SUNY DOWNSTATE Medical Center

UNIVERSITY HOSPITAL OF BROOKLYN
POLICY AND PROCEDURE

Subject:	Encryption and Decryption Policy	**No. HIS-13**	
		Page	1 of 7
Prepared by:	David W. Loewy, PhD	**Original Issue Date:**	9/2015
Reviewed by:	Shoshana Milstein, RHIA, CHP, CCS Dilip Nath. MBA, SCM, SCD, ITIL	**Supersedes Date:**	9/2015
		Effective Date:	9/2017
Committee Approvals:	Governing Body	**TJC Standards:**	IM.02.01.01 The hospital protects the privacy of health information
Approved by:	John Dooley, DMC, CIO Margaret Jackson, MA, RN Miriam Vincent, MD, PhD, JD Michael Lucchesi, M.D. Patricia Winston, MS, RN William Walsh, MBA, MSW	**Issued by: Health Information Systems**	

1) Introduction

a) **SUNY DOWNSTATE MEDICAL CENTER** has adopted this Encryption and Decryption Policy in order to recognize the requirement to comply with the Health Insurance Portability and Accountability Act ("HIPAA"), as amended by the Health Information Technology for Economic and Clinical Health ("HITECH") Act of 2009 (Title XIII of division A and Title IV of division B of the American Recovery and Reinvestment Act "ARRA") and the HIPAA Omnibus Final Rule (Effective Date: March 26, 2013). We acknowledge that full compliance with the HIPAA Final Rule is required by or before September 23, 2013.

b) **SUNY DOWNSTATE MEDICAL CENTER** hereby acknowledges our duty and responsibility to

protect the privacy and security of Individually Identifiable Health Information ("IIHI") generally, and Protected Health Information ("PHI") as defined in the HIPAA Regulations, under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under principles of general and professional ethics. We also acknowledge our duty and responsibility to support and facilitate the timely and unimpeded flow of health information for lawful and appropriate purposes.

2) Scope of Policy

a) This policy governs the Encryption and Decryption of Protected Health Information for **SUNY DOWNSTATE MEDICAL CENTER**. All personnel of **SUNY DOWNSTATE MEDICAL CENTER** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

b) Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

3) Assumptions

a) **SUNY DOWNSTATE MEDICAL CENTER** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
b) **SUNY DOWNSTATE MEDICAL CENTER** must comply with HIPAA and the HIPAA implementing regulations pertaining to encryption and decryption, in accordance with the requirements at § 164.312(a)(1-2).
c) The establishment and implementation of an effective encryption and decryption policy is a crucial element in our overall objective or providing reasonable protections for individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).

4) Policy Statement:

a) Media which cannot be protected by other methods of access control shall utilize encryption and decryption to protect ePHI from unauthorized disclosure. Encryption and Decryption may also be utilized in combination with other access controls where indicated by risk analysis.

b) **SDMC** will identify systems that require ePHI to be encrypted.

c) **SDMC** will identify members of the workforce who require encryption capabilities.

d) **SDMC** will need to balance the challenge of protecting "data at rest" such as that defined in the Access Control standard of the HIPAA Security Rule against the increase in security technology complexity and administrative overhead including performance considerations and usability.

e) **SDMC** will test encryption and decryption capabilities of products and systems to ensure proper functionality.

f) It is the Policy of **SDMC** to establish and maintain this encryption and decryption policy in full compliance with all the requirements of HIPAA.

g) Responsibility for the development and implementation of this encryption and decryption policy, and any procedures associated with it, shall reside with Data Security Officer, who shall ensure that this policy is maintained, updated as necessary, and implemented fully throughout our organization.

h) Specific procedures shall be developed to specify the proper usage and application of encryption and decryption for all computers and workstations that access individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).

i) It is the Policy of **SDMC** to fully document all encryption and decryption-related activities and efforts, in accordance with our Documentation Policy.

5) Policy Specifics

a) **Desktop Computers**

i) SDMC desktop computers are generally accepted as having a lower risk of being stolen and as such most will not need to have encryption software installed. However Desktop computers which are located in unrestricted areas which are open to the public (for example: reception desks etc) will need to have encryption software installed:

ii) The preferred method of encryption for SDMC desktop computer devices is whole disk encryption.

b) **Laptops, Tablets**

i) All SDMC laptop computer devices must have SDMC approved encryption software installed prior to their use within the SDMC. In addition to encryption software the laptop must be password protected and have up to date anti-virus software installed.

ii) The preferred method of encryption for laptop computers, mobile computer devices and smart devices is whole disk encryption. Mobile computer devices and smart devices which are not capable of whole disk encryption must use file/folder level encryption to encrypt all confidential and restricted information stored on the device.

c) **USB connected device (**Thumb Drive, Portable Storage Device, Smart Phones)

i) All confidential and restricted information stored on removable storage devices must be encrypted. In addition to being encrypted, removable storage devices must be stored in a locked cabinet or drawer when not in use.

ii) Removable storage devices except those used for backup purposes, which are not removed from SDMC premises, must not be used for the long-term storage of confidential and restricted information.

iii) The preferred method of encryption for removable storage devices is whole disk/device encryption. Where whole disk encryption is not possible, then file/folder level encryption must be used to encrypt all confidential and restricted information stored on the removal storage device.

Approved Encryption Algorithms and Protocols

d) **Symmetric Key Encryption Algorithms**
i) Triple Data Encryption Standard (3DES)
(1) (Minimum encryption key length of 168 bits) ii)
Advanced Encryption Standard (AES)
(1) (Minimum encryption key length of 256 bits) iii)
Blowfish
(1) (Minimum encryption key length of 256 bits)

e) **Asymmetric Key Encryption Algorithms**
i) Digital Signature Standard (DSS) ii)
Rivest, Shamir & Adelman (RSA)
iii) Elliptic Curve Digital Signature Algorithm (ECDSA)

f) **Encryption Protocols**
i) IPSec (IP Security) ii) SSL
(Secure Socket Layer) iii) SSH
(Secure Shell) iv) TLS (Transport
Layer Security)
v) S/MIME (Secure Multipurpose Internet Extension)

g) **Encryption Key Management**
i) Key management must be fully automated ii)
Private keys must be kept confidential iii) Keys in
transit and storage must be encrypted

6) Definitions:

a) **HIPAA:** Health Insurance Portability and Accountability Act of 1996

b) **Electronic Protected Health Information (ePHI):** Electronic health information or health care payment information, including demographic information collected from an individual, which identifies the individual or can be used to identify the individual. ePHI does not include students records held by educational institutions or employment records held by employers.

c) **Protected Health Information (PHI):** Information that is a subset of health information, including demographic information collected from an individual, and:

i) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and

ii) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and

iii) That identifies the individual; or iv) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

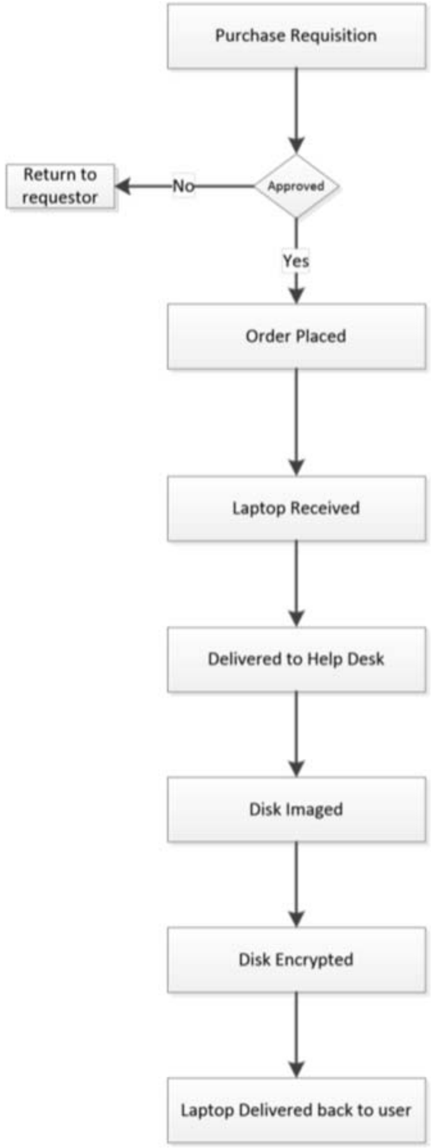
d) **Portable Device such as but not limited to:** Laptops, Tablets

e) **USB Device such as but not limited:** Thumb Drive, Portable Storage Device, Smart Phone, etc

7) Procedures:

a) New Laptop Devices

All clinical Laptops are to have whole disk encryption before being deployed to end user.



Purchase requisition

□ The assistant CIO will approve or deny all requests for purchase of new laptop computers for SUNY Downstate Medical center.

□ The requestor will place order for Laptop computer

□ The Laptop will be received either by receiving or the individual requesting Laptop

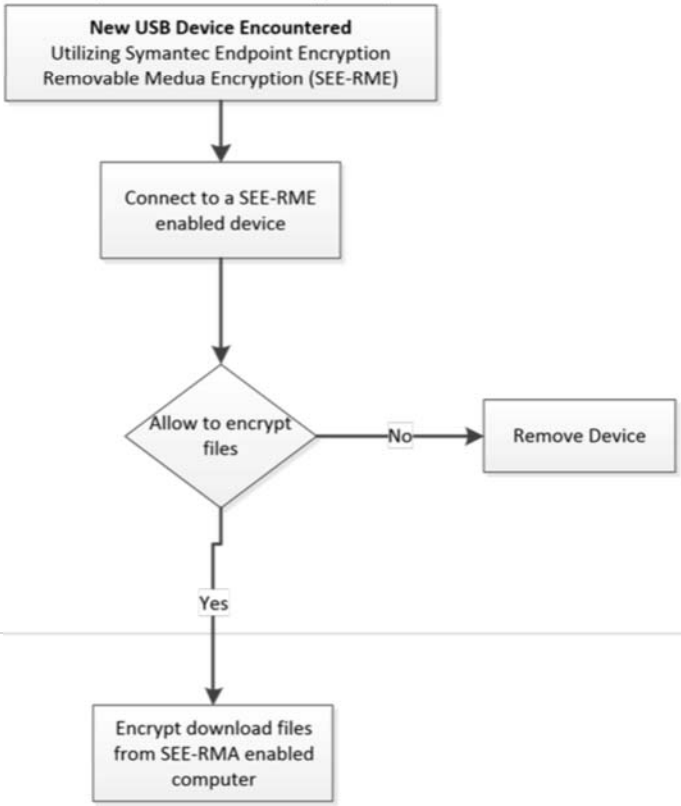
□ The new laptop must be delivered to the helpdesk

□ The help desk will install disk image

□ The imaged hard drive will be encrypted utilizing Symantec Disk Encryption

□ The new PC will be returned to the user and configured for enrollment into Symantec Disk Encryption/

9) USB Storage Devices: Thumb Drive, Portable Storage Device, Tablets, Smart Phones All USB storage devices must utilize file/folder level encryption must be used to encrypt all confidential and restricted information stored on the removal storage device.


New USB Device Encountered
Utilizing Symantec Endpoint Encryption
Removable Medua Encryption (SEE-RME)
Connect to a SEE-RME enabled device
Allow to encrypt files
No
Remove Device
Yes
Encrypt download files from SEE-RMA enabled computer

Connect device to USB port to download data

SEE-RME auto copies .exe & .dmg applications to usb storage device

All files copied from this computer to USB device is encrypted

10) Compliance and Enforcement

a) All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **SUNY DOWNSTATE MEDICAL CENTER'S** Sanction Policy.

11) Attachments: None

12) References None

Date Reviewed	Revision Required (Circe One)		Responsible Staff Name and Title