Automated Safeguards for Simple Storage Service (S3)

AWS Simple Storage Service (S3) is a highly scalable and durable object based storage service built to store and retrieve data from anywhere. It is designed with 99.999999999% durability, and the ability to store millions of objects. S3 buckets grow elastically as you store or remove data, so your applications have the storage they need, when they need it. S3 offers varying Storage Classes, allowing customers to choose the appropriate storage level and price point to meet their needs.

Object storage is fundamentally different than file or block storage. S3 storage can only be accessed through a REST/API, via:

- **BUCKET** - A bucket is a logical container of objects, where security permissions can be set and inherited by the child objects. You can’t have objects in S3 without a Bucket created first.
- **OBJECT** - An Object is a reference to a single item of unstructured data such as file, backup, or anything else. The key term is single because you can’t put two files in a single object.
- Each file would become an individual object that would be addressable separately including API access, permissions, and metadata.

See cloud object storage for more details regarding object storage.

With S3 you pay for only what you use, depending on the amount of data that is stored, the amount of times that data is accessed, and any associated data transfer costs. S3 Storage and Request pricing is dependent on the Storage Class and region. See https://aws.amazon.com/s3/pricing/ for details.

Amazon S3 contains a large feature set, including powerful and flexible security controls, storage management options, data lifecycle policies, file versioning, audit controls, and many others. ClearDATA recommends customers visit https://aws.amazon.com/s3/features/ for up to date features and architecture guidance.

Compliance Guidance

ClearData enables the following compliance/remediation features for S3:

- **Log Monitoring Status** - verifies that logging is enabled on your S3 buckets. If logging is not enabled on new buckets, ClearDATA Automated Safeguards enable it.
- **Versioning Enabled Status** - verifies that object versioning is enabled on S3 buckets. If object versioning is not enabled on new buckets, ClearDATA Automated Safeguards enable it.
- **Static Webhosting Status** - reviews S3 buckets to determine whether they are configured to host static websites. If static web hosting is enabled on new buckets, ClearDATA Automated Safeguards disable it.
- **Bucket Policy Status** - ensures that your AWS S3 buckets are not publicly accessible via bucket policies in order to protect against unauthorized access. If the bucket policy is determined to allow public access on new buckets, ClearDATA Automated Safeguards modify the bucket policy to prevent public access.
- **Buckets Access Control List (ACL) Status** - detects misconfigured S3 bucket access policies to prevent the leakage of sensitive information or allow unauthorized data access, alteration, or deletion. If the bucket ACL is determined to allow public access on new buckets, ClearDATA Automated Safeguards modify the bucket policy to prevent public access.
- **Policy PUT Encryption** - ensures that default encryption is enabled at the bucket level to automatically encrypt all objects when stored in Amazon S3.   If a PUT policy enforcing encryption is not enabled on new buckets, ClearDATA Automated Safeguards enable it using AES-256 option to use Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3).
- **Server Side Encryption** - ensures that your AWS S3 buckets are protecting your sensitive data at rest by enforcing Server-Side Encryption. If Server Side Encryption is not enabled on new buckets, ClearDATA Automated Safeguards enable it using AES-256 option to use Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3).
- **Secure Transport** - ensures that your AWS S3 buckets enforce encryption of data over the network (as it travels to and from Amazon S3) using Secure Sockets Layer (SSL). If secure transport is not enforced on new buckets, ClearDATA Automated Safeguards enable it.

Log Monitoring Status

HIPAA 45 CFR 164.308(a)(1)(ii)(D) requires a Covered Entity to implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports. ClearDATA monitors your S3 bucket to ensure logging is enabled and stores bucket logs in a target bucket. With the Server Access Logging feature enabled for your S3 buckets, you can track bucket access requests, use the log data to take protective measures against unauthorized user access, and routinely track and manage details about your S3 bucket for appropriate access and external threats. Access log information can be useful in security and access audits. ClearDATA monitors your S3 bucket to ensure logging is enabled and stores bucket logs in a target bucket. With the Server Access Logging feature enabled for your S3 buckets, you can track bucket access requests, use the log data to take protective measures against unauthorized user access, and routinely track and manage details about your S3 bucket for appropriate access and external threats. Access log information can be useful in security and access audits. This check verifies that logging is enabled on your S3 buckets. S3 logging provides a way to obtain details about S3 bucket activity. When logging is enabled, AWS S3 delivers access logs to a target bucket of your choosing. If you do not select a logging bucket, ClearDATA will create one for you. An access log record contains details about the requests made to a bucket. These requests can include the request type, the resources specified, and the time and date the request was processed. By default, AWS does not enable logging for S3 buckets. This additional insight into bucket activity can be useful when troubleshooting and may be requested by support engineers. Logging cannot be activated retroactively to an issue.

Remediation

If Server Access Logging is not enabled on a bucket ClearDATA will automatically and transparently enable the settings and, if necessary, configure a logging bucket.

Versioning Enabled Status

HIPAA 164.312(c)(2) requires a Covered Entity to implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner. ClearDATA provides an assessment of S3 bucket configuration settings to ensure that S3 buckets have lifecycle policy (versioning) enabled. This assessment assures that AWS S3 buckets have the versioning flag enabled to preserve and recover overwritten and deleted S3 objects as an extra layer of data protection and data retention. This check verifies that object versioning is enabled on S3 buckets. Using lifecycle policies versioning-enabled S3 buckets allow you to preserve, retrieve, and restore every version of an S3 object (a file). S3 versioning can be used for data protection and retention scenarios such as recovering objects that have been accidentally or intentionally deleted or overwritten by users or applications. Versioning also allows the archival of previous versions of objects to AWS Glacier for long-term, low-cost storage. By default, versioning is disabled for a new bucket.

Remediation

If versioning is not enabled on a bucket ClearDATA will automatically and transparently enable the setting.

Static Webhosting Status

HIPAA 164.312(c)(1) requires a Covered Entity to implement policies and procedures to protect electronic protected health information from improper alteration or destruction. ClearDATA monitors your Amazon S3 Buckets configured as websites to ensure they are regularly reviewed for security purposes. ClearDATA will provide a FAILED status on any Buckets that host static websites where the S3 bucket is known to contain PHI or PII. This will provide safeguards around your S3 bucket to ensure web browsers cannot access all data in your S3 bucket through the S3 website endpoint for your bucket. This check reviews S3 buckets to determine whether they are configured to host static websites. If so, the configuration of the bucket must be appropriate to the sensitivity level of the data stored on or accessed by the bucket. The bucket must be accessible only by the appropriate website endpoint, and no PHI/PII should be available to unauthorized users. ClearDATA strongly recommends that website hosting be disabled.

Remediation

If the Static Webhosting option is enabled on the bucket ClearDATA will automatically disable the option.

Bucket Policy Status

HIPAA 164.312(e)(1) requires a Cover Entity to implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network. ClearDATA monitors bucket policies to ensure that AWS S3 buckets are not publicly accessible. Allowing unrestricted access through bucket policies provides anyone the ability to list the objects within the bucket (ListBucket), download objects (GetObject), upload/delete objects (PutObject, DeleteObject), view objects permissions (GetBucketAcl), edit objects permissions (PutBucketAcl) and more. ClearDATA strongly recommends using bucket policies to limit the access to a particular AWS account (authorized account) instead of providing public access to anyone on the Internet. This check ensures that your AWS S3 buckets are not publicly accessible via bucket policies in order to protect against unauthorized access. Granting public access to your S3 buckets via bucket policies can allow malicious users to view, get, upload, modify and delete S3 objects, actions that can lead to data loss and unexpected charges on your AWS bill.

Remediation

If the bucket policy is determined to be too broad, such as allowing public access, the policy will be removed.

Buckets ACL Status

HIPAA 164.312(a)(1) required a Covered Entity to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights. ClearDATA monitors bucket policies that grant FULL CONTROL access to your S3 buckets. Granting authenticated "FULL_CONTROL" access to AWS S3 buckets can allow other AWS accounts or IAM users to view, upload, modify and delete S3 objects without any restrictions. Exposing your S3 buckets to AWS signed accounts or users can lead to data leaks, data loss and unexpected charges for the S3 service. You must routinely track and manage details about your storage activity for appropriate access and external threats. This includes monitoring bucket policies to identify misconfigurations that could allow inappropriate access to an S3 bucket. ClearDATA services include the visualization of these trends for you to access and view. Access log information can be useful in security and access audits. This check detects misconfigured S3 bucket access policies to prevent the leakage of sensitive information or allow unauthorized data access, alteration, or deletion. ClearDATA strongly encourages you to ensure that S3 buckets do not grant FULL_CONTROL access to authenticated users (i.e., signed AWS accounts or AWS IAM users) to prevent unauthorized access. An S3 bucket that allows full control access to authenticated users will give any AWS account or IAM user the ability to LIST (read) objects, UPLOAD /DELETE (write) objects, VIEW (READ_ACP) objects permissions and EDIT (WRITE_ACP) permissions for the objects within the bucket. ClearDATA recommends against setting these permissions for the 'Any Authenticated AWS User' ACL predefined group in a production environment. Granting Public access allows anyone unfettered access to read directory structures, read files and access files (even if encrypted) unles the Write/Delete permissions is checked and the default is read only for public buckets. Exposing S3 buckets to AWS signed accounts or users can lead to data leaks, data loss and unexpected charges for the S3 service.

Remediation

If the bucket ACL is determined to be too broad, such as allowing access to Authenticated Users and therefore all users, the ACL may be removed.

Policy PUT Status

HIPAA 164.312(a)(2)(iv) requires a Covered Entity to implement a mechanism to encrypt and decrypt electronic protected health information. ClearDATA monitors customer compliance to GDPR Article 32 the encryption subsection of GDPR Article 32 Section 1(a). To comply with the requirements for data storage encryption, your S3 buckets must be protected with server-side encryption keys (SSE-S3) which use bucket policies and deny PUT requests for objects that do not include a server-side encryption header. This check ensures that default encryption is enabled at the bucket level to automatically encrypt all objects when stored in Amazon S3. The S3 objects are encrypted during the upload process using server-side encryption with either AWS S3-managed keys (SSE-S3) or AWS KMS-managed keys (SSE-KMS). S3 default encryption enables AWS to encrypt S3 data at the bucket level instead of object level in order to protect it from attackers or unauthorized users. To encrypt all objects stored in a bucket, include encryption information (i.e. "x-amz-server-side-encryption" header) with every object storage request. Also, to encrypt S3 objects without default encryption, a bucket policy must be configured to deny storage requests that do not include the encryption information.

Remediation

If the bucket policy does not enforce an encrypted transport when using the PUT command, the policy will be updated to enforce that encryption connection.

Server Side Encryption

HIPAA 164.312(a)(2)(iv) requires a Covered Entity to implement a mechanism to encrypt and decrypt electronic protected health information. ClearDATA monitors customer compliance to 45 CFR 164.312(a)(2)(iv), the encryption subsection of 45 CFR 164.312(a)(1). To comply with the requirements for data storage encryption, your S3 buckets must be protected with server-side encryption keys (SSE-S3) which use bucket policies (AES-256/KMS) and deny PUT requests for objects that do not include a server-side encryption header. This check ensures that your AWS S3 buckets are protecting your sensitive data at rest by enforcing Server-Side Encryption. When processing sensitive data that is crucial to your business, it is highly recommended that you implement encryption in order to protect it from attackers or unauthorized personnel. Using S3 Server-Side Encryption (SSE) will enable Amazon to encrypt your data at the object level as it writes it to disks and decrypts it transparently for you when you access it. Note: Server-Side Encryption (SSE) utilizes one of the strongest block ciphers available, 256-bit Advanced Encryption Standard (AES-256), to encrypt your S3 objects.

Remediation

If bucket encryption is not enabled when it is provisioned ClearDATA will automatically and transparently enable bucket encryption.

Secure Transport

HIPAA 164.312(e)(1) requires a Covered Entity to implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network. ClearDATA monitors the customer compliance to 45 CFR 164.312(a)(2)(iv) the encryption subsection of 45 CFR 164.312(a)(1) ClearDATA recommends that your AWS S3 buckets enforce encryption of data over the network (as it travels to and from Amazon S3) using Secure Sockets Layer (SSL). This encryption denies all regular, unencrypted HTTP requests to your buckets when dealing with sensitive or private data. his check ensures that your AWS S3 buckets enforce encryption of data over the network (as it travels to and from Amazon S3) using Secure Sockets Layer (SSL). When S3 buckets are not configured to strictly require SSL/TLS connections, the communication between the clients (users, applications) and these buckets is vulnerable to eavesdropping and man-in-the-middle (MITM) attacks. ClearDATA strongly recommends enforcing SSL-only access by denying all regular, unencrypted HTTP requests to your buckets when dealing with sensitive or private data.

Remediation

If the bucket setting does not enforce an encrypted transport when using the PUT command, the settings will automatically and transparently be updated to enforce that encryption connection.

Shared Responsibility

ClearDATA ensures that all all of the compliance requirements are met for all newly created S3 buckets based on the guidance above.

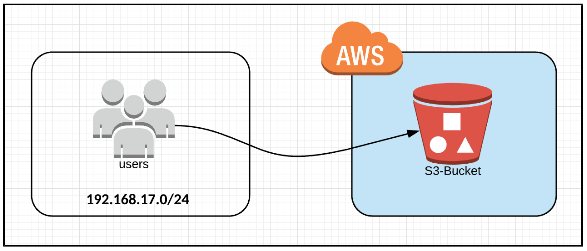
Customers are responsible to not use PHI in bucket names, object names, or metadata because this data is not encrypted using S3 server-side encryption and is not generally encrypted in client-side encryption architectures.

Please contact your ClearDATA team for a copy of the full Responsibilities Matrix.

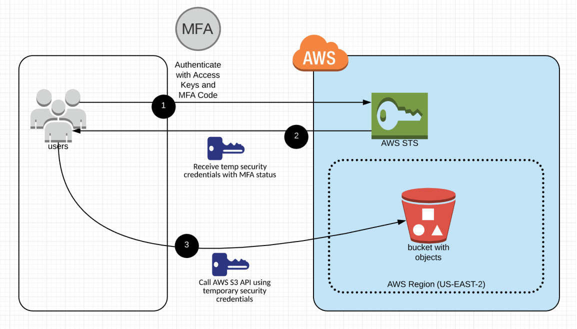
Exclusion

Disabling automated remediation at done the bucket level. Please contact ClearDATA Support to request that an exclusion be placed to allow for the bucket to be created.

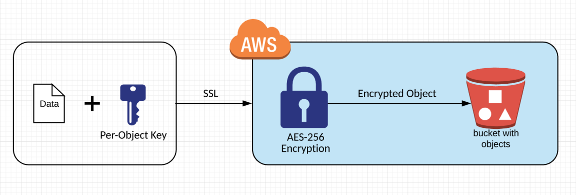
Private bucket with access restricted to a source CIDR block



Private bucket with access requiring multi-factor authentication


MFA
Authenticate with Access Keys and MFA Code
AWS
1
2
users
AWS STS
Receive temp security credentials with MFA status
3
bucket with objects
Call AWS S3 API using temporary security credentials
AWS Region (US-EAST-2)

Private bucket with contents encrypted with S3 server side encryption



Users can be added to the DPHI-S3 IAM group in order to access the S3 service. Customers have access to all S3 buckets, with the exception of ClearDATA managed buckets that may be located in the customer account.

Item	ClearDATA	Customer
Enforcement of Automated Safeguards	RA	IC
Ensure no PHI is used in bucket names, object names, or metadata	IC	RA