Compliant Research Data Architecture and Data Sharing

San Francisco | May 29th, 2024

Tim Jones

Senior Solutions Architect
State and Local Government
AWS

Agenda

- Why now?
- Research presents a unique challenge
- Why AWS?
- How AWS delivers
- AWS and data

Why now?

Why now?

Securing research data has never been more important.

Hacker Groups

Criminal gangs

Ransomware

IP theft

Nation states

Internal threats

Why now?

Securing research data has never been more important.
Research data has value and is an active target.

Hacker groups

Criminal gangs

Ransomware

IP theft

Nation states

Internal threats

Why now?

Securing research data has never been more important.
Research data has value and is an active target.

Ransom costs | **Remediation costs** | **Forensic costs**

Hacker groups

Criminal gangs

Ransomware

IP theft

Nation states

Internal threats

Reputational damage

Why now?

Responsible stewardship of research data is expected.

HIPAA
GDPR
CCPA

Data privacy

Responsible use

NIST / CUI
DFARS
CMMC

Why now?

Responsible stewardship of research data is expected.
Compliance defines specific responsibilities for research data.

HIPAA
GDPR
CCPA

Data privacy

Responsible use

NIST / CUI
DFARS
CMMC

Why now?

Responsible stewardship of research data is expected.
Compliance defines specific responsibilities for research data.

Penalties and fines
data breach

Funding withheld
non-compliance/data exfiltration

HIPAA
GDPR
CCPA

NIST / CUI
DFARS
CMMC

Data privacy

Responsible use

Reputational damage

Why now? – DoD compliance requirements

US Department of Defense

Defense Federal Acquisition Regulation Supplement (DFARS) 252.204

- Cybersecurity Maturity Model Certification (CMMC)
  - Appearing in DoD contracts/grants: 2021-2025
  - Third-party assessed and certified solution to CMMC level 1-5
- NIST 800-171 Self Assessment Requirement
  - Basic Self Assessments must be reported to the Supplier Performance Risk System (SPRS) every three years
  - Random audits by Defense Industrial Base Cybersecurity Assessment Center (DIBCAC)
- Non-compliance with DFARS rules will block funding from the Department of Defense

Research is a Unique challenge

Research presents a unique challenge

Research is challenging to secure and make compliant because it often operates within and between islands across campus.

Factors:

- Faculty/researcher procured and managed equipment

- Faculty/researcher/student population
  - Collaborative, distributed, mobile, and transient
  - Bring your own device (BYOD)

Research presents a unique challenge

On-prem campus solutions for secure and compliant research have limits.

Factors:

- Based on point-in-time technology and are either overly generic or tailored to an initial research project's needs.
- Adapting to evolving research and compliance requirements is complex and expensive.
- Researchers often resist using a solution that doesn't meet their specific needs.

Why AWS?

Why AWS?

Elevates your institution's research capabilities along with its security and compliance posture

Inherit global security and compliance controls

Scale with superior visibility and control

Highest standards for privacy and data security

Automate and reduce risk with deeply integrated services

Largest community of security partners and solutions

Why AWS?

Leverages a security and identity foundation with the highest standards for privacy and data security and built for the most security-sensitive organizations

Meet data residency requirements
Choose an AWS Region and AWS will not replicate it elsewhere unless you choose to do so

Encryption at scale with keys managed by our AWS KMS or managing your own encryption keys with CloudHSM using FIPS 140-2 Level 3 validated HSMs

Comply with local data privacy laws by controlling who can access content, its lifecycle, and disposal

Access services and tools that enable you to to build compliant infrastructure on top of AWS

How?

The architectural best practices portfolio

ACCELERATE CLOUD ADOPTION WITH CONFIDENCE

EXPERTISE

AWS well-architected

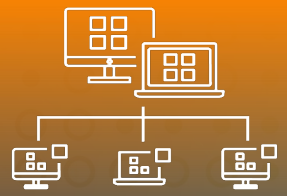
Improve operational excellence, security, reliability, performance efficiency, cost optimization, and sustainability

Sustainable architecture

Enhance sustainability in the cloud via energy reduction and workload efficiency

AWS solutions

Deploy turnkey solutions or kick-start the building process with preconfigured architecture patterns



Architecture center

Access a robust content library, including reference architecture diagrams, best practices, and more

AWS SERVICES

You need a landing zone

- A secure, scalable, multi-account AWS environment based on AWS best practices
- A starting point for net new development and experimentation
- A starting point for migrating applications
- An environment that allows for iteration and extension over time

Landing zone elements

Secure and compliant

Meets the organization's security and auditing requirements

Scalable and resilient

Ready to support highly available and scalable workloads

Adaptable and flexible

Configurable to support evolving mission requirements

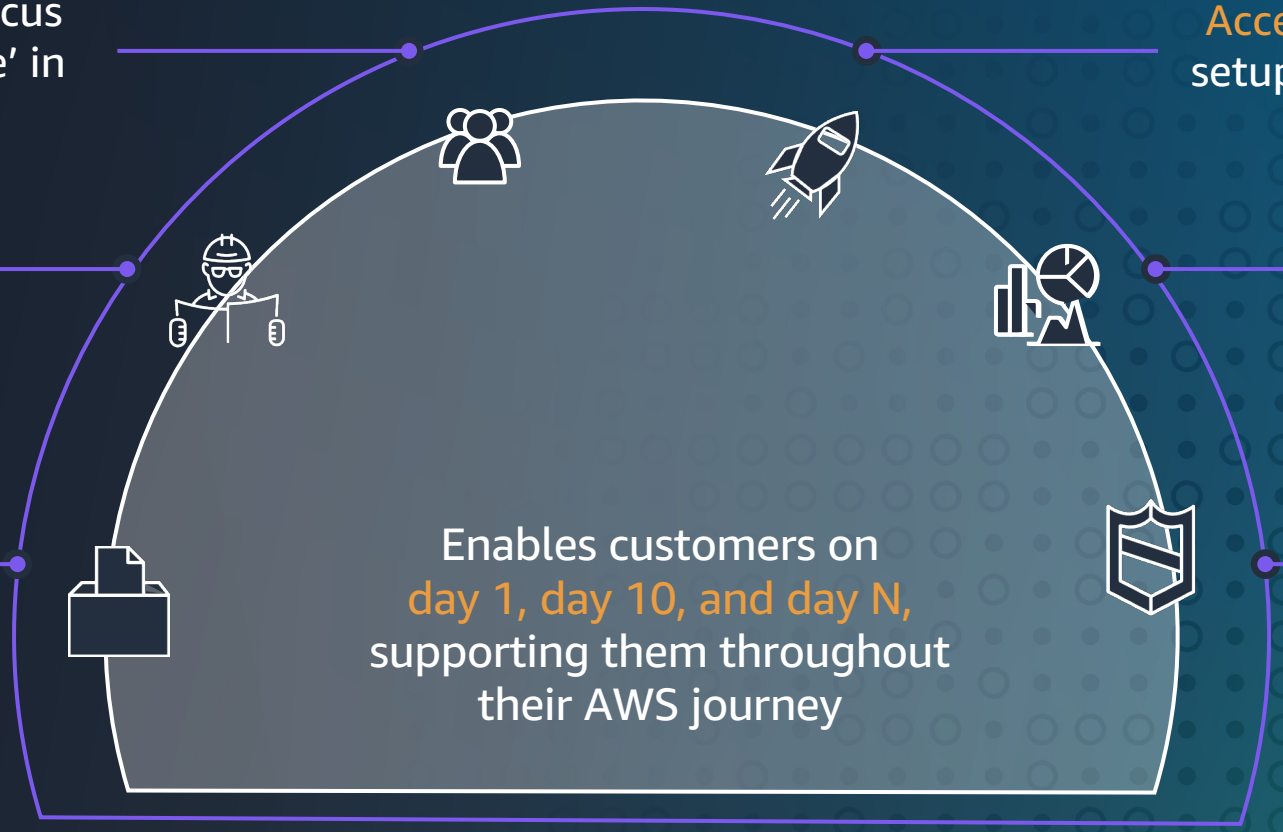
The **Landing Zone Accelerator on AWS** is an open-source software solution that accelerates the implementation of a customer's technical security controls and infrastructure foundation on AWS

Landing Zone Accelerator benefits

Customer resources focus on learning to ‘operate’ in the cloud

Leverages AWS expertise

Flexibility to integrate with other management tools



Accelerate environment setups in days, not weeks

Innovate through open source model

Establish a compliant and improved security posture

How AWS delivers

Example: secure and compliant landing zone

UCSD Health Secure Research Cloud (HSRC) for HIPAA compliance

Drivers

- Prevent removal of research data assets and inappropriate third-party data transfers.
  (IRB vs. policy and legal compliance)
- Prevent proliferation of unmanaged cloud accounts.
  (and gain visibility to monitor activity, data types, workloads, and potential risks)
- Prevent ransomware and research data on mobile devices as a breach source
  (unmanaged, unprotected, or misconfigured devices)

Partnered with AWS, UCSD Health IS security, institutes, and research groups early

- Compliance is more than technical controls: BAA, governance, and policy

How AWS delivers

Example: secure and compliant landing zone

UCSD Health Secure Research Cloud (HSRC) for HIPAA compliance

Solution goals

1. Access controls – technical policies and procedures allowing only authorized persons to access electronic protected health information (ePHI)
2. Audit controls – hardware, software, and/or procedural mechanisms to record and examine access and other activity
3. Integrity controls – policies, procedures, and measures to ensure and confirm ePHI is not improperly altered or destroyed
4. Transmission security – technical security measures guarding against unauthorized access to ePHI transmitted over a network

How AWS delivers

Example: deployment of a research workload

UCSD Health Virtual Research Desktop (VRD) – within UCSD HSRC (saw earlier)

Researcher enablement

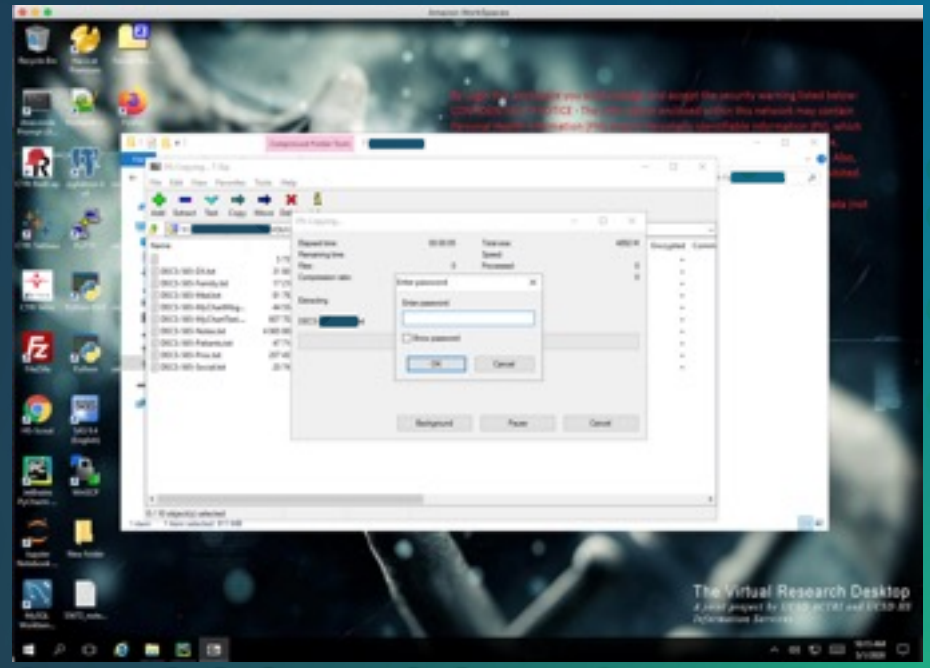
- A solution that balances security and privacy while still providing a quality user experience
- Access to ePHI via UCSD Data Extraction Concierge Service (DECS) and VRDs
  (data extracted from clinical data warehouse by DECS and placed into investigator's VRD "secure" folder)
- Hardened Amazon WorkSpaces Windows 10 virtual machines
  - Runs within UCSD HSRC and approved by UCSD Health CISO for ePHI
  - Provisioned with: SPSS, R/RStudio, Python/PyCharm, Java 8, and others
  - With approval, access to internal databases

How AWS delivers

Example: deployment of a research workload

UCSD Health Virtual Research Desktop (VRD) – within UCSD HSRC (saw earlier)

View of remote desktop from investigator's computer



VRD desktop with application running

How AWS delivers

Outcomes

UCSD HSRC and VRD

- A flexible environment that supports security, compliance, and researcher workflow
- Structured, limited, and controlled access to ePHI data for research using defined process
- Automated security controls and configuration monitoring limits configuration drift
- Consistent logging makes audits and re-assessments less challenging
- Ability to flexibly add additional research tools and data environments as needed
- Security, compliance, and administrative support (early involvement key)
- Faculty and researcher project/environment support (early involvement key)

What about data

AWS Clean Rooms helps organizations collaborate on datasets without sharing underlying data

Multi-party collaborations

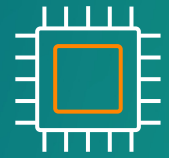
Collaborate with up to five parties in a single collaboration; extract insights from multiple companies

No AWS data movement

Use Amazon S3 data with direct permissioning and no AWS data movement

Query controls and enforcement

Configure analysis rules to restrict the type of analysis allowed on your data



Cryptographic computing

Pre-encrypt data so that it is encrypted at all times, including during query execution

Programmatic access

Automate and integrate functionality into existing workflows and products; create white-labeled clean room offering

Amazon DataZone

Unlock the power of all data for all users WITH TRUSTED AUTONOMY

Data producers

Teams who want to share data

Amazon DataZone

Team who runs the data marketplace

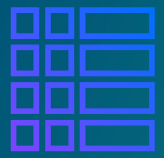
Data consumers

Teams who want to use data

Amazon DataZone

Unlock data across organizational boundaries with built-in governance

Manage **organization-wide governance** in one place



Catalog your data with business context

Simplify access to analytics for everyone in your organization

Solve specific business use cases through **data projects**

Q & A

Thank you!

Tim Jones
awstijon@amazon.com

Track: Data and Analytics
Session: Compliant research data architecture & data sharing management

Learning Day Content

https://sanfrancisco2024.awslearningday.com/

Baylor College of Medicine's human genome sequencing center uses AWS to innovate

Challenge

One of the projects Baylor HGSC is involved with is the Cohorts for Heart and Aging Research in Genomic Epidemiology project (CHARGE). Baylor needed a cost-efficient, easily maintainable solution that would enable it to provide safe, effective worldwide collaboration without delays caused by setting up a physical infrastructure. The solution also needed to meet clinical standards and HIPAA requirements.

Solution

Baylor decided to partner with DNAnexus, which provides an API-based PaaS that enables clinical and research enterprises to efficiently and securely move their analysis pipelines and data into AWS.

Benefits

- Completed its first analysis in 10 days—five times faster than with the local infrastructure—and was able to share the findings quickly.
- The scalability of AWS helps CHARGE scientists gain more predictive power over the conditions they are studying

BCM
Baylor College of Medicine

"There are all kinds of limitations in our ability to find the horizons of science. But now, thanks to AWS and DNAnexus, we can focus on the science instead of the infrastructure."

CHOP Accelerates Pediatric Research using AWS-Powered Data Resource

Challenge

As medical researchers generate more and more clinical data, they're faced with the challenge of storing and organizing that data so that researchers can access, study, and cross-reference it to facilitate medical breakthroughs.

Benefits

CHOP provided the research community with access to genomic and associated clinical data and increased KFDRC's collaborative potential.

CHOP stored 26 billion occurrences of 215 million unique genomic variants from 5,000 participants, while meeting the FHIR industry standard.

Solution

CHOP built the Gabriella Miller Kids First Data Resource Center (KFDRC), a data source that brings genomics, clinical and imaging data as an open resource for researchers to focus on discovers in pediatric cancer and structural birth defects.

Children's Hospital of Philadelphia

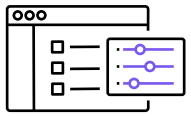
All of our system is currently built on AWS. . . . We went from zero to managing a few petabytes of genomic data within a year using this setup."

Allison Heath
Director of Data Technology and Innovation, Center for Data-Driven Discovery in Biomedicine

AWS offers customers tools and guidance to enable compliance

Terms & Conditions

Transparency



Agreements and third-party audit reports to support services and compliance objectives

Compliance, security tools & services

Industry frameworks and assets

Services and assets to automate controls, collect evidence and manage audits demands

Deep industry expertise

Regulatory engagement

Mechanisms to advocate for and share best practices with customers

Customers rely on AWS's compliance with global standards

Certifications & attestations

- Cloud Computing Compliance Controls Catalogue (C5)
- Cyber Essentials Plus
- DoD SRG
- FedRAMP
- FIPS
- IRAP
- ISO 9001
- ISO 27001
- ISO 27017
- ISO 27018
- MLPS Level 3
- MTCS
- PCI DSS Level 1
- SEC Rule 17-a-4(f)
- SOC 1, SOC 2, SOC 3

Laws, regulations and privacy

- CISPE
- GDPR
- FERPA
- GLBA
- HIPAA
- HITECH
- IRS 1075
- ITAR
- My Number Act
- Data Protection Act – 1988
- VPAT / Section 508
- Data Protection Directive
- Privacy Act [Australia]
- Privacy Act [New Zealand]
- PDPA - 2010 [Malaysia]
- PDPA - 2012 [Singapore]
- PIPEDA [Canada]
- Agencia Española de Protección de Datos

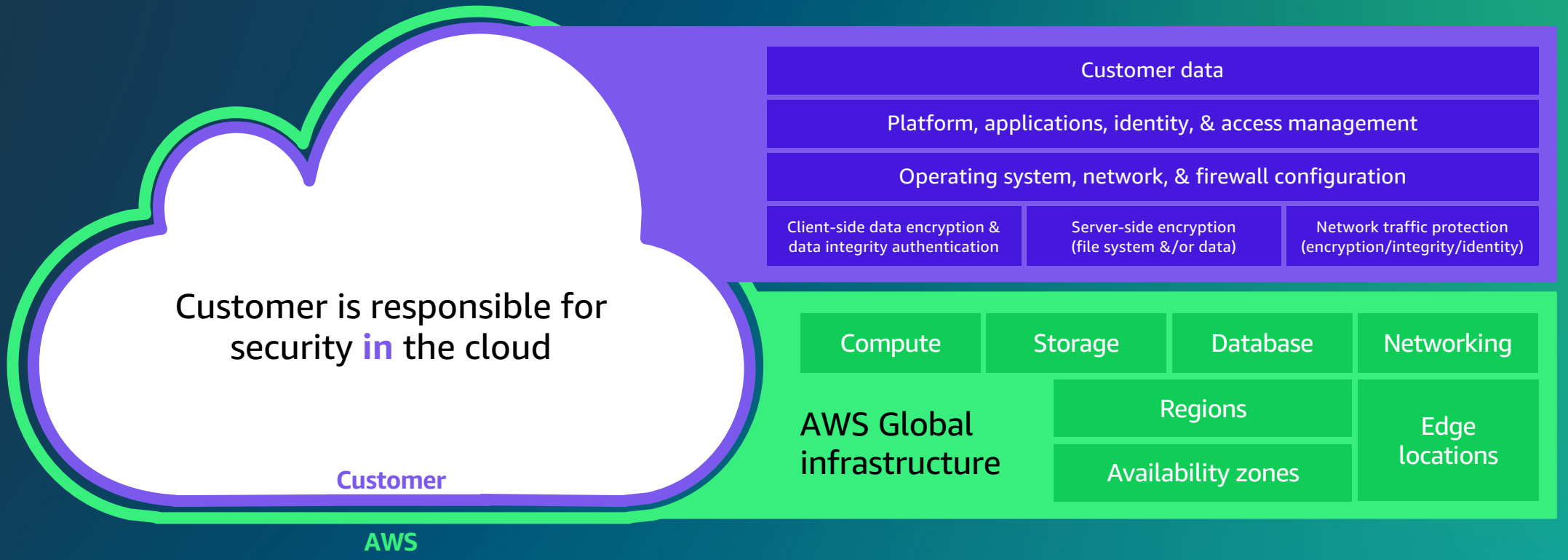
Alignments & frameworks

- CIS (Center for Internet Security)
- CJIS (US FBI)
- CSA (Cloud Security Alliance)
- Esquema Nacional de Seguridad
- EU-US Privacy Shield
- FISC
- FISMA
- G-Cloud
- GxP (US FDA CFR 21 Part 11)
- ICREA
- IT Grundschutz
- MITA 3.0 (US Medicaid)
- MPAA
- NIST
- Uptime Institute Tiers
- Cloud Security Principles
- BioPhorum IT Controls

= industry or global standard

https://aws.amazon.com/compliance/programs/

Shared responsibility



AWS is responsible for security **of** the cloud

Data privacy is our top priority at AWS

Storage: you choose the AWS region(s) in which your content is stored and the type of storage you use

Security: you choose how your content is secured

Access: AWS does not access or use customer content except as necessary to provide the service offerings, or to comply with the law or a binding order of a government body

Disclosure of customer content: we will not disclose customer content unless we're required to do so to comply with the law or a binding order of a government body

Security assurance: AWS security protections and control processes are independently validated by multiple third-party independent assessments

For more information, visit our Data Privacy Center on our website: **https://aws.amazon.com/compliance/data-privacy/**

Example obligations of the BAA & shared responsibility

AWS obligations

- Limit on use and disclosures
- Physical controls
- Reporting or impermissible uses
- Reporting of security incidents
- Reporting of breaches
- Subcontractors
- Account of disclosures
- Internal records

Your obligations

- Identification of the HIPAA account
- Appropriate use of the HIPAA account
- Use HIPAA eligible services to host and process PHI
- Appropriate configuration of services
  - Encryption
  - Logging
  - Necessary consents
  - Disclosure restrictions

HIPAA in the Cloud

AWS, HIPAA and HITRUST

The **HITRUST CSF** serves to unify **security controls** based on aspects of US federal law (such as **HIPAA and HITECH),** state law (such as Massachusetts's Standards for the Protection of Personal Information of Residents of the Commonwealth) and recognized non-governmental compliance standards (such as PCI DSS) into a single framework that is tailored for **healthcare needs**

Disclaimer: AWS customers should consult their legal advisors to understand how HIPAA, or related laws, apply to them.

HIPAA eligible ≠ HIPAA compliant

Customers may use any AWS service in an account designated as a HIPAA account, but they should only process, store, and transmit protected health information (PHI) in the HIPAA-eligible services

Eligible services
https://aws.amazon.com/compliance/hipaa-eligible-services-reference/

HIPAA Eligible services are not automatically compliant. They must follow the appropriate guidance

Guidance
https://docs.aws.amazon.com/whitepapers/latest/architecting-hipaa-security-and-compliance-on-aws/welcome.html

Customer applications & compliance

Customer Applications

Your own accreditation

Your own certifications

Your own external audits

AWS Services

Applications built on top of AWS services, **are not implicitly compliant** to security controls (that AWS services are complaint with).

Customers need to **certify applications separately** by engaging with external auditors.

Research for health on AWS