dash

AWS HIPAA Compliance Matrix

Who Is Responsible For HIPAA Compliance?

Most major public cloud providers including, Amazon Web Services (AWS), Google Cloud Platform (GCP) and Microsoft Azure follow a “Shared Responsibility Model” for security and compliance. This means that security and compliance are a shared responsibility between the cloud platform and the cloud customer. This applies not only for regulatory compliance such as HIPAA/HITECH, PCI DSS, and FedRAMP, but also for cybersecurity frameworks such as NIST CSF and ISO 27001. Cloud providers implement a certain set of security protections and safeguards, but customers are responsible for building secure solutions with these cloud services.

ADMINISTRATIVE SAFEGUARDS			
164.308(a)(1)(i)	**Security Management Process**	Customer	ComplyOps - Risk Mgmt Policy
164.308(a)(1)(ii)(A)	Risk Analysis	Customer	ComplyOps - Risk Mgmt Policy
164.308(a)(1)(ii)(B)	Risk Management	Customer	ComplyOps - Risk Mgmt Policy
164.308(a)(1)(ii)(C)	Sanction Policy	Customer	ComplyOps - Employee Policy
164.308(a)(1)(ii)(D)	Information System Activity Review	Customer	ComplyOps - Risk Mgmt Policy
164.308(a)(1)(ii)(D)	**Assigned Security Responsibility**	Customer	ComplyOps - Roles Policy
164.308(a)(3)(i)	**Workforce Security**	Customer	ComplyOps - Employee Policy
164.308(a)(3)(ii)(A)	Authorization and/or Supervision	Customer	ComplyOps - Employee Policy
164.308(a)(3)(ii)(B)	Workforce Clearance Procedure	Customer	ComplyOps - Employee Policy
164.308(a)(3)(ii)(C)	Termination Procedures	Customer	ComplyOps - Employee Policy
164.308(a)(4)(i)	**Information Access Management**	Customer	ComplyOps - System Access Policy
164.308(a)(4)(ii)(A)	Isolation Health Clearinghouse Functions	Customer	ComplyOps - System Access Policy
164.308(a)(4)(ii)(B)	Access Authorization	Customer	ComplyOps - System Access Policy
164.308(a)(4)(ii)(C)	Access Establishment and Modification	Customer	ComplyOps - System Access Policy
164.308(a)(5)(i)	**Security Awareness Training**	Customer	ComplyOps - Employee Policy
164.308(a)(5)(ii)(A)	Security Reminders	Customer	ComplyOps - Administrative Reminders
164.308(a)(5)(ii)(B)	Protection from Malicious Software	Customer	ComplyOps Monitoring
164.308(a)(5)(ii)(C)	Log-in Monitoring	Customer	ComplyOps Monitoring
164.308(a)(5)(ii)(D)	Password Management	Customer	ComplyOps Monitoring
164.308(a)(6)(i)	**Security Incident Procedures**	Customer	ComplyOps - Incident Response Policy
164.308(a)(6)(ii)	Response and Reporting	Customer	ComplyOps - Incident Response Policy
164.308(a)(7)(i)	**Contingency Plan**	Customer	ComplyOps - Disaster Recovery Policy
164.308(a)(7)(ii)(A)	Data Backup Plan	Customer	ComplyOps - Disaster Recovery Policy
164.308(a)(7)(ii)(B)	Disaster Recovery Plan	Customer	ComplyOps - Disaster Recovery Policy
164.308(a)(7)(ii)(C)	Emergency Mode Operation Plan	Customer	ComplyOps - Disaster Recovery Policy
164.308(a)(7)(ii)(D)	Testing and Revision Procedures	Customer	ComplyOps - Disaster Recovery Policy
164.308(a)(7)(ii)(E)	Applications and Data Criticality Analysis	Customer	ComplyOps - Disaster Recovery Policy
164.308(a)(8)	**Evaluation**	Customer	Customer
164.308(b)(1)	**Business Associate Contracts and Other Arrangements**	AWS	AWS
164.308(b)(4)	Written Contract	AWS	AWS

HIPAA Standard	HIPAA Compliance Standard	Responsibility	With ComplyOps
PHYSICAL SAFEGUARDS			
164.310(a)(1)	**Facility Access Controls**	AWS	AWS
164.310(a)(2)(i)	Contingency Operations	AWS	AWS
164.310(a)(2)(ii)	Facility Security Plan	AWS	AWS
164.310(a)(2)(iii)	Access Control Validation Procedures	AWS	AWS
164.310(a)(2)(iv)	Maintenance Records	AWS	AWS
164.310(b)	**Workstation Use**	Customer	ComplyOps - Disposable Media Policy
164.310(c)	**Workstation Security**	Customer	ComplyOps - Disposable Media Policy
164.310(d)(1)	**Device and Media Controls**	AWS	AWS
164.310(d)(2)(i)	Disposal	AWS	AWS
164.310(d)(2)(ii)	Media Re-use	AWS	AWS
164.310(d)(2)(iii)	Accountability	AWS	AWS
164.310(d)(2)(iv)	Data Backup and Storage	AWS	AWS
TECHNICAL SAFEGUARDS			
164.312(a)(1)	**Access Control**	Customer	ComplyOps - System Access Policy
164.312(a)(2)(i)	Unique User Identification	Customer	ComplyOps - System Access Policy
164.312(a)(2)(ii)	Emergency Access Procedure	Customer	ComplyOps - System Access Policy
164.312(a)(2)(iii)	Automatic Logoff	Customer	ComplyOps - System Access Policy
164.312(a)(2)(iv)	Encryption and Decryption	Customer	ComplyOps - System Access Policy
164.312(b)	**Audit Controls**	Customer	ComplyOps Monitoring
164.312(c)(1)	**Integrity**	Customer	ComplyOps Monitoring
164.312(c)(2)	Mechanism to Authenticate ePHI	Customer	ComplyOps Monitoring
164.312(d)	**Person or Entity Authentication**	Customer	ComplyOps - System Access Policy
164.312(e)(1)	**Transmission Security**	Customer	ComplyOps Monitoring
164.312(e)(2)(i)	Integrity Controls	Customer	ComplyOps Monitoring
164.312(e)(2)(ii)	Encryption	Customer	ComplyOps Monitoring
ORGANIZATIONAL REQUIREMENTS			
164.314(a)(1)	**Business Associate Contracts or Other Arrangements**	AWS	AWS + Customer
164.314(a)(2)	Business Associate Contracts	AWS	AWS + Customer
164.314(b)(1)	**Requirements for Group Health Plans**	Customer	ComplyOps - System Access Policy
164.314(b)(2)(i)	Implement Safeguards	Customer	ComplyOps - System Access Policy
164.314(b)(2)(ii)	Ensure Adequate Separation	Customer	ComplyOps - System Access Policy
164.314(b)(2)(iii)	Ensure Agents Safeguard	Customer	ComplyOps - System Access Policy
164.314(b)(2)(iv)	Report Security Incidents	Customer	ComplyOps - Incident Response Policy
164.316(a)	**Policies and Procedures**	Customer	ComplyOps - Policy Mgmt Policy
164.316(b)(1)	Documentation	Customer	ComplyOps - Policy Mgmt Policy
164.316(b)(2)(i)	Time Limit	Customer	ComplyOps - Policy Mgmt Policy
164.316(b)(2)(ii)	Availability	Customer	ComplyOps - Policy Mgmt Policy
164.316(b)(2)(iii)	Updates	Customer	ComplyOps - Policy Mgmt Policy

Simplify Cloud Compliance

Dash ComplyOps makes it easy for organizations to address all administrative and technical safeguards required under the shared responsibility model. Organizations can use ComplyOps to build administrative policies for the organization and implement technical security controls. Dash continuous compliance monitoring scans your organization's AWS cloud environment for security and compliance issues and enables your team to quickly fix cloud security issues maintain compliance in AWS. Learn how your team can streamline your cloud security program with Dash.