logicworks

HIPAA Compliance on AWS

Checklist

HIPAA on AWS Checklist

logicworks

Healthcare companies that are accustomed to complete control over physical systems often struggle to understand their responsibilities in a cloud environment. Who is responsible for which aspects of compliance? Can healthcare companies trust Amazon with their mission-critical apps and sensitive data? What are the rules and boundaries for AWS compliance?

Mastering these intricacies can help you create compliance-ready systems on AWS. In this checklist, we list the requirements that the team at Logicworks uses to build HIPAA compliant environments on AWS. We then map each of these requirements to a specific control in HIPAA or HITRUST requirements.

Important Information about HIPAA on AWS

New AWS customers often ask: Is AWS compliant with HIPAA? The answer to this question is complex. The short answer is that AWS is not "HIPAA compliant", but it provides services that facilitate HIPAA compliance.

The U.S. Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules for protecting Protected Health Information (PHI) does not provide a certification or Attestation of Compliance to cloud providers or to healthcare companies. HIPAA is a set of federal regulations, not a security standard. A company and its business associates can be periodically audited for compliance with HIPAA regulations by the HHS Office for Civil Rights (OCR), and in the course of that audit it can meet or fail to meet those requirements, but it cannot be "Certified HIPAA Compliant".

In order to process, store, or transmit PHI in AWS, a healthcare company (the "covered entity") must sign a Business Associate Agreement (BAA) with AWS, meaning that AWS is performing function or activities on behalf of the covered entity. However, signing a BAA with AWS does not mean that the customer is "HIPAA compliant". The customer can maintain compliance with HIPAA regulations through its own efforts to use cloud tools, architect applications, control access, etc. in a manner that complies with those regulations. AWS only assumes responsibility for physical hardware security controls of a limited number of covered services.

HIPAA on AWS Checklist

logicworks

The HITRUST CSF integrates the requirements of the HIPAA Security Rule with the standards of NIST, HITECH, PCI DSS, and other controls, facilitating a unified cont ol rationalization. The HITRUST CSF is a cybersecurity framework that can be used (like NIST, ISO, etc.) as a foundation for your HIPAA assessment. In this guide, we've also supplied the relevant HITRUST control for each requirement.

About this Checklist

The goal of this checklist is to help provide guidance on specific controls and tools to use in AWS that help maintain compliance with HIPAA standards. Wherever possible, we also provide a link to relevant AWS documentation and the specific HIPAA and HITRUST control. Following this checklist does not guarantee HIPAA or HITRUST compliance.

About Logicworks

Logicworks is an AWS Premier Consulting Partner with 25+ years of experience managing complex healthcare IT projects. We undergo six annual compliance audits, including HIPAA and HITRUST, and currently manage 80 million+ ePHI records across dozens of healthcare customers on AWS.

This guide was created by Logicworks' Information Security and Compliance teams, and directly reflects our approach to architecting for healthcare customers on AWS.

aws partner network

Premier

Consulting Partner

- Security Competency
- Migration Competency
- Healthcare Competency
- DevOps Competency
- MSP Partner

HIPAA on AWS Checklist

logicworks

Requirement	How to Satisfy Requirement on AWS	Link to AWS Documentation	Relevant HIPAA/ HITRUST Control	Status
Access Control				
Use role-based access control (RBAC) to assign permissions to users, groups, and applications	Manage roles and permissions in the Access control (IAM) console page.	https://docs.aws.amazon.com/IAM/latest/UserGuide/getting-started.html	HIPAA §164.312(a)(1)), §164.308(a)(3), HITRUST: 01.b, 01.c	
Rotate passwords and keys every 45-90 days	Set up AWS Key Management System and rotate keys.	https://docs.aws.amazon.com/kms/latest/developerguide/overview.html	HIPAA §164.308(a)(5), HITRUST: 01.d	
Use two-step authentication	Enable MFA for IAM users or purchase a 3rd party MFA solution.	https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa.html	HIPAA: §164.308(a)(5) HITRUST: 05.k 01.j	
Monitor for suspicious actions related to your user accounts	Monitor for risky sign-ins using AWS CloudTrail and receive alerts related to unusual behavior. Potentially use AWS Guard Duty, which uses machine learning and anomaly detection to indentify and prioritize potential threats.	https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-getting-started.html	HIPAA §164.308(a)(5)(ii)(C), §164.312(b), §164.308(a)(1)(ii)(D), HITRUST 09.aa - 09.ae	
Remove access for terminated users	Remove old users from role in AWS IAM.	https://docs.aws.amazon.com/IAM/latest/UserGuide/id_users_manage.html#id_users_deleting	HIPAA §164.308(a)(3)(ii)(C), HITRUST 02.g, 02.h, 02.i	

HIPAA on AWS Checklist

logicworks

Requirement	How to Satisfy Requirement on AWS	Link to AWS Documentation	Relevant HIPAA/ HITRUST Control	Status
Restrict permissions to external accounts	Remove any users with non-AD accounts (ex. abc@yahoo.com).	https://docs.aws.amazon.com/IAM/latest/UserGuide/id_users_manage.html	HIPAA §164.312(a)(1)), HITRUST 01.j	
Networking				
Restrict inbound and outboud traffic, deny all other traffic	Create security rules with a Security Group.	https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html	HIPAA §164.312(c)(1), HITRUST 09.m	
Install and maintain a firewall configuration	Implement AWS WAF and integrate logs into AWS CloudWatch logs.	https://docs.aws.amazon.com/waf/latest/developerguide/getting-started.html	HIPAA §164.312(c)(1), HITRUST 01.m	
Use strong cryptography and security protocals over public networks	Configure HTTPS on an AWS CloudFront-managed (or your own) certificate.	https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/using-https.html	HIPAA §164.312(c)(1), §164.312(e)(1)(B)), HITRUST 06.d	
Protect against DDoS attacks	Architect your infrastructure for scale using Route 53, CloudFront, and AWS WAF. Optionally integrate with AWS Shield, a managed DDoS protection service.	https://docs.aws.amazon.com/waf/latest/developerguide/shield-chapter.html	HIPAA: § 164.316(a), § 164.308(a)(1)(ii)(B) HITRUST: 03.a, 03.c, 03.d, 01.04, 05.h, 06.f	
Install and maintain an Intrusion Detection System (IDS)	Implement a 3rd party IDS solution.	https://aws.amazon.com/mp/scenarios/security/ids/	HIPAA §164.312(c)(1)), §164.308(a)(1)(ii)(D) HITRUST 09.ab, 09.m, 09.q, 09.v, 09.x, 10.c, 10.d, 11.a	

HIPAA on AWS Checklist

logicworks

Requirement	How to Satisfy Requirement on AWS	Link to AWS Documentation	Relevant HIPAA/ HITRUST Control	Status
Implement internal and external vulnerability scanning	Implement a 3rd party vulnerability scanning solution. There is no AWS-native solution.	https://aws.amazon.com/security/penetration-testing/	HIPAA §164.316(a), §164.308(a)(1)(ii)(B) HITRUST 03.a, 03.c, 03.d, 01.04, 05.h, 06.f	
Monitoring and Logging				
Enable monitoring of resource performance	AWS CloudWatch is enabled by default. You can set up custom metrics in CloudWatch as necessary and send metric data for instances in 1-minute periods for an additional cost ("detailed monitoring").	https://aws.amazon.com/cloudwatch/getting-started/	N/A	
Retain audit trail history if necessary, usually for up to one year	Automate long-term log archival from Amazon S3 to Amazon Glacier and specify retention time using log profiles.	https://docs.aws.amazon.com/amazonglacier/latest/dev/working-with-vaults.html	HIPAA §164.312(b), §164.308(a)(1)(ii)(D), HITRUST 09.aa, 09.ab, 09.ad, 09.ae	
Regularly review logs	Either manually review logs from AWS CloudWatch Logs, VPC flow logs, and other sources or purchase an external log reviewer service.	N/A	HIPAA §164.312(b), §164.308(a)(1)(ii)(D) HITRUST 01.s, 06.i, 09.aa, 09.ab, 09.ad, 09.ae	
Virtual Machines				
Install anti-virus on your instances	Implement a 3rd party anti-virus solution.	https://aws.amazon.com/marketplace/search/results?x=0&y=0&searchTerms=Antivirus	HIPAA §164.308(a)(5)(ii)(B) HITRUST 09.j, 09.ab, 02.e, 09.k	

HIPAA on AWS Checklist

logicworks

Requirement	How to Satisfy Requirement on AWS	Link to AWS Documentation	Relevant HIPAA/ HITRUST Control	Status
Regularly patch your Azure VMs	Use AWS Systems Manager to schedule and automate updates.	https://docs.aws.amazon.com/systems-manager/latest/userguide/systems-manager-state.html	HIPAA §164.308(a)(5)(ii)(B), HITRUST 10.m	
Use CIS Hardened Images	Purchase CIS Hardened Images in the AWS Marketplace.	https://aws.amazon.com/marketplace/seller-profile?id=dfa1e6a8-0b7b-4d35-a59c-ce272caee4fc	HIPAA §164.310(c), HITRUST 10.m	
Automation				
Provision and update resources using declarative templates	Use AWS CloudFormation templates rather than building resources in the AWS CLI. When you need to change a resource, tear it down and rebuild from the template.	https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/Welcome.html	N/A	
Automate release management	Use AWS CodeDeploy to automate your CI/CD pipeline with predefined approval workflows.	https://docs.aws.amazon.com/codedeploy/latest/userguide/welcome.html	N/A	
Miscellaneous				
Encrypt data in transit	Use AWS Certificate Manager to provision and manage certificates so you can configure SSL/TLS protocol.	https://docs.aws.amazon.com/acm/latest/userguide/acm-overview.html	HIPAA §164.312(e)(2)(ii), HITRUST 06.d	

HIPAA on AWS Checklist

logicworks

Requirement	How to Satisfy Requirement on AWS	Link to AWS Documentation	Relevant HIPAA/ HITRUST Control	Status
Encrypt data at rest	Enable server-side encryption in Amazon S3, EBS, and EFS, etc. by requesting the service to encyrpt your data before saving it to disks. Use customer-managed keys in AWS Key Management Services.	https://docs.aws.amazon.com/kms/latest/developerguide/overview.html	HIPAA §164.312(e)(2)(ii), HITRUST 06.d	
Establish a data backup plan	Conigure backups from Amazon EBS volumes, RDS databases, file systems, etc. to Amazon S3, or use AWS Backup as a fully-managed solution.	https://docs.aws.amazon.com/aws-backup/latest/devguide/whatisbackup.html	HIPAA §164.308(a)(7), §164.308(7)(ii) (B), §164.308(7)(ii) (A), HITRUST 09.l	
Implement a Business Associate agreement with covered entities	Access and sign the Amazon BAA in Amazon Artifacts. Use only Covered Services.	https://aws.amazon.com/artifact/faq/	HIPAA §164.314 (i)	
Enable File Integrity Monitoring (FIM)	Implement a 3rd party FIM solution or open-source solution (such as OSSEC).	N/A	HIPAA §164.312(c)(1)), §164.308(a)(1)(ii)(D) HITRUST 09.ab, 09.m, 09.q, 10.c, 10.d	