FERPA Compliance on AWS

Family Educational Rights and Privacy Act of 1974 (FERPA)

May 2015

Notices

This document is provided for informational purposes only. It represents AWS's current product offerings and practices as of the date of issue of this document, which are subject to change without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of AWS's products or services, each of which is provided "as is" without warranty of any kind, whether express or implied. This document does not create any warranties, representations, contractual commitments, conditions or assurances from AWS, its affiliates, suppliers or licensors. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

Contents

Abstract 3
Introduction 4
AWS Regions, Availability Zones, and Endpoints 6
AWS Management Environment 7
AWS Shared Responsibility Model 8
Infrastructure Services 8
Container Services 9
Abstracted Services 10
Security and Compliance of and in the Cloud 11
Creating a FERPA-Compliant Environment with AWS 13
Conclusion 15
AWS Certifications and Reports 15
Further Reading 17

Abstract

This Family Educational Rights and Privacy Act (FERPA) compliance whitepaper is designed to assist educational agencies and institutions that are considering the use of Amazon Web Services (AWS) for education data. This document introduces the AWS shared responsibility model that is in place to meet data privacy and data security requirements and to ensure proper protection of education data in compliance with FERPA. It does not provide "how-to" configuration guidance.

Introduction

The Family Educational Rights and Privacy Act (FERPA) of 1974 was enacted to support and promote the protection of privacy and reasonable governance of student education records. FERPA provides students:

- The right to inspect and review their education records.
- Governance over disclosure of their education records.
- A mechanism to amend incorrect education records.

The U.S. Department of Education doesn't recommend any specific cloud solution. As noted in Frequently Asked Questions-Cloud Computing on the U.S. Department of Education Privacy Technical Assistance Center website:

> "It is important to keep in mind that FERPA may not be the only statute governing your planned migration to the cloud. In each specific situation, it is necessary to take into consideration any additional applicable federal and individual state data privacy laws that may contain more stringent requirements for data protection than FERPA. PTAC recommends that in evaluating cloud computing alternatives to your current data center solutions you consult with your organization's legal staff to ensure you consider and address all applicable federal, state, and local laws and regulations."

FERPA doesn't prohibit the use of cloud computing solutions for the purpose of hosting education records. However, FERPA does require states to use reasonable methods to ensure the security of their information technology (IT) solution. FERPA defines "education records" as "records, files, documents, and other materials that are maintained by an educational agency or institution, or by a person acting for such agency or institution." Education records also include any record that pertains to an individual's previous attendance as a "student of an

institution." Although the law provides different levels of protection for each type of education record, in general, the rule requires covered institutions and agencies to reasonably safeguard student education records from any intentional or unintentional use or disclosure that is in violation of the requirements for FERPA. The primary intent of FERPA is to protect student identities and the privacy of their student records related to educational information, personally identifiable information (PII), and directory information.

Covered entities subject to FERPA are turning to cloud computing as a highly efficient way to manage and secure vast amounts of education records and student data. Security is a core functional requirement of FERPA, requiring that mission-critical information be protected from accidental or deliberate theft, leakage, integrity compromise, and deletion. AWS offers a complete set of global compute, storage, database, analytics, application and deployment services that enable education entities to deploy applications and services cost-effectively and with flexibility, scalability, and reliability.

Under the AWS shared responsibility model, which is discussed later in this whitepaper, AWS provides a global secure infrastructure and foundational compute, storage, networking, and database services, as well as higher-level services. AWS customers are responsible for protecting the confidentiality, integrity, and availability of their data in the cloud, and for meeting specific compliance and regulatory requirements, such as FERPA for information protection.

AWS does not directly process or access customer content. AWS customers maintain control of their data at all times, and have the ability to edit, or mark their content for deletion. Customer responsibility for protecting the confidentiality, integrity, and availability of their data in the AWS cloud may vary, depending on the type of AWS service.

Some of the AWS services covered in this white paper are Amazon Elastic Compute Cloud (Amazon EC2), Amazon Simple Storage Service (Amazon S3), Amazon Elastic Block Store (Amazon EBS), Elastic Load Balancing, Amazon Elastic MapReduce (Amazon EMR), Amazon Relational Database Service (Amazon RDS), AWS Identity and Access Management (IAM), Amazon Virtual Private Cloud (Amazon VPC), AWS CloudTrail, AWS Config, AWS Key Management Service (KMS), Amazon DynamoDB, and Amazon CloudWatch.

In addition to these core services and security tools, AWS offers several application-level services to support service notifications related to changes in the customer environment, such as Amazon Simple Queue Service (Amazon SQS), Amazon Simple Email Service (Amazon SES), Amazon Glacier, and Amazon Simple Notification Service (Amazon SNS).

AWS Regions, Availability Zones, and Endpoints

AWS has data centers around the world. These data centers are organized into regions and Availability Zones. Each region is a separate geographic area. Each region has multiple, isolated locations known as Availability Zones. To reduce data latency in your applications, most AWS products allow you to select a regional endpoint to make your requests.

Use AWS regions to manage network latency and regulatory compliance. When you store data in a region, it is not replicated outside that region. It is your responsibility to replicate data across regions, if your business needs require that. AWS provides information about the country, and, where applicable, the state where each region resides; you are responsible for selecting the region to store data with your compliance and network latency requirements in mind. Regions are designed for availability and consist of at least two, often more, Availability Zones. Availability Zones are designed for fault isolation. They are connected to multiple Internet Service Providers (ISPs) and different power grids. They are interconnected using high-speed links, so applications can rely on local area network (LAN) connectivity for communication between Availability Zones within the same region. You are responsible for carefully selecting the Availability Zones where your systems will reside. Systems can span multiple Availability Zones. You should design your systems to survive temporary or prolonged failure of an Availability Zone in the event of a disaster.

AWS provides web access to services through the AWS Management Console and through individual service consoles. AWS provides programmatic access to services through application programming interfaces (APLs) and command line interfaces (CLIs). Service endpoints, which are managed by AWS, provide management (backplane) access.

AWS Management Environment

AWS data centers offer:

- State-of-the art electronic surveillance and multi-factor access control systems.
- Around-the-clock staffing by trained security guards, who authorize access on the basis of least privilege.
- Environmental systems that minimize the impact of disruptions to operations.
- Resiliency, through the multiple AWS geographic regions and Availability Zones, during natural disasters or system failures.

Physical and Environmental Security

AWS data centers, although housed in nondescript facilities, are built using innovative architectural and engineering techniques. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff using video surveillance, intrusion detection systems, and other electronic means.

Secure Network Architecture

Network devices, including firewall and other boundary devices, are in place to monitor and control communications at the external boundary of the network and at key internal boundaries within the network. These boundary devices enforce the flow of information between network fabrics through rule sets, access control lists (ACLs), and device configurations.

Secure Access Points

To allow for more comprehensive monitoring of inbound and outbound communications and network traffic, AWS has strategically placed a limited number of access points to the cloud. In addition, AWS has implemented network devices that are dedicated to managing interfacing communications with ISPs. AWS employs a redundant connection to more than one communication service at each Internet-facing edge of the AWS network. These connections each have dedicated network devices.

Network Monitoring and Protection

AWS uses a variety of automated monitoring systems to provide a high level of service performance and availability. AWS monitoring tools are designed to detect unusual or unauthorized activities and conditions at ingress and egress communication points. These tools monitor server and network usage, port scanning activities, application usage, and unauthorized intrusion attempts. The tools can be used to set custom performance metric thresholds for unusual activity.

AWS Shared Responsibility Model

AWS offers a variety of infrastructure and platform services, which fall into three categories: infrastructure, container, and abstracted services. Each category comes with a slightly different shared responsibility model, depending on how you interact with and access the functionality.

Infrastructure Services

This category includes compute services, such as Amazon EC2, and related services, such as Amazon EBS, Auto Scaling, and Amazon VPC.

With these services, you can design and build a cloud infrastructure using technologies similar to and compatible with on-premises solutions. You control the operating system, and you configure and operate any identity management system that provides access to the user layer of the virtualization stack.

Figure 1 shows the building blocks for the shared responsibility model for infrastructure services.

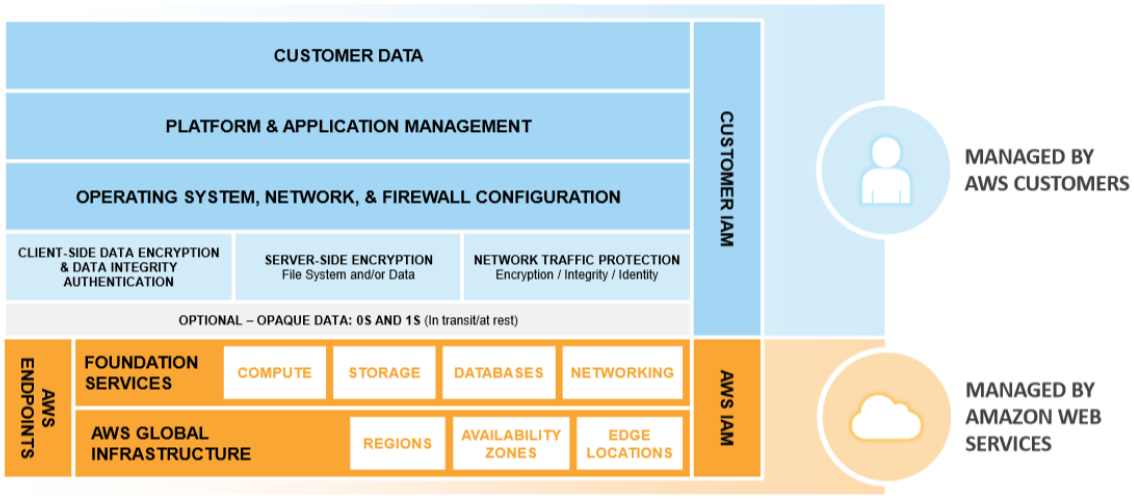

Figure 1: Shared Responsibility Model for Infrastructure Services

Container Services

This category includes container services, such as Amazon RDS, Amazon EMR, and AWS Elastic Beanstalk.

Services in this category typically run on separate Amazon EC2 or other infrastructure instances, but sometimes you don't manage the operating system or the platform layer. AWS provides a managed service for these application containers. You are responsible for setting up and managing network controls, such as firewall rules, and for managing platform-level identity and access management separately from IAM.

Figure 2 shows the shared responsibility model for container services.

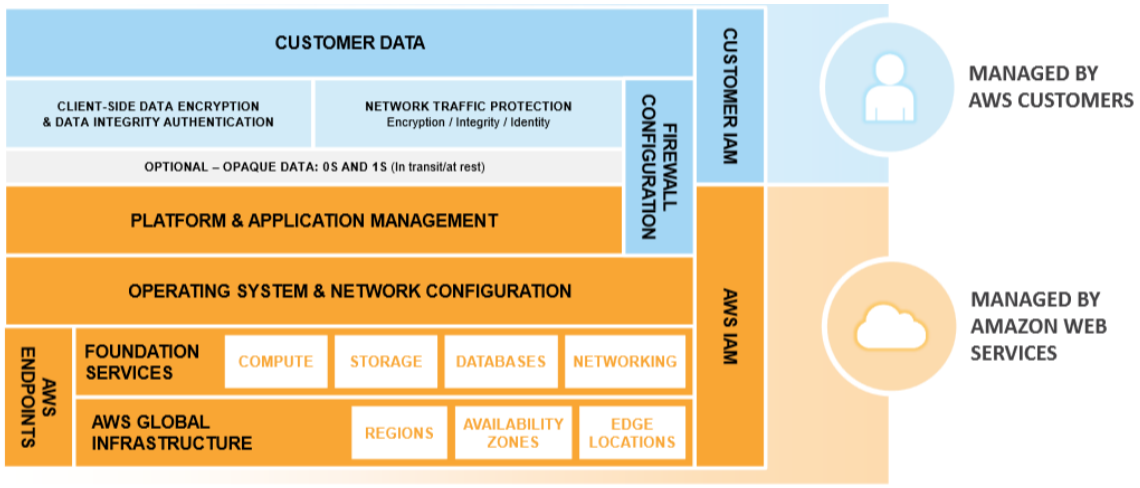

Figure 2: Shared Responsibility Model for Container Services

Abstracted Services

This category includes high-level storage, database, and messaging services, such as Amazon S3, Amazon Glacier, DynamoDB, Amazon SQS, and Amazon SES. These services abstract the platform or management layer on which you can build and operate cloud applications. You access the endpoints of these abstracted services using AWS APIs; AWS manages the underlying service components or the operating system on which they reside. You share the underlying infrastructure, and abstracted services provide a multi-tenant platform, which isolates your data in a secure fashion and provides for powerful integration with IAM.

Figure 3 shows the shared responsibility model for AWS abstracted services.

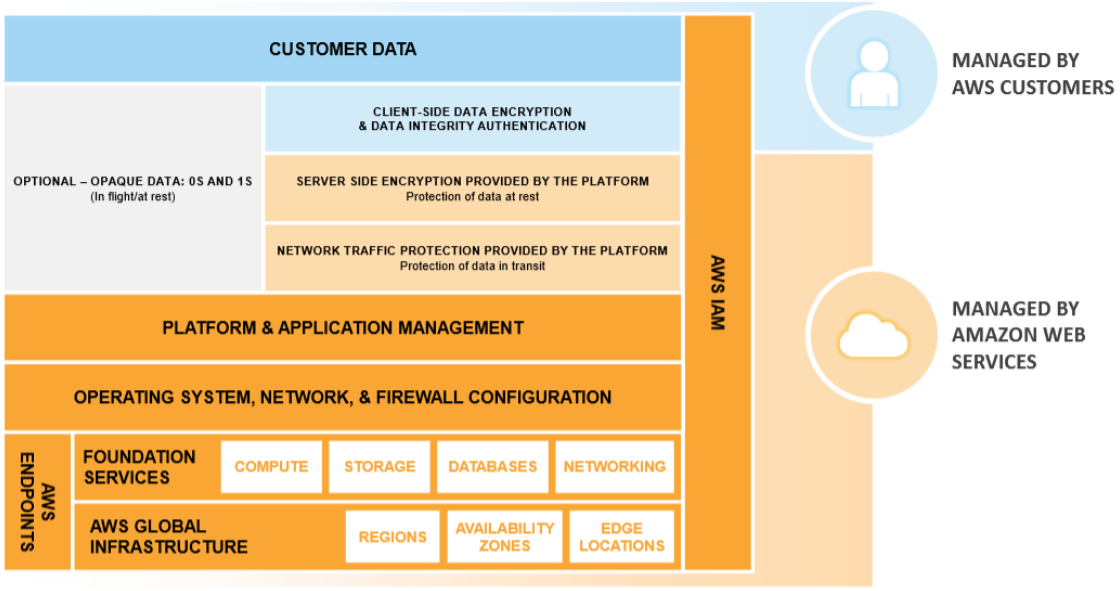

Figure 3: Shared Responsibility Model for Abstracted Services

For more information about the shared responsibility model, see [AWS Security Best Practices](#).

Security and Compliance of and in the Cloud

How does leveraging AWS make security and compliance activities easier? It helps to think of the AWS cloud in two distinct ways: in terms of the compliance of the AWS infrastructure (security and compliance of the cloud) and the security of workloads running on top of the AWS infrastructure (security and compliance in the cloud).

AWS operates, manages, and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the AWS services operate. Customers with workloads on the AWS infrastructure that use virtual private clouds, security groups, operating systems, databases, authentication, and so on depend on AWS for a number of security controls.

Cross-Service Security Controls

These are security controls that you must implement across all services in your AWS instance. Although your use of AWS services will vary according to your risk

posture and security control interpretation, you must document cross-service controls for your use of AWS services.

Example: Multi-factor authentication can be used to help secure IAM users, groups, and roles in the customer environment to meet FERPA requirements for access management, authentication, and authorization for an educational agency, institution, or service organization.

Service-Specific Security Controls

These are service-specific security implementations, such as the Amazon S3 security access permission settings, logging, event notification, or encryption. You may need to document service-specific controls in your use of Amazon S3 to meet a security control objective related to student records, PII, or directory services related to education records.

Example: Server-side encryption with Amazon S3-managed encryption keys (SSE-S3) can be enabled for all objects classified as student records and educational or directory information related to the FERPA privacy and security rule.

Optimized Network, Operating System, and Application Controls

These are controls you may need to document to meet specific control elements related to the use of an operating system or application deployed in AWS.

Example: You can use operating system hardening rules or an optimized private Amazon Machine Image (AMI) to meet security controls in change management.

In addition to a growing understanding of shared, inherited, or dual (AWS and customer) security controls in a cloud environment, there are processes and guidelines that differentiate between the security of a cloud service provider and your responsibilities as a consumer of cloud services. For information about integrating AWS into an existing security framework or designing and performing security assessments of your organization's use of AWS, see AWS Compliance Whitepapers.

Creating a FERPA-Compliant Environment with AWS

The following section provides a high-level overview of services and tools that educational agencies, institutions, and customers should consider as part of their FERPA implementation on AWS:

- **Built-in firewalls**: You can configure built-in firewall rules to control access to your Amazon EC2 virtual instances — from totally public to completely private, or somewhere in between.
- **Authentication and authorization:** In the AWS environment, there are two layers of authentication and authorization to consider: IAM credentials and AWS customer-controlled credentials such as Microsoft Active Directory-based credentials. IAM provides authentication and authorization for direct access to AWS services by using either local IAM accounts or integrating access controls into your corporate directory, such as Active Directory.
- **Guest operating system:** AWS customers control virtual instances in Amazon EC2 and Amazon VPC. You have full administrative access and control over accounts, services, and applications. Although AWS provides images that can be used to deploy host operating systems, you must develop and implement system configuration and hardening standards for your operating systems to align with all applicable FERPA requirements.
- **Storage:** AWS storage options like Amazon EBS, Amazon S3, and Amazon RDS allow you to make data easily accessible to your applications or for backup. Inbound and outbound access to systems that contain sensitive data on the Internet must meet FERPA requirements. To limit access to data from the Internet, Amazon S3 can be configured to require SSL and to allow access to predefined IP addresses only.
- **Private subnets:** Amazon VPC allows you to add another layer of network security to your instances through the creation of private subnets and the addition of an IPsec VPN tunnel between your home network and your Amazon VPC.

- **Encrypted data storage:** The data and objects you store in Amazon EBS, Amazon S3, Amazon Glacier, Amazon Redshift, Oracle, and SQL Server can be optionally encrypted with Advanced Encryption Standard (AES) 256, a secure symmetric-key encryption standard using 256-bit encryption keys.
- **Dedicated connection option:** AWS Direct Connect allows you to establish a dedicated network connection from your premises to AWS. Using industry standard 802.1q VLANs, this dedicated connection can be partitioned into multiple logical connections to enable you to access both public and private IP environments within your AWS cloud.
- **Perfect forward secrecy:** For more communication privacy, AWS services, such as Elastic Load Balancing and Amazon CloudFront, offer newer, stronger cipher suites. These cipher suites allow SSL/TLS clients to use perfect forward secrecy. Session keys are ephemeral; because they are not stored anywhere, captured data cannot be decoded, even if the secret long-term key itself is compromised.
- **Security logs:** AWS CloudTrail provides logs of user activity within your AWS account so you can see which actions are performed on each of your AWS resources and by whom. The AWS API call history enables security analysis, resource change tracking, and compliance auditing.
- **Asset identification and configuration:** With the AWS Config service, you can discover and view the configuration of each of your AWS resources. You can receive notifications each time a configuration changes and use the configuration history to perform incident analysis.
- **Centralized key management:** The AWS Key Management Service provides a convenient management option for creating and administering the keys used to encrypt your data at rest.
- **CloudHSM:** If you must use Hardware Security Module (HSM) appliances for cryptographic key storage, AWS CloudHSM provides a highly secure and convenient way to store and manage keys.
- **AWS Trusted Advisor**: AWS Trusted Advisor monitors AWS resources and alerts you to security configuration gaps, such as overly permissive access to Amazon EC2 instance ports and Amazon S3 storage buckets, minimal use of role segregation using IAM, and weak password policies.

Trusted Advisor is provided automatically when you sign up for Business-level or Enterprise-level support.

AWS security engineers and solution architects have written whitepapers and operational checklists to help you select the best options for your needs. There are also recommended security practices, such as storing secret keys and passwords in a secure manner and rotating or changing them frequently.

Conclusion

AWS delivers services to hundreds of thousands of businesses, including enterprises, educational institutions, and government agencies in more than 190 countries. AWS customers include financial services providers, healthcare providers, government agencies, and educational agencies. They trust AWS with their most sensitive information, including PII, protected health information, and financial records.

AWS services are designed to give you flexibility over the configuration and deployment of your solutions, as well as control over your content — where it's stored, how it's stored, and who has access to it. With the AWS shared responsibility model in mind, you can use the security controls and features offered by AWS services to deploy solutions that meet data privacy and data security requirements and ensure protection of education data in compliance with FERPA.

AWS Certifications and Reports

AWS certifications and reports are produced by AWS third-party auditors and attest to the design and operating effectiveness of the AWS environment. These include:

Service Organization Controls (SOC) 1/ International Standards for Assurance Engagements (ISAE) 3402: AWS publishes a SOC 1, Type II report. The SOC 1 report audit attests that the AWS control objectives are appropriately designed and that the controls safeguarding customer data are operating effectively.

SOC 2-Security: AWS publishes a SOC 2, Type II report, which provides additional transparency into AWS security based on a defined industry standard and further demonstrates the AWS commitment to protecting customer data.

SOC 3-Security: AWS publishes an SOC 3 report, which is a publically available summary of the AWS SOC 2 report that includes the American Institute of CPAs (AICPA) SysTrust security seal.

Information Security Registered Assessors Program (IRAP) Australia: AWS completed an independent assessment that determined all applicable Information Security Model (ISM) controls relating to the processing, storage, and transmission of Controlled Unclassified Information (CUI) Dissemination Limiting Marker (DLM) are in place for the AWS Sydney region.

International Organization for Standardization (ISO) 9001: The AWS ISO 9001 certification directly supports customers who develop, migrate, and operate their quality-controlled IT systems in the AWS cloud. Customers can leverage AWS compliance reports as evidence for their own ISO 9001 programs and industry-specific quality programs, such as GxP in life sciences, ISO 13485 in medical devices, AS9100 in aerospace, and ISO/TS 16949 in automotive. AWS customers who don't have quality system requirements can still benefit from the additional assurance and transparency an ISO 9001 certification provides.

ISO 27001: AWS is certified under the ISO 27001 standard, a widely adopted global security standard that outlines requirements for information security management systems.

Payment Card Industry (PCI)–Security: AWS is Level 1 compliant under the PCI Data Security Standard (PCI DSS). AWS customers can run applications to store, process, and transmit credit card information in the cloud on PCI-compliant technology infrastructure.

Defense Information Assurance Certification and Accreditation Process (DIACAP) and Federal Information Security Management Act (FISMA): A provisional authorization under the Cloud Security Model attests to AWS compliance with Department of Defense standards, reducing the time required for a Department of Defense mission owner to assess and authorize one of its systems for operation on AWS.

Department of Defense CSM Levels 1-2, 3-5: A provisional authorization under the CSM attests to AWS compliance with Department of Defense standards, reducing the time required for a Department of Defense mission owner to assess and authorize one of its systems for operation on AWS.

Federal Risk and Authorization Management Program (FedRAMP): AWS has twice been awarded Agency Authority to Operate (ATO) under FedRAMP at the Moderate impact level. All U.S. government agencies can leverage the AWS ATO packages stored in the FedRAMP repository to evaluate AWS for their applications and workloads, provide authorizations to use AWS, and transition workloads to the AWS environment.

Further Reading

To understand how you can address your privacy and data protection requirements, read the AWS risk, compliance, and security whitepapers and other documentation for best practices, checklists, and guidance:

- AWS Documentation
- AWS Compliance
- Amazon Web Services: Overview of Security Processes
- AWS Security Best Practices
- Securing Data at Rest with Encryption
- Amazon Web Services: Risk and Compliance
- Securing the Microsoft Platform on Amazon Web Services
- Creating Healthcare Data Applications to Promote HIPAA and HITECH Compliance
- Auditing Security Checklist for Use of AWS
- Security at Scale: Logging in AWS
- Family Educational Rights and Privacy Act (FERPA)