Whitepaper on HIPAA compliance in the AWS cloud

Introduction

What is HIPAA?

The Health Insurance Portability and Accountability Act (HIPAA) was introduced in 1996. Title II of the regulation, known as the Administrative Simplification (AS) provisions, consists of the Privacy Rule and the Security Rule. Within the HIPAA Privacy Rule, national standards were established to protect individuals' medical records and other personal health information.

The Security Rule requires appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of electronic protected health information (ePHI). The HIPAA rules apply to covered entities such as health plans, health care clearinghouses, health care providers that conduct certain health care transactions electronically, and business associates of covered entities.

Why HIPAA matters

HIPAA was designed to protect patient data and a growing number of health care data breaches have led to increased HIPAA enforcement over the years. The Office of Civil Rights (OCR) has been responsible for enforcing the HIPAA rules. Since the April 2003 compliance deadline, OCR has received more than 177,854 complaints and has initiated more than 884 compliance reviews.

Health Information Technology for Economic and Clinical Health Act (HITECH)

HITECH was enacted in 2009 to promote the adoption and meaningful use of health information technology and to reinforce HIPAA rules. HITECH established breach notification requirements to provide greater transparency for individuals whose information may be at risk.

OCR's audit program

HITECH requires OCR to conduct periodic audits of covered entity and business associate compliance with the HIPAA rules. In 2011 and 2012, in order to assess compliance with HIPAA's requirements, OCR implemented a pilot audit program to examine the controls and processes implemented by 115 covered entities.

OCR also conducted an extensive evaluation of the effectiveness of the pilot program. Drawing on that experience and the results of the evaluation, OCR implemented phase two of its audit program in 2016 under which both covered entities and business associates can be audited. The assessment can include or extend to hosted environments.

Table of Contents

1. Considerations for cloud customers

1.1. Covered entities and business associates under HIPAA

Under HIPAA, a covered entity is a health care provider, a health plan, or a health care clearinghouse. A business associate is a person or entity who performs or assists in performing an activity regulated by the associated HIPAA rules, for or on behalf of the covered entity.
If a covered entity or business associate engages a cloud service provider (CSP) such as Amazon Web Service (AWS) to store or process ePHI, the CSP itself is a business associate under HIPAA. It is important for customers moving to a public cloud environment to understand this distinction, because a business associate agreement (BAA) should then be enacted to define both privacy and security responsibilities of the covered entity and the business associate.

1.2. Business associate agreements

HIPAA requires a BAA between the covered entity and a business associate such as AWS. These agreements serve to define and limit the permissible uses and disclosures of ePHI, as appropriate. Examples of functions a business associate might provide include claims processing, billing, benefits management, member care, and provider data analysis.
If a customer (covered entity or business associate) plans to use protected health information (as defined by HIPAA) within AWS services, the customer should first accept the AWS business associate addendum (AWS BAA). AWS services can be used with health care applications, but only services covered by the AWS BAA can be used to store, process, or transmit ePHI. Customers can review, accept, and check the status of their AWS BAA through a self-service portal available in AWS Artifact.

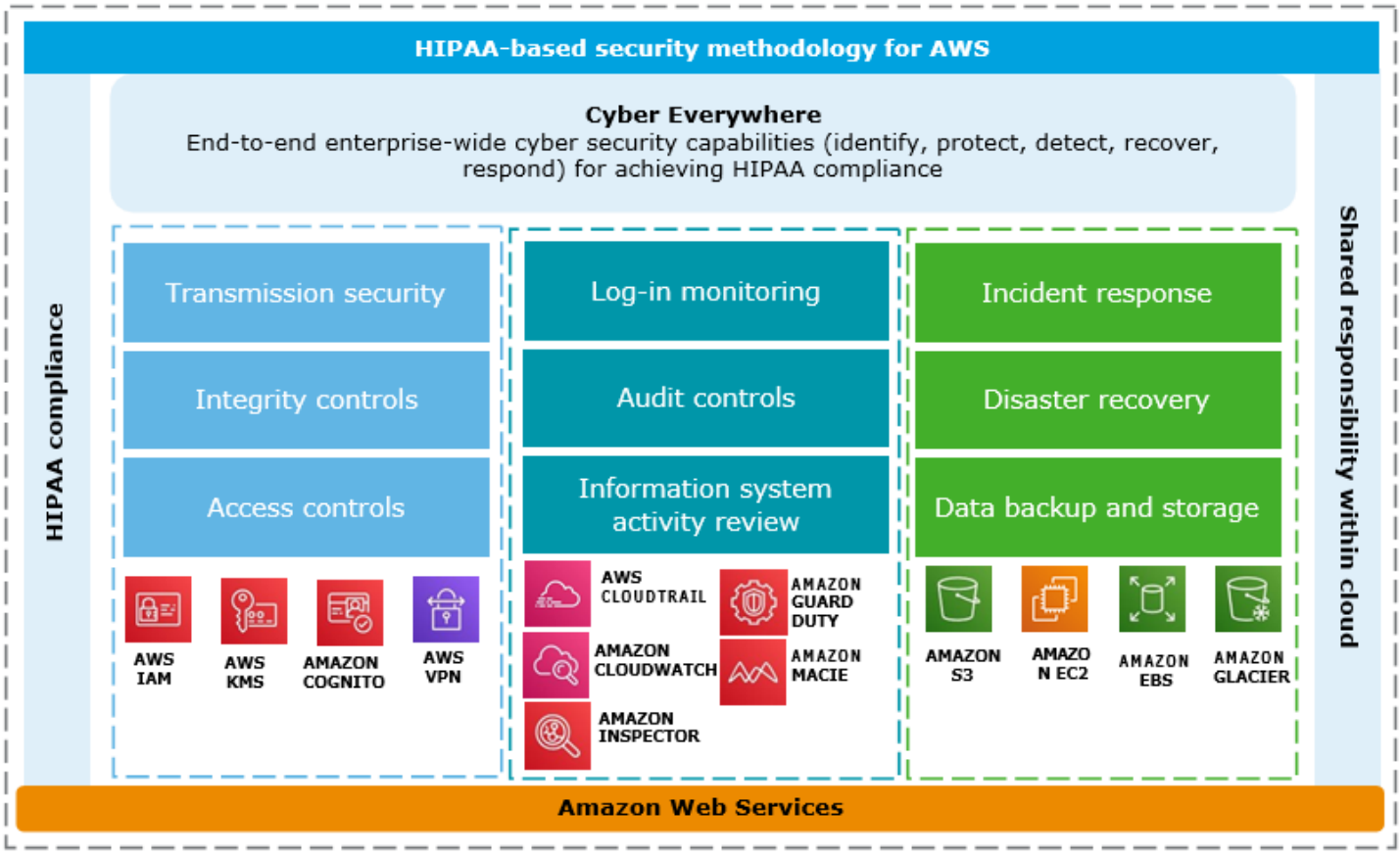
Shared responsibility within the cloud
The AWS Shared Responsibility Model can be extended to the HIPAA control areas to assist with defining responsibilities.

Illustrative scenario: Health care provider hosts customer portal on AWS

In this scenario, a health care provider and AWS are jointly responsible for meeting HIPAA security requirements.

Illustrative HIPAA control area	AWS responsibility	Health care provider responsibility
Access controls	Provide identity and access management capabilities for AWS services.	Implement policies and procedures for identity and access management that are consistent with the AWS BAA and HIPAA.
Audit controls	Enable logging and monitor capabilities for AWS services and ability to capture and log API actions against the AWS environment.	Employ auditing procedures that allow security analysts to periodically examine detailed activity logs or reports.
Incident response and disaster recovery	Provide and maintain disaster recovery capabilities for rapid recovery of IT infrastructure and data ensuring adequate durability and availability of services.	Develop a resilient architecture capable of responding to, and recovering from, incidents.

2. Architecting for HIPAA on AWS



2.1. Establishing HIPAA compliant controls to secure data and systems

Effective controls across an organization's security infrastructure are imperative for creating a well- architected end-to-end security posture. The goal for architects and developers is to create an infrastructure capable of withstanding potential cyber-attacks.
Once again, controls should align with safeguards documented within the HIPAA Security Rule.

2.2. Assessing cybersecurity risk in the handling and storage of ePHI data

Understanding your responsibilities within HIPAA is important to securing ePHI within the AWS cloud, and a critical first step is the identification and assessment of cybersecurity risk. There are several sources of guidance available to assist entities in this effort:

- Validating authenticated and authorized access to ePHI
- Checking ePHI transmission
- Maintaining integrity of systems and ePHI
- Validating secure transmission and storage of ePHI

The National Institute of Standards and Technology (NIST) has also developed special publications that provide guidance on HIPAA compliance, including NIST Special Publication 800- 66: An Introductory Resource Guide for Implementing the HIPAA Security Rule.

2.3. Secure transmission and storage of ePHI through integrity controls and encryption

The HIPAA Security Rule includes addressable implementation specifications for the encryption of ePHI in transit, in use, and at rest. AWS offers a wide set of features and services to make encryption of ePHI manageable and easier to audit, including the AWS Key Management Service **(AWS KMS).**
Customers can also take advantage of the encryption features native to HIPAA-eligible services such as AWS Simple Storage Service **(S3)**. In addition to encryption at-rest, customers can enable encryption in- transit using TLS (encryption protocol) certificates, and they can leverage *AWS Certificate Manager* **(ACM)** for certificate management.

Organizations can enforce network security and segmentation using AWS services such as Amazon Virtual Private Cloud **(VPC)**. These services allow for segmentation of the network and data flows from non-ePHI-related compute and storage services. For developers, **Amazon API Gateway** is a HIPAA-eligible service that makes it easy to create, publish, maintain, monitor, and secure application programming interfaces (APIs) at scale. The APIs created with Amazon API Gateway expose HTTPS endpoints only, thereby providing encryption in-transit. Amazon API Gateway does not support unencrypted (HTTP) endpoints.

2.4. IAM, MFA, password management, and access authorization controls

AWS Identity and access management (IAM) involves the strategies and methods used to authenticate and authorize actions that specific users can perform.

AWS IAM is a critical component of HIPAA security. Within an AWS environment, access management strategies and associated technical controls are needed at the AWS infrastructure layer, the operating system layer, and the application layer. The HIPAA Security Rule documents addressable requirements for implementing authentication and authorization mechanisms to protect ePHI from being altered or destroyed in an unauthorized manner.

HIPAA contains requirements for covered entities to include procedures for creating, changing, and safeguarding passwords. AWS customers can manage passwords for account root users and for IAM users in their account.

Customers can set a password policy on their AWS account to specify complexity requirements and mandatory rotation periods for their IAM users' passwords to prevent password re-use.

Under HIPAA, covered entities should implement policies and procedures before granting access to PHI. Authorization in AWS is accomplished by permissions that are dictated by policies and then applying these to users via role mapping or group membership. A strategy for creating policies and assigning them to users is required to grant administrators the rights they need to perform their job functions while upholding a least-privilege approach. Users are mapped to roles and then they assume the role in AWS.

2.5. Recognizing resiliency as an important feature of HIPAA

Under HIPAA, covered entities must meet the Emergency Access Procedure requirement, which includes the need for availability in any HIPAA-compliant environment. To meet this requirement, covered entities must enable administrative controls, such as a data backup and disaster recovery plan.

This contingency plan for protecting data in the event of a disaster should focus on the creation and maintenance of retrievable exact copies of ePHI. This involves maintaining highly available systems, keeping both the data and system replicated offsite, and enabling continuous access to both. In addition, implementing and testing identity and access management controls must be accounted for within the contingency plan. Secure authorization and authentication must be enabled, even during times where emergency access to ePHI is needed.

AWS provides tools and resources that customers can use to build scalable backup and recovery solutions. To implement a data backup plan on AWS, Amazon's Elastic Block Store **(EBS)** offers persistent storage for Amazon EC2 virtual server instances.

These volumes can be exposed as standard block devices and offer off-instance storage that persists independently from the life of an instance.
To align with HIPAA guidelines, customers can create **point-in-time snapshots** of Amazon EBS volumes that are automatically stored in Amazon S3 and are replicated across multiple Availability Zones--distinct locations engineered to be isolated from failures in other Availability Zones. These snapshots can be accessed easily and can protect data for long-term durability.

Amazon S3 also provides a highly available solution for data storage and automated backups. By simply loading a file or image into Amazon S3, multiple redundant copies are automatically created and stored in separate data centers. These files can be accessed easily (based on permissions), can be versioned, and are stored until deleted.

AWS has many **options for databases**. Customers can run their own database on Amazon **EC2**, use one of the managed service database options provided by the Amazon Relational Database Service **(RDS)**, or leverage any of AWS's managed non-relational databases, such as **DynamoDB**, **ElasticSearch**, or **Redis**. Amazon RDS creates a storage volume snapshot of a customer's database instance, backing up the database instance, not just individual databases.

2.6. Auditing and monitoring

Auditing and monitoring controls are essential to meeting the requirements of the HIPAA Security Rule. Auditing controls are technical safeguards that should be addressed through technical controls by anyone who wishes to store, process, or transmit ePHI.

Monitoring controls include procedures for monitoring log-ins and reporting discrepancies. A combination of services such as **AWS Config, AWS CloudTrail, AWS Security Hub, Amazon GuardDuty, and Amazon CloudWatch** create a cost-effective solution for auditing and monitoring resources in the AWS environment. AWS Config provides an assessment and audit of configurations of various AWS resources, while AWS CloudTrail captures API calls/console login made to an account.

CloudTrail logs can also be directly ported to an Amazon S3 bucket for further analysis by a third-party security incident and event management (SIEM) solution.

2.7. Continuous monitor to avoid HIPAA data breaches

AWS customers can collect logs from various sources and centrally store them in an S3 bucket, allowing for easy ingestion of logs into SIEM tools. SIEM capabilities such as alerting, interpreting, and parsing data can be leveraged through an established third-party vendor, **Splunk**, or they can be leveraged across several AWS services. **Amazon Athena**, allows for analytical queries that parse data, while Amazon CloudWatch Event provides alerts for certain actions within the AWS environment.

Amazon Macie uses machine learning to discover and classify unstructured, business-critical data, as well as analyze access patterns and user behavior within S3 buckets. While SIEM might alert customers about malicious activity anywhere in their accounts, because Macie can understand and classify data at-rest, it can determine which data is business critical and focus its alerts in these areas.

2.8. Monitor identity log-in attempts

The HIPAA Security Rule requires covered entities to implement procedures to monitor log-in attempts and report discrepancies. Customers who have enabled **CloudTrail** can see log entries associated with sign-in events, including the internet protocol (IP) address of the entity signing in and whether MFA was enforced for that sign-in. In addition to logging these events, CloudTrail captures successful sign-ins by users in IAM and root.

2.9. Analyze risks by identifying and remediating vulnerabilities

Under HIPAA, covered entities are required to conduct assessments of potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by them and by their business associates.
Amazon Inspector is a HIPAA-eligible automated security assessment service designed to help improve the security and compliance of applications deployed on Amazon EC2. Organizations can use Amazon Inspector to automatically evaluate applications for vulnerabilities or deviations from leading practices. After performing an assessment, Amazon Inspector produces a detailed list of security findings prioritized by level of severity. These findings can be reviewed directly or as part of detailed assessment reports that are available via the Amazon Inspector console.

2.10. Collect evidence and be audit ready

In designing an information system that is consistent with HIPAA requirements, customers should include auditing capabilities so that security analysts can test detailed activity logs or reports to see who had access, from what IP address, what data was accessed, etc.

Using Amazon EC2, customers can run activity log files and audits to the packet layer on their virtual servers, just as they do on traditional hardware. They can also track IP traffic that reaches their virtual server instance. Administrators can back up the log files into Amazon S3 for long-term, durable storage. AWS CloudTrail can be leveraged to monitor all API calls made and this can demonstrate to be a critical source for audits/forensic investigations.