Policy Number: TBD

Effective Date: 5/15/2019
Last Revised: ___________

SUNY DOWNSTATE MEDICAL CENTER
POLICY AND PROCEDURE

Subject: **Cloud Data Security Policy**

Prepared by: David W. Loewy, PhD,
Information Security Officer

Reviewed by: Dilip Nath. Interim CIO

Lynn Reid-McQueen Legal Counsel

Shoshana Milstein

Approvals:

Dilip Nath

Lynn Reid-McQueen

Michelle Daniels-Devore

No.

Page 1 of 10

Original Issue Date: **5/15/2019**

Supersedes Date: New

Effective Date: **5/15/2019**

Issued by: **Information Services & Technology Department**

Cloud Data Security Policy

Scope:

This policy applies to all persons accessing and using third party services capable of storing or transmitting electronic data that is owned or leased by SUNY Downstate Medical Center (SUNY DMC). This includes all consultants or agents of SUNY DMC and any parties who are contractually bound to handle data produced by SUNY DMC, and in accordance with SUNY DMC contractual agreements and obligations.

Purpose:

The purpose of this policy is to ensure that SUNY DMC Protected or SUNY DMC Sensitive data is not inappropriately stored or shared using public cloud computing and/or file sharing services. Cloud computing and file sharing, for this purpose, is defined as the utilization of servers or information technology hosting of any type that is not controlled by, or associated with, SUNY DMC for services such as, but not limited to, social networking applications (i.e. all social media, blogs and wikis), file storage (drop box,etc), and content hosting (publishers text book add-ons).

Reason for Policy:

This policy endorses the use of cloud services for file storing and sharing 1) with vendors who can provide appropriate levels of protection and recovery for SUNY DMC information, and 2) with explicit restrictions on storage of SUNY DMC Electronic Protected Information. While cloud storage of files can expedite collaboration, some guidelines must be in place for the kind and type of SUNY DMC information that is appropriate for storing and sharing using these services.

Federal and State laws and regulations place a premium on institutions' ability to understand the risks of Information Technology (IT) services and systems and make appropriate determinations about risk tolerance. Some cloud providers, for instance, may mine stored data for marketing purposes. There are a number of information security and data privacy concerns about use of cloud computing services at the SUNY DMC including:

- SUNY DMC no longer protects or controls its data stored in the cloud, leading to lessened security and a potential inability to comply with various regulations and data protection laws;
- Loss of privacy of data, due in part to aggregation with data from other cloud consumers;
- SUNY DMC will be dependent upon a third party for critical infrastructure and data handling processes;
- Potential security and technological defects in the infrastructure provided by a cloud vendor;
- Without a service level agreement between SUNY DMC and a cloud vendor, SUNY DMC may not have access or control over the stored data.

Policy:

The following table outlines the data classification and proper handling of SUNY DMC data.

		Cloud Storage (See appendix for approved services)	**Network Drive** *(SUNY DMC ID and Password Required)*	**Local Storage**
Data Classification	**SUNY DMC Protected**	**Not Allowed**	**Allowed** No special requirements, subject to any applicable laws	**Not Allowed**
	SUNY DMC Sensitive	**Allowed but Not Advised** Requires Dept. Manager approval	**Allowed** No special requirements, subject to any applicable laws	**Allowed but Not Advised** Requires Dept. Manager approval
	SUNY DMC Public	**Allowed** No special requirements	**Allowed** No special requirements	**Allowed** No special requirements

Use of central and departmental servers, where authentication is required, is the best place to store all categories of SUNY DMC data, particularly SUNY DMC Protected data.

Under no circumstances should SUNY DMC Protected Data be stored on any device or any storage vehicle that is not authorized by SUNY DMC IT Services.

Definitions:

SUNY DMC Protected Data - Any data that contains personally identifiable information concerning any individual and is regulated by Federal, State or Local privacy regulations. Examples of Protected Data include, but are not limited to: student academic records; patient health information; social security numbers of employees, patients and students; confidential research records; individual financial records.

SUNY DMC Sensitive Data - Any data that is not classified as SUNY DMC Protected Data, but which is information that SUNY DMC would not distribute to the general public. Examples of Sensitive Data may include, but are not limited to: institutional and departmental financial data; strategic plans and information that may be considered proprietary.

SUNY DMC Public Data - Any data that SUNY DMC is comfortable distributing to the general public. For example, press releases and general information regarding the hospital and the SUNY DMC schools and colleges.

General Data Protection Terms:

In determining whether a cloud storage vendor provides sufficient protections, SUNY DMC should ensure the following criteria are met in order to ensure a minimum level of information security protection:

- Data transmission and encryption requirements
- Authentication and authorization mechanisms
- Intrusion detection and prevention mechanisms
- Logging and log review requirements
- Security scan and audit requirements
- Security training and awareness requirements

Compliance with Legal and Regulatory Requirements:

SUNY DMC has many federal laws that it must follow. These include the Family Educational Rights and Privacy Act of 1974 (FERPA), the Health Insurance Portability and Accountability Act (HIPAA), and the Gramm-Leach-Bliley Act (GLBA). New York State Laws also affect the relationship with a cloud-computing vendor.

NOTE: A relationship with a cloud-computing vendor may also be impacted by private industry regulations. For example, departments at SUNY DMC that accept credit cards, must also follow the Payment Card Industry (PCI) Data Security Standard (DSS) issued by the major credit card companies. Finally, cloud-computing services that use, store, or process SUNY DMC data must also follow applicable SUNY system and local DMC policies. Such policies may include Information Technology Services policies and SUNY DMC's data handling requirements.

Exit Strategy:

Cloud services should not be engaged without developing an exit strategy for disengaging from the vendor or service and integrating the service into business continuity and disaster recovery plans. SUNY DMC must determine how data would be recovered from the vendor.

Questions. Any questions regarding the application of this policy or the appropriateness of a particular cloud storage service should be addressed to the Information Security Officer or CIO.

Appendix:

<u>Listing of Cloud Storage Services</u>

This listing is meant to serve only as a partial list of cloud storage services. Any cloud storage service not explicitly listed as approved should be assumed to be not approved and would require consultation with IT.

Services Approved for SUNY DMC Use	Services Not Approved for SUNY DMC Use
	Dropbox
(Enterprise) Microsoft OneDrive	iCloud
	Microsoft OneDrive (Personal Account)
	Amazon Cloud Drive
	Google Drive
	Box

This list is accurate as of March 1, 2018.

Specific Guidelines for Use of OneDrive

Individuals who use enterprise Microsoft OneDrive accounts for SUNY DMC work are responsible for ensuring that SUNY DMC Protected information is not placed or stored in unapproved or inappropriate locations. OneDrive is permitted for institutional use; however, only information classified as SUNY DMC Public or SUNY DMC Sensitive, when approved by the Department Manager, may be placed or stored in OneDrive. When sharing files and folders with other collaborators, individuals are responsible for reviewing access levels to ensure that data is not inappropriately shared. The enterprise OneDrive account may not be utilized to collect, process, or store data covered by laws such as HIPAA, FERPA, FISMA, IPIPA, and GLBA.