CUIMC Cloud Account Shared Responsibility Agreement

When deploying compute instances or other components on a cloud provider's platform, there exists a shared responsibility between CUIMC and the public cloud provider. The public cloud provider has the responsibility to make sure that their cloud platform is performant, secure, and appropriately updated with the latest security. As public cloud consumers, CUIMC personnel are responsible for the performance, security, and software updates of CUIMC applications and storage that run on a public cloud. This means that security needs to be a top priority for CUIMC personnel. A security breach or data leakage can expose Protected Health Information (PHI) data or other private information. This not only exposes our patients to an invasion of their privacy but causes our patients to lose faith in CUIMC's ability to keep their information confidential and secure. The public cloud provider is usually not at fault. These privacy exposures usually occur when a system is not fully secured or patched by the organization that is running their application on a public cloud. There have been many personal data exposures that have occurred in recent years that have caused organizations public embarrassment and they have been made to pay multi-million-dollar fines. Many of these security breaches and data leakages are simply caused by having systems or data accessible via the Internet with anonymous access or poor passwords.

Below is a matrix of the public cloud security responsibilities:

CUIMC Public Cloud Consumer/Operator	Responsible for the security of components running on a public cloud and public cloud data storage security.	Access privileges to and patching of application, database and web virtual instances. Access privileges to and patching of applications running on virtual or serverless instances. Patching operating systems and application containers such as Kubernetes and Docker. Patching third party applications such as Apache, IIS, Tomcat, MSSQL, MySQL and Postgres. Block, file and object store data access. Virtual network ingress and egress control.

Public Cloud Provider	Responsible for the security of the public cloud infrastructure.	Physical hosts and physical network components that make up the infrastructure of the public cloud. Applications that run the public cloud such as a console or a serverless engine.

Cloud providers can provide some policy guardrails to prevent an accidental exposure and do usually default to the principle of least privilege (https://csrc.nist.gov/glossary/term/least-privilege). These privileges can usually be overridden by the public cloud consumer and in many cases the overridden privileges are the cause of an access or data breach.

CUIMC-IT implements the following policies. Autonomous CUIMC departments not under CUIMC-IT's purview will also need to implement these same policies.

CUIMC Cloud Requirement	CUIMC-IT Provides	CUIMC Customer/Operator Action(s)
A security breach triage and reporting process is implemented.	An established process to follow.	Notify CUIMC-IT Security if a breach is detected.
Access logs and audit trails are centrally aggregated and analyzed for issues and compliance. Notifications should be sent to alert the appropriate administrators.	By default, logs are aggregated and analyzed.	Identify the appropriate individuals who need to receive alerts.
Access to PHI or other sensitive data via anonymous access is prohibited.	CUIMC-IT policies prevent anonymous access to object store assets.	Circumventing any policies or allowing anonymous access without first consulting CUIMC-IT is prohibited.
Accounts should never be shared.	N/A	All staff should be aware that account sharing is prohibited.
Account termination and asset owner transfer process should be created.	A process is in place to deactivate an employee after separation.	Make CUIMC-IT aware that an employee has separated from CUIMC and who the new asset owner is.
Adhere to the cloud providers HIPAA guidelines when dealing with PHI data. Not all services are HIPAA certified.	CUIMC-IT uses the guidelines published from the individual cloud providers to deploy cloud assets.	Notify CUIMC-IT if there has been any breach of protocol when dealing with PHI data so that remediation of the issue can be executed.

Adhere to all CUIMC-IT ISO policies and best practices.	CUIMC-IT constantly revises security polices and best practices to reflect current industry policies and best practices.	Review CUIMC-IT Policies.
Adhere to the principle of least privilege and access.	CUIMC-IT creates all assets following this policy.	Do not create assets with global access privileges. Always limit access.
Adhere to the cloud platform, application and system best security policies and industry wide best practices.	CUIMC-IT constantly reviews industry best practices and policies.	Review CUIMC-IT's best practices. Update assets when necessary.
Applications, networks and systems should be periodically audited and probed to make sure they are secure.	CUIMC-IT ISO constantly audits network and systems.	N/A
Backup or snapshots are performed for data recovery, compliance and disaster recovery.	CUIMC-IT can assist customers create and maintain backup strategies.	Follow the cloud providers best practices for backups. Create a backup strategy that best works for your data.
Backups should be retained for the duration that has been established for each type of data and by the data owner.	CUIMC-IT can assist customers create and maintain backup strategies.	Analyze data retention requirements for your data and create a data retention strategy.
Block based, file based, and object-store based data should be properly secured and encrypted.	CUIMC-IT encrypts data at rest.	Use encryption at rest when storing data.
Cloud components should be properly tagged to provided contact, owner and environmental information.	CUIMC-IT tags assets during creation.	Any assets created should be tagged with the appropriate tags.
Cloud access API Key/Secret should be periodically rotated when temporary keys/secrets cannot be used.	CUIMC-IT will institute a periodic Key/Secret age check.	Rotate keys/secrets periodically.
Cloud platform operators need to be aware of the latest security exploits especially zero-day exploits	CUIMC-IT keeps updated on the latest security issues and reviews and applies and remediation.	Make sure that any customer applications are updated to remediate and security issues.

and remediate the exploit as soon as a fix is available.		
Cloud component creation actions such as use and deletion, data access and sign on are logged centrally.	CUIMC-IT uses centralized logging and auditing.	N/A
Critical object-store data should be replicated and access restricted. Users should be prevented from deleting buckets.	CUIMC-IT removes the delete bucket permissions.	Identify any critical data that needs to be replicated and backups up. Work with CUIMC-IT on a backup strategy.
Delete old unused data.	N/A	Delete any data that is no longer being used.
Restrict network access especially when sensitive data needs to be made available on a network.	CUIMC-IT restricts access to networks using security groups and network access control lists.	Do not allow unrestricted network access.
Root, encryption and access keys, secrets and passwords should be stored securely with more than one individual that has access.	CUIMC-IT uses a secure repository.	Make sure that there are always multiple owners for assets. Secure all keys and passwords.
Security groups should be used on each cloud component where possible to prevent non-authorized access and to establish a non-trusted network.	CUIMC-IT restricts access to individual instances. It follows a policy of Non-trusted Networking.	Use security groups to restrict access to assets.
Security updates to applications, frameworks and operating systems are performed periodically and as soon as possible when issues arise.	CUIMC-IT performs updates on CUIMC-IT controlled instances especially when zero-day vulnerabilities are found.	Update assets regularly. Be aware of current security issues and deploy patches when necessary.
Two factor authentications should be enabled for cloud console access.	CUIMC-IT enables Two Factor Authentication.	N/A
Use only secure protocols such as HTTPS, SCP and SFTP to communicate.	CUIMC-IT will only use secure communications protocols on assets under their control.	Use secure protocols for all communications.
Use Infrastructure as Code to deploy cloud assets to	CUIMC-IT deploys infrastructure via code where possible.	Deploys assets via code where possible.

prevent infrastructure configuration drift.		
Use a private source repository such as GitLab to for all cloud application source and templates. Verify that access keys/secrets, userids and passwords are not in the source files.	CUIMC-IT verifies that its repositories do not contain keys/secrets or passwords.	Verifies that its repositories do not contain keys/secrets or passwords.
Use known hardened and secure operating systems images for virtual instance and container deployment.	CUIMC-IT creates a hardened image to use for its instance deployments.	Creates a hardened image to use for deployments.

Each public cloud provider has their own set of security, HIPAA compliance, and privacy guidelines. These guidelines will also list the services that are HIPAA compliant. Not all cloud-based services are certified to run applications that use or store PHI data. For example, at one time many public cloud providers required that you used dedicated hosts to run your virtual instances. Below is a list of the compliance and HIPAA policies of CUIMC and the major public cloud providers:

https://cumcprod.service-now.com/kb?id=kb_article_view&sys_kb_id=79a05a31dbafa3009ffb84eb0b96190d

https://www.hipaa.cumc.columbia.edu/

https://www.hipaa.cumc.columbia.edu/hipaa-policies

https://cloud.google.com/security/compliance/#/

https://cloud.google.com/security/compliance/hipaa/

https://cloud.google.com/security/compliance/hipaa-compliance/

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

https://aws.amazon.com/compliance/hipaa-compliance/

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

https://azure.microsoft.com/en-us/overview/trusted-cloud/compliance/

https://servicetrust.microsoft.com/ViewPage/HIPAABlueprint

For workloads and data storage that handle PHI data a Business Associate Agreement (BAA) must be in place with the public cloud provider:

https://www.hipaa.cumc.columbia.edu/business-associates