FERPA Compliance on AWS

Family Educational Rights and Privacy Act of 1974 (FERPA)

December 2017

aws

[Resource Guide]

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

Introduction **4**

AWS Shared Responsibility Model **5**

Creating a FERPA-Compliant Environment with AWS **6**

Compute 7

Storage 8

Database 9

Networking and Content Delivery 11

Security, Identity, and Compliance 12

AWS Certifications and Reports **13**

Information Management **14**

Auditing 14

Data Destruction 14

Backup and Disaster Recovery 14

Partner Network **16**

NIST Guidance on PII **16**

Further Reading **17**

Abstract

The FERPA Compliance on AWS Resource Guide 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 which is designed to provide protection of education data in compliance with FERPA.

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 parents of students and eligible students:

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

FERPA requires states to use reasonable methods to ensure the security of their information technology (IT) solutions. This may be achieved by hosting education records on cloud computing solutions[1]. The law, in general, requires covered institutions and agencies to reasonably safeguard student education records from improper use or disclosure. 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."

Securing student record information, including students' personally identifiable information ("PII"), is essential for educational institutions and vendors that provide them services which fall under the purview of FERPA. As a hyperscale cloud provider, AWS implements physical and logical controls for internal services and provides robust offerings externally for customers to leverage in order to comply with FERPA.

In a 2017 article published on its website, Gartner,[2] a leading IT research organization, concluded that "the security posture of major cloud providers is as good as or better than most enterprise data centers and security should no longer be considered a primary inhibitor to the adoption of public cloud services." Additionally in an assessment sponsored by AWS, International Data Corporation (IDC[3]), a global provider of advisory services for IT professionals, found that enterprises can be, and likely will be, more secure in the cloud.

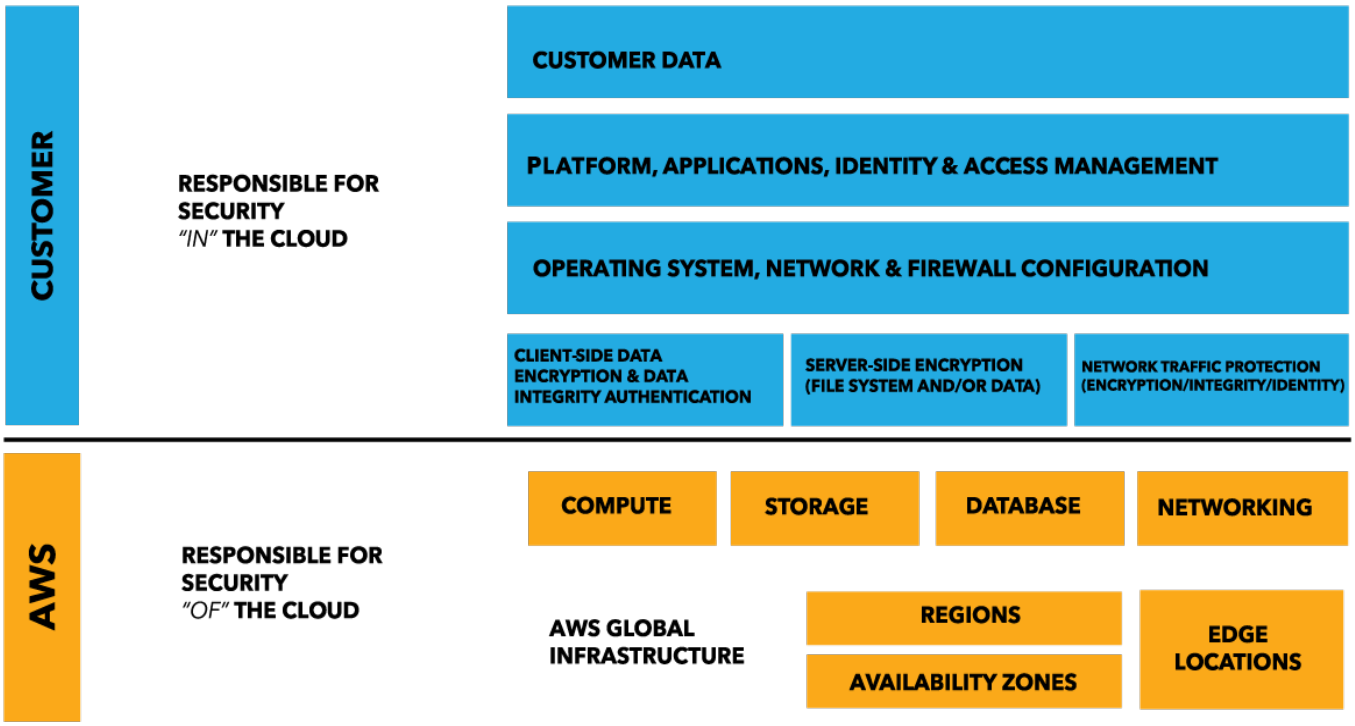
1 http://ptac.ed.gov/sites/default/files/FAQ_Cloud_Computing.pdf

2 http://www.gartner.com/smarterwithgartner/is-the-cloud-secure/

3 Pete Lindstrom, "Assessing the Risk: Yes, the Cloud Can Be More Secure Than Your On-Premises Environment," International Data Corporation (July 2015).

AWS Shared Responsibility Model

Security and compliance are shared responsibilities between AWS and the customer. This model can help relieve customers' operational burden as 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 service operates. In turn, the customer has responsibility and management of the guest operating system (including updates and security patches), other associated application software as well as the configuration of the AWS provided security group firewall. As shown in the chart below, this differentiation of responsibility is commonly referred to as Security "of" the Cloud versus Security "in" the Cloud. Customers should carefully consider the services they choose as customers' responsibilities vary depending on the nature of the services, the integration of those services into their IT environment, and applicable laws and regulations. The Shared Responsibility Model is designed to provide flexibility and customer control over their deployments.



AWS Shared Responsibility Model

For more information about the Shared Responsibility Model, see the Shared Responsibility Model[4] webpage.

4 https://aws.amazon.com/compliance/shared-responsibility-model/

Creating a FERPA-Compliant Environment with AWS

Because FERPA was authored in 1974, it lacks clear guidance on modern technology use, which means that educational institutions are often left to create their own solutions.

As part of this solution customers are encouraged to take steps such as creating device compliance policies, threat protection plans, data loss prevention plans that suit their organization to protect sensitive information, and use encryption and access controls. Access controls also provide auditing and logging capabilities to customers in order to validate privacy and data protection policies that customers have in place.

AWS offers a comprehensive set of features and services to make encryption of PII easy to manage and simpler to audit, including the AWS Key Management Service (KMS). Customers with FERPA compliance requirements have a great deal of flexibility in how they meet encryption requirements for PII. The following section provides a high-level overview of services and tools that educational agencies, institutions, and customers should consider as part of their

Note: The services listed below are not exhaustive, but cover a wide variety that can be configured for compliance with FERPA.

Compute

AWS offers multiple compute products, which customers can use to deploy, run, and scale their applications as virtual servers, containers, or code.

Service	Description	PII Related Information
Amazon EC2[1]	Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides secure, resizable compute capacity in the cloud. It is designed to make web-scale cloud computing easier for developers.	Customers may use EC2 to store, process and transmit PII, but should leverage encryption at layers to safeguard the data at rest and in transit. In addition, customers should make sure the instance is properly hardened and monitored for compliance.
AWS Systems Manager[2]	A management service that helps you automatically collect software inventory, apply OS patches, create system images, and configure Windows and Linux operating systems.	Systems Manager encrypts customer content in transit and at rest. When outputting data that may contain PII to other services (such as S3), customers must follow the receiving service's guidance for storing PII. Customers should not include PII in metadata or identifiers, such as document names and parameter names.
Amazon EC2 Container Service (ECS)[3]	A highly scalable, high performance container management service that supports Docker containers and allows you to easily run applications on a managed cluster of Amazon EC2 instances.	Customers should ensure that the container application is properly hardened and secured. Amazon EC2 Container Service allows you to specify an IAM role for each ECS task. This allows the ECS container instances to have a minimal role, respecting the 'Least Privilege' access policy and allowing you to manage the instance role and the task role separately.
Amazon Elastic MapReduce (EMR)[4]	Provides a managed Hadoop framework that makes it easy, fast, and cost-effective to process vast amounts of data across dynamically scalable Amazon EC2 instances.	Amazon EMR automatically configures Amazon EC2 firewall settings that control network access to instances, and you can launch clusters in an Amazon Virtual Private Cloud (VPC), a logically isolated network you define. For objects stored in Amazon S3, you can use Amazon S3 server-side encryption or Amazon S3 client-side encryption with EMRFS, with AWS Key Management Service or customer-managed keys.
Elastic Load Balancing (ELB)[5]	Automatically distributes incoming application traffic across multiple Amazon EC2 instances.	Customers may use ELB to terminate and process sessions containing PII. Customers have the flexibility to implement two different architectures: 1. Terminate HTTPS, HTTP/2 over TLS (for Application) 2. SSL/TLS listener that uses an encrypted protocol for connections Sessions containing PII must encrypt both front-end and back-end listeners for transport encryption.

Compute Resources

1: https://aws.amazon.com/ec2/
https://aws.amazon.com/blogs/security/how-to-protect-data-at-rest-with-amazon-ec2-instance-store-encryption/
2: https://aws.amazon.com/systems-manager/
3: https://aws.amazon.com/ecs/
4: https://aws.amazon.com/blogs/big-data/secure-amazon-emr-with-encryption/
5: http://docs.aws.amazon.com/elasticloadbalancing/latest/userguide/what-is-load-balancing.html

Storage

AWS offers a range of cloud storage services to support both application and archival compliance requirements. Big data analytics, data warehouses, Internet of Things, databases, and backup and archive applications all rely on some form of data storage architecture.

Service	Description	PII Related Information
Amazon Simple Storage Service (S3)[6]	Object storage built to store and retrieve any amount of data from anywhere – websites and mobile apps, corporate applications, and data from IoT sensors or devices.	Customers should configure their S3 buckets for least privilege and ensure buckets and objects are not world accessible, unless by design. S3 logging should be enabled and S3-SSE (server side encryption) should be enabled or the data should be encrypted prior to storing on S3.
Amazon Elastic Block Store (EBS)[7]	Designed to provide persistent block storage volumes for use with Amazon EC2 instances in the AWS Cloud.	Customers should continue to evaluate and determine whether Amazon EBS encryption satisfies their compliance and regulatory requirements. With Amazon EBS encryption, a unique volume encryption key is generated for each EBS volume; customers have the flexibility to choose which master key from the AWS Key Management Service is used to encrypt each volume key
Amazon Elastic File System (EFS)[8]	Designed to provide simple, scalable file storage for use with Amazon EC2 instances in the AWS Cloud.	Customers should continue to evaluate and determine whether Amazon EFS encryption satisfies their compliance and regulatory requirements. EFS resources are accessed via EC2 or local compute resources, so access to the share should be controlled at the compute level.
Amazon Glacier[9]	A secure, durable, and extremely low-cost cloud storage service for data archiving and long-term backup.	Customers should configure their Glacier vaults for least privilege. All data in the service will be encrypted on the server side. Amazon Glacier handles key management and key protection for you. Amazon Glacier uses one of the strongest block ciphers available, 256-bit Advanced Encryption Standard (AES-256). 256-bit is the largest key size defined for AES. Customers wishing to manage their own keys can encrypt data prior to uploading it. Where long term data retention is required, Glacier Vault Locks should be enabled to provide retention.

Storage Resources

6: http://docs.aws.amazon.com/AmazonS3/latest/dev/UsingEncryption.html
http://docs.aws.amazon.com/general/latest/gr/rande.html#s3_region
7: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html
8: https://aws.amazon.com/premiumsupport/knowledge-center/encrypt-data-efs
9: https://aws.amazon.com/blogs/security/amazon-glacier-introduces-vault-lock

Database

AWS offers a wide range of database services to fit customer's application requirements. These database services can be launched in minutes with just a few clicks.

Service	Description	PII Related Information
Amazon DynamoDB[10]	A fast and flexible NoSQL database service for all applications that need consistent, single-digit millisecond latency at any scale.	Connections to Amazon DynamoDB containing PII must use endpoints that accept encrypted transport (HTTPS). It is recommended that PII stored in Amazon DynamoDB be encrypted at rest. Customers can use the application development framework of their choice to encrypt PII in applications before storing the data in Amazon DynamoDB. Alternatively, a client-side library for encrypting content is available from the AWS Labs GitHub repository.
Amazon RDS (Oracle)[11]	Oracle® Database is a relational database management system developed by Oracle. Amazon RDS makes it easy to set up, operate, and scale Oracle Database deployments in the cloud. With Amazon RDS, you can deploy multiple editions of Oracle Database in minutes with cost-efficient and resizable hardware capacity	Customers can encrypt Oracle databases using keys that customers manage through AWS KMS. On a database instance running with Amazon RDS encryption, data is stored at rest. Customers can also leverage Oracle Transparent Data Encryption (TDE). Customers can also use AWS CloudHSM to store Amazon RDS Oracle TDE keys. Connections to Amazon RDS for Oracle containing PII must use transport encryption using Oracle Native Network Encryption.
Amazon RDS (MySQL)[12]	Amazon RDS allows you to use the AWS Management Console or a simple set of web services APIs to create, delete and modify relational database instances (DB Instances). You can also control access and security for your instance(s) and manage your database backups and snapshots	Amazon RDS (MySQL) allows customers to encrypt their databases using keys that they manage through AWS Key Management Service (KMS). On a database instance running with Amazon RDS encryption, data stored at rest in the underlying storage is encrypted, as are its automated backups, read replicas, and snapshots. AWS recommends that customers run their database instances in private subnets in their VPC, which allows them to isolate their database in their own virtual network and connect to their on-premises IT infrastructure using industry-standard encrypted IPsec VPNs. Customers can configure firewall settings and control network access to their database instances. Resource-level Permissions should be configured so that applications and users have least-privilege permissions enabled.
Amazon RDS (Postgres)[13]	Amazon RDS for PostgreSQL gives you access to the capabilities of a familiar PostgreSQL database engine. This means that the code, applications, and tools you already use today with your existing databases can be used with Amazon RDS.	Amazon RDS for PostgreSQL allows customers to encrypt their databases using keys that they manage through AWS Key Management Service (KMS). On a database instance running with Amazon RDS encryption, data stored at rest in the underlying storage is encrypted as are automated backups, read replicas, and snapshots. AWS recommends that customers run database instances in private subnets in their VPC, which allows them to isolate their database in their own virtual network and connect to their on-premises IT infrastructure using industry-standard encrypted IPsec VPNs. Customers can configure firewall settings and control network access to their database instances. Resource-level Permissions should be configured so that applications and users have least-privilege permissions enabled.

Service	Description	PII Related Information
Amazon Aurora[14]	Amazon Aurora is a MySQL and PostgreSQL compatible relational database built for the cloud, that combines the performance and availability of high-end commercial databases with the simplicity and cost-effectiveness of open source databases.	Amazon Aurora provides multiple levels of database security, including network isolation using Amazon VPC, encryption at rest using keys that customers create and control through AWS Key Management Service (KMS), and encryption of data in transit using SSL. On an encrypted Amazon Aurora instance, data in the underlying storage is encrypted, as are the automated backups, snapshots, and replicas in the same cluster.
Amazon RDS for MariaDB[15]	MariaDB is a popular open source relational database created by the original developers of MySQL. Amazon RDS makes it easy to set up, operate, and scale MariaDB deployments in the cloud. With Amazon RDS, customers can deploy scalable MariaDB databases in minutes with cost-efficient and resizable hardware capacity	Amazon RDS for MariaDB allows customers to encrypt MariaDB databases using keys that customers manage through AWS KMS. Connections to RDS for MariaDB containing PII must use transport encryption
Amazon Redshift[16]	A fast, fully managed data warehouse that makes it simple and cost-effective to analyze data using standard SQL and existing Business Intelligence (BI) tools.	Amazon Redshift uses a Fourier, key-based architecture for encryption. These keys consist of data encryption keys, a database key, a cluster key, and a master key. The cluster key encrypts the database key for the Amazon Redshift cluster. Customers can use either AWS KMS or an AWS CloudHSM (Hardware Security Module) to manage the cluster key. Connections to Amazon Redshift containing PII must use transport encryption.

Database Resources

10: http://docs.aws.amazon.com/general/latest/gr/rande.html#ddb_region
https://github.com/awslabs/aws-dynamodb-encryption-java
11: http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Appendix.Oracle.Options.AdvSecurity.html
http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Appendix.OracleCloudHSM.html
http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Appendix.Oracle.Options.NetworkEncryption.html
12: http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_MySQL.html
13: http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.Encryption.html
http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/UsingWithRDS.SSL.html
14: https://aws.amazon.com/rds/aurora/details/postgresql-details/#security
https://aws.amazon.com/rds/aurora/details/mysql-details/#security
15: http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.Encryption.html
16: http://docs.aws.amazon.com/redshift/latest/mgmt/working-with-db-encryption.html
http://docs.aws.amazon.com/redshift/latest/mgmt/connecting-ssl-support.html

Networking and Content Delivery

AWS networking products are designed to enable customers to isolate their cloud infrastructure, scale their request handling capacity, and connect their physical network to their private virtual network.

Service	Description	PII Related Information
Amazon Virtual Private Cloud (VPC)[17]	Provides functionality to provision a logically isolated section of the Amazon Web Services (AWS) cloud where customers can launch AWS resources in a virtual network that they define.	Amazon VPC offers features such as stateless network access control lists and dynamic reassignment of instances into stateful security groups afford flexibility in protecting the instances from unauthorized network access. Amazon VPC also allows customers to extend their own network address space into AWS, as well as providing a number of ways to connect their data centers to AWS. Amazon VPC Flow Logs provide an audit trail of accepted and rejected connections to instances processing, transmitting or storing PII
Amazon CloudFront[18]	A global content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to viewers with low latency and high transfer speeds.	Amazon CloudFront can used in front of web facing applications designed to provide only valid web traffic is reaching origin servers. All CloudFront customers benefit from the automatic protections of AWS Shield Standard, at no additional charge. CloudFront is also seamlessly integrated with AWS WAF and AWS Shield Advanced to help protect your applications from more sophisticated threats and DDoS attacks
AWS Direct Connect[19]	Makes it easy for customers to establish a dedicated network connection from their premises to AWS. Using AWS Direct Connect, customers can establish private connectivity between AWS and your datacenter, office, or colocation environment.	AWS Direct Connect allows customers to have dedicated connections between their facility and an AWS Edge Location for high-speed and low latency interconnections. Because AWS Direct Connect is a physical connection, the same transport layer requirements that customers would normally use to protect data in transit should be leveraged, such as TLS encapsulation or tunneling traffic via a VPN connection.

Networking and Content Delivery Resources

17: http://aws.amazon.com/vpc/

18: http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/using-https.html
http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/PrivateContent.html

19: https://aws.amazon.com/directconnect/

Security, Identity, and Compliance

Cloud Security at AWS is the highest priority. AWS customers benefit from a data center and network architecture built to meet the requirements of the most security-sensitive organizations.

Service	Description	PII Related Information
AWS KMS[20]	AWS Key Management Service (KMS) is a managed service that makes it easy to create and control the encryption keys used to encrypt data, and uses Hardware Security Modules (HSMs) to protect the security of keys. AWS Key Management Service is integrated with several other AWS services to help customers protect the data that they store with these services. AWS Key Management Service is also integrated with AWS CloudTrail to provide customers with logs of all key usage to help meet their regulatory and compliance needs.	Master keys in AWS KMS can be used to encrypt/decrypt data encryption keys used to encrypt PII in customer applications or in AWS services that are integrated with AWS KMS. AWS KMS can be used in conjunction with a FERPA account, but PII may only be processed, stored, or transmitted in FERPA-eligible services. KMS does not need to be a FERPA-eligible service so long as it is used to generate and manage keys for applications running in other FERPA-eligible services. For example, an application processing PII in Amazon EC2 could use the GenerateDataKey API call to generate data encryption keys for encrypting and decrypting PII in the application. The data encryption keys would be protected by customer master keys stored in AWS KMS, creating a highly auditable key hierarchy as API calls to AWS KMS are logged in AWS CloudTrail.
AWS Shield[21]	A managed Distributed Denial of Service (DDoS) protection service designed to safeguard web applications running on AWS. AWS Shield provides always-on detection and automatic inline mitigations that minimize application downtime and latency.	AWS Shield cannot be used to store or transmit PII, but instead can be used to safeguard web applications that do operate with PII. As such, no special configuration is needed when engaging AWS Shield
Amazon Inspector[22]	An automated security assessment service that helps improve the security and compliance of applications deployed on AWS. Amazon Inspector automatically assesses applications for vulnerabilities or deviations from best practices.	Amazon inspector can be used to validate the configuration of your compute environment to ensure that monitored hosts are compliant with policy as well as not susceptible to risks for CVE exposure
Amazon Macie[23]	Amazon Macie provides data classification and data access information to help ensure data is appropriately handled and accessed.	Amazon Macie allows customers to have better insight into what data they are storing and how it's being accessed and exposed.
Amazon GuardDuty[24]	Amazon GuardDuty provides threat intelligence and monitoring of a customer's account and VPC resources.	Amazon GuardDuty can be used to detect misconfigurations in a customer's account, provide threat intelligence such as instances communicating with known bad actors as well as alerting and automating to remediate these issues.

Security, Identity, and Compliance Resources

20: http://docs.aws.amazon.com/kms/latest/developerguide/programming-encryption.html
https://aws.amazon.com/blogs/big-data/encrypt-and-decrypt-amazon-kinesis-records-using-aws-kms/
21: https://aws.amazon.com/blogs/aws/aws-shield-protect-your-applications-from-ddos-attacks/
22: http://docs.aws.amazon.com/inspector/latest/userguide/inspector_settingup.html
23: https://aws.amazon.com/blogs/security/how-to-query-personally-identifiable-information-with-amazon-macie/
24: https://aws.amazon.com/guardduty/

AWS Certifications and Reports

AWS provides information about its risks and compliance program. This information can assist customers in documenting a control and governance framework with AWS included as an important part of that framework. These include:

- **System and Organization Controls (SOC) 1/ International Standards for Assurance Engagements (ISAE) 3402:** AWS publishes a SOC 1, Type II report. The SOC 1 report attests that the AWS control objectives are appropriately designed and that the controls safeguarding customer data are operating effectively.
- **SOC 2-Security, Availability, & Confidentiality:** AWS publishes a SOC 2, Type II report, which provides additional transparency into the AWS control environment based on a defined industry standard and further demonstrates the AWS commitment to protecting customer data.
- **SOC 3-Security, Availability, & Confidentiality:** 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.
- **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 specifies security management requirements for the development and management of a comprehensive information security management system.
- **ISO 27017:** AWS is certified under the ISO 27017 standard, which supplements the ISO 27001 standard by specifying requirements for cloud service providers to enhance their information security management system by implementing cloud-specific information security controls.
- **ISO 27018:** AWS is certified under the ISO 27018 standard, a global security standard that outlines information security requirements for cloud service providers to protect personal data in the cloud.
- **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.
- **Federal Risk and Authorization Management Program (FedRAMP):** AWS holds a FedRAMP Joint Authorization Board (JAB) Provisional Authority to Operate (P-ATO) at the High impact level. All U.S. government agencies can leverage the AWS P-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.
- **NIST Cybersecurity Framework, v1.0:** AWS conforms to each category and subcategory identified in the NIST CSF, v1.0 and aligns with corresponding FedRAMP and/ or ISO security control requirements.

More information about AWS cloud compliance, see https://aws.amazon.com/compliance/.

Information Management

While FERPA does not require a records retention plan, it does have direct impact on access to and use of existing records. Therefore, AWS encourages organizations to have an up-to-date records retention plan that complies with the requirements of FERPA. Privacy Technical Assistance Center (PTAC) has provided general guidance and best practices on information management and these resources can be found at http://ptac.ed.gov.

Auditing

While FERPA does not specifically require formal audits, customers should put auditing capabilities in place to allow security analysts to examine detailed activity logs or reports to see who had access, IP address entry, what data was accessed, etc. This data may then be tracked, logged, and stored in a central location in compliance with an educational institution's data retention policy.

Using services like Amazon EC2 or EMR, customers can process activity log files and audits down to the packet layer on their virtual servers, just as they do on traditional hardware. Customers may also track any IP traffic that reaches their virtual server instance. Administrators can back up the log files into Amazon S3 for long-term reliable storage.

Data Destruction

FERPA does not require particular methods of data destruction. However, other applicable laws or local privacy regulations may require specific secure data disposal methods. Customers should check with their legal counsel to fully understand their data destruction requirements.

Customers can always use encryption on their data to better ensure that only authorized key material holders may decrypt the data.

Backup and Disaster Recovery

AWS provides several capabilities to back up electronic PII. To implement a data back-up plan on AWS, Amazon EBS offers persistent storage for Amazon EC2 virtual server instances. These volumes can be exposed as standard block devices, and they offer off-instance storage that persists independently from the life of an instance. Customers can create point-in- time snapshots of Amazon EBS volumes that automatically are stored in Amazon S3 and are replicated across multiple facilities. These snapshots can be accessed at any time 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 facilities. These files can be accessed by authorized users at any time, from anywhere (based on permissions), and are stored until intentionally deleted.

Disaster recovery is the process of protecting an organization's data and IT infrastructure in

times of disaster. This involves maintaining highly available systems, keeping both the data and system replicated off-site, and enabling continuous access to both. AWS offers a variety of disaster recovery mechanisms.

With Amazon EC2, administrators can start server instances very quickly and can use an Elastic IP address (a static IP address for the cloud computing environment) for graceful failover from one machine to another. Amazon EC2 also offers Availability Zones.

Administrators can launch Amazon EC2 and Amazon RDS instances in multiple Availability Zones. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. Common points of failures like generators and cooling equipment are not shared across Availability Zones. Additionally, they are physically separate, such that even extremely uncommon disasters such as fires, tornados or flooding would only affect a single Availability Zone. Availability Zones within the same Region benefit from low-latency network connectivity.

Elastic Load Balancing automatically distributes incoming application traffic across multiple targets, such as Amazon EC2 instances, containers, and IP addresses. It can handle the varying load of application traffic across multiple Availability Zones and ensures only healthy targets receive traffic. Auto Scaling helps maintain application availability by provisioning additional resources based on metrics such as CPU utilization. For additional redundancy, Amazon Route 53 supports DNS health checks and automated failover from one AWS Region to another.

For more information about disaster recovery, see http://aws.amazon.com/disaster-recovery.

FERPA implementation on AWS.

Partner Network

The AWS Partner Network (APN) is the global partner program for AWS. It is focused on helping APN Partners build successful AWS-based businesses or solutions by providing business, technical, marketing, and go-to-market support

AWS Education Competency Partners have demonstrated success in building solutions for educational institutions that securely store, process, transmit, and analyze student information. Working with these Competency Partners gives you access to innovative, cloud-based solutions that have a proven track record handling educational data. For more information, see https://aws.amazon.com/education/partner-solutions/.

NIST Guidance on PII

National Institute of Standards and Technology (NIST) publishes 800 series documents that provide guidance to federal agencies on computer security policies. NIST SP 800-53 Rev 4 and NIST SP 800-122 (April 2010 publication) are part of this family of publications. NIST SP 800-53 is a comprehensive security controls catalog developed for federal agencies and NIST SP 800-122 is designed to assist federal agencies in protecting confidentiality of PII in information systems[5]. NIST SP 800-122 deals specifically with protection of PII. Section 4.3 of this document describes a list of security controls corresponding to PII.

To help customers quickly develop a FERPA compliant solution on AWS, we have mapped NIST SP 800-122 controls to the AWS NIST SP 800-53[6] Quick Start[7]. Additionally, appendix J of NIST SP 800-53 document, Privacy Controls Catalog, provides further guidance on additional controls that customers are encouraged to consider while developing security systems for their organizations.

5 http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf

6 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

7 A Quick Start template automatically configures AWS resources and deploys a multi-tier, Linux-based web application in a few simple steps, in about 30 minutes.

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)
- PTAC guidance on best practices for data destruction