanisms within applications and operating systems to also enforce access authorizations.
21	§164.312(a)(2)(i)	Assign a unique name and/or number for identifying and tracking user to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4).	AWS Identity and Access Management (IAM) built-in features provide the capability for uniquely identifying and authenticating users. Your organization, at its discretion, may provide user accounts and privileges to both organizational non-organizational users in addition to organizational users. ClearDATA configures CloudTrail and Amazon S3 Bucket logging which provides tracking/audit trail feeds to your ClearDATA Compliance Dashboard giving you the capability to monitor the use of AWS IAM accounts for both interactive and non-interactive API-based user activity and data access activity. An Amazon S3 bucket centrally contains the CloudTrail audit logs.
22	164.312(a)(2)(ii)	Establish (and implemented as needed) procedures for obtaining necessary ePHI during an emergency.	The use of multiple AWS Availability Zones, Amazon S3 storage, and a replicated RDS database constitutes a built-in, live alternate storage and processing capability. ePHI storage is limited to the Amazon RDS database, Amazon S3 buckets, and potentially secondary EBS volumes attached to the application/web server EC2 instances, which employ storage redundancy to maintain exact copies of ePHI at all times. ClearDATA also configures all EBS volumes to be backed up through the use of EBS snapshots, with all backups retained for 30 days. AWS built-in features provide the connectivity capabilities for accessing the AWS account environment from any location approved and configured by the customer, which supports the capability for accessing AWS resources and ePHI data during an emergency. ClearDATA can work with your organization to create the procedural documentation regarding how to access ePHI data in an emergency situation.

#	Statute	Rule	Description
23	164.312(a)(2)(iii)	Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.	The AWS console and remote API/CLI sessions employ Amazon STS tokens which automatically expire after 24 hours by default, regardless of activity, which terminates the electronic session. ClearDATA works with your organization to ensure that the operating system is configured to terminate SSH/RDP connections after a set timeout threshold if the 24 hours auto log off timer for the AWS console is not sufficient, at the application level, your organization is responsible for ensuring that the application has an auto log off timer.
24	164.312(a)(2)(iv)	Implement a mechanism to encrypt and decrypt ePHI	For data at rest, AES-256 Server Side encryption is employed for data stored in S3 and RDS databases, as well as for full disk encryption of an EBS data volume that is attached to the application/web server EC2 instances, to support the capability of storing ePHI on a local volume if required. For data in transit, to protect against exposure of any cleartext ePHI transmitted deliberately or incidentally during interactive systems management operations, all AWS Management Console sessions, API call sessions, and Amazon S3 object access can only be conducted over encrypted sessions via TLS; EC2 instances and associated security groups are configured for encrypted SSH sessions only. For web user access, the Elastic Load Balancer (ELB) employs TCP pass-through to the EC2 endpoints to enforce end-to-end HTTPS encryption. While this architecture includes secondary encrypted volumes for EC2 instances, ClearDATA can help your organization configure the system to use that volume according to organizational requirements, such as for the paging file, system logging, and application logs to the secondary drive to prevent any spillage of ePHI on a non-encrypted volume. ClearDATA can also employ any file encryption /decryption tools, PKI system, Amazon KMS, Amazon CloudHSM, etc. to provide any other encryption /decryption or key management capabilities required by your organization.
25	164.312(b)	Implement audit controls, hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.	ClearDATA ensures that AWS CloudTrail, S3 bucket logging, and Elastic Load Balancer (ELB) logging are enabled to record security-relevant user/API activities, data access activities, and source and destination addresses. Log records are stored in an S3 bucket for access by auditors and/or log analysis tools. ClearDATA also enables CloudWatch for audit log monitoring and make sure that the operating system has logging enabled. ClearDATA's Security and Compliance dashboard can aid your organizational requirement to implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI to enable the §164.308(a)(1)(ii)(D) Information System Activity Review procedure.
26	164.312(c)(1)	Integrity: Implement policies and procedures to protect ePHI from improper alteration or destruction.	ClearDATA employs a combination of access control mechanisms and cryptographic mechanisms to protect confidentiality and integrity (to include alteration and destruction) of data at rest and in transit. For data at rest, Amazon S3 storage buckets include access control policies which restrict data read/write/delete to authorized AWS IAM roles/groups, with a default-deny permissions model. A baseline set of IAM policies are in place for associated job functions for those authorized IAM users assigned to the IAM roles/groups. AES-256 Server Side encryption is employed for data stored in S3, RDS databases and for full disk encryption of an EBS data volume that is attached to the application/web server instances, to support the capability of storing ePHI on a local volume if required. In addition, versioning is enabled on S3 buckets so that original content is retained upon any data object changes for potential comparison, and bucket logging is enabled to log changes.

#	Statute	Rule	Description
			Continued For data in transit, to protect against exposure of any cleartext ePHI transmitted deliberately or incidentally during interactive systems management operations, all AWS Management Console sessions, API call sessions, and Amazon S3 object access can only be conducted over encrypted sessions via TLS; EC2 instances and associated security groups are configured for encrypted SSH sessions only. For web user access, the Elastic Load Balancer (ELB) employs TCP pass-through to the EC2 endpoints to enforce end-to-end HTTPS encryption.
27	164.312(c)(2)	Implement electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner.	ClearDATA ensures that AWS CloudTrail, S3 bucket logging, and Elastic Load Balancer (ELB) logging are enabled to log all security-relevant user/API activities, data access activities, with the associated source and destination IP addresses. Log records are stored in an S3 bucket for access by auditors and/or log analysis tools. Versioning is enabled on the web data and log S3 buckets so that original content is retained upon any data object changes for potential comparison, and bucket logging is enabled to log changes. ClearDATA can assist you with employing any additional required file integrity management system and/or logging tools to perform corroboration or to detect unauthorized changes or removal of Amazon S3 objects, RDS database objects, as well as files that reside on EC2 instance filesystems, per organizational requirements.
28	164.312(e)(1)	Transmission security: Implement technical security measures to guard against unauthorized access to ePHI being transmitted over an electronic communications network.	ClearDATA and AWS employ TLS for Console access, CLI, and API endpoints for AWS service access, Amazon S3 for object access, and AWS Elastic Load Balances (ELB) endpoints for user web access. TLS/SSH ports and protocols are enforced by Security Groups.
29	164.312(e)(2)(i)	Implement security measures to ensure electronically transmitted ePHI is not improperly modified without detection until disposed of.	ClearDATA ensures that transmitted information is protected via a combination of network access control mechanisms (for data confidentiality) and encryption features (for both confidentiality and integrity). The AWS Management Console sessions, AWS API calls and Amazon S3 object access can only be conducted over TLS. All EC2 instances and associated security groups are configured for SSH login access only. ClearDATA can assist your organization with employing any additional required file integrity management system and/or logging tools to detect unauthorized changes to Amazon S3 objects, RDS database objects, as well as files that reside on EC2 instance filesystems, per organizational requirements.
30	164.312(e)(2)(ii)	Implement a mechanism to encrypt ePHI whenever deemed appropriate.	ClearDATA employs encryption mechanisms for data at rest and in transit. For data at rest, AES-256 Server Side encryption is employed for data stored in S3, RDS databases and for full disk encryption of an EBS data volume that is attached to the EC2 instances, to support the capability of storing ePHI on a local volume if required. For data in transit, to protect against exposure of any cleartext ePHI transmitted deliberately or incidentally during interactive systems management operations, all AWS Management Console sessions, API call sessions, and Amazon S3 object access can only be conducted over encrypted sessions via TLS; EC2 instances and associated security groups are configured for encrypted SSH sessions only. For web user access, the Elastic Load Balancer (ELB) employs TCP pass-through to the EC2 endpoints to enforce end-to-end HTTPS encryption.

Conclusion

The cloud is an incredible resource, providing access to a tremendous amount of processing power at a minimal expense. However, organizations must remain aware of the fact that using the cloud is essentially using a shared space. It was much easier to be certain that a connection was secure when the physical wire was traceable. It was much easier to see that a network was isolated when the firewall is disconnected from the internet. In the cloud, even isolated networks are shared and should be built with that in mind.

Containers Solve Specific Healthcare Challenges

The care-giving process generates massive amounts of data that follows the patient throughout the process. Data is not only generated by the EMR, but also by ancillary applications, including monitoring, care collaboration, patient management and consent, medication management, home monitoring, and telemedicine.

Containers enable information to flow in a way that is nearly instantaneous, secure and compliant, and transparent and effective, whether from a doctor's laptop to a production environment or perhaps from a physical machine in a data center to a virtual machine in a private or public cloud.

Effective use of containers allows remaining efforts to focus on data standards and compatibility, whether using FHIR (XML), HL7 (pick a flavor), or even JSON. Removing the barriers of how the application and data is delivered can yield significant benefits to the healthcare data lifecycle by putting the right data in the right place, at the right time; ultimately resulting in improved patient experience and care.

Containers can be Secure and Bolster Compliance

Containers do not present fundamentally new compliance challenges or require an overhaul of existing compliance strategies. In fact, containers can actually make compliance easier.

Care must be taken, however, to ensure that your container strategy, deployment methodology, monitoring protocols, and vulnerability management practices are harmonized in a manner that complies with the HIPAA Security Rule, as well as industry recognized security frameworks such as NIST, ISO, CSF and PCI DSS.

HIPAA compliance using containers should primarily consider encryption of all data, including PHI, in motion, and at rest, as well as solid isolation of decrypted data from other programs running in AWS's cloud.

ClearDATA recommends that organizations choose a container provider that has undergone the rigorous, independent examination of the HITRUST Alliance.

About ClearDATA

ClearDATA is the trusted managed cloud provider, designed for today's healthcare security needs. The ClearDATA managed cloud protects sensitive healthcare data using purpose-built DevOps automation, compliance and security safeguards, and healthcare expertise—all backed by managed cloud services.

More than 350,000 healthcare professionals trust the ClearDATA HIPAA-compliant cloud to protect their patient data and power their critical applications.

Authors and Contributors

Chris Bowen, Chief Privacy & Security Officer

Matt Ferrari, Chief Technology Officer

Ross Vandegrift, Principal DevOps Engineer

Dave Malone, Director of Engineering

Nathan Anderson, Director of Engineering

Jim Gibson, Director of Strategic Accounts

Conor Colgan, Solution Architect

Allen Nearing, DevOps Engineer

About Us

ClearDATA is the nation's fastest growing healthcare cloud computing company. More than 310,000 healthcare professionals rely on ClearDATA's HIPAA compliant cloud computing HealthDATA platform and infrastructure to store, manage, protect and share their patient data and critical applications.

For more information

101 West 6th Street, Austin TX

(800) 804-6052

www.cleardata.com

ClearDATA
SECURE • HEALTHCARE • CLOUD

amazon web services | Partner Network
ADVANCED CONSULTING PARTNER
HEALTHCARE COMPETENCY
AUTHORIZED PUBLIC SECTOR PARTNER