Title: **HIPAA Information, Security and Privacy Policy**	**Policy Category:** **Risk Management & Security**
Issuing Authority: **Enterprise Risk Management**	**Responsibility:** **Enterprise Risk Management**
Publication Date: **11/18/2022**	**Next Review Date:** **11/18/2025**

Printed copies are for reference only. Please refer to the electronic copy for the latest version.

Policy Statement/Background:

The purpose of this policy is to establish direction, procedures, and requirements to ensure the appropriate protection of Stony Brook University ("University") information and infrastructure systems as they relate to Protected Health Information ("PHI") and the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") regulations.

This policy is intended to emphasize for University workforce members the necessity of PHI security and privacy in the various communication and information system environments and their role in maintaining security and privacy of same. The policy will also assign specific responsibilities for the provision of PHI data and PHI security and for the security of the various infrastructure environments. This policy is also intended to conform to federal, state and local regulations and statutes affecting the security and privacy of PHI.

Scope

This policy applies to all University workforce members, including employees, students, medical staff, trainees, volunteer staff, contractors, consultants and other representatives, including those affiliated with third parties who access University Computing Systems and University Computer Network Systems which contain PHI (herein after referred to as "University workforce members"). It applies equally to all computer systems, networking systems, physical medical records (including wireless), firewalls, servers, peripheral equipment, workstations, personal computers (desktop

and portables), personal data assistants (PDA's), including wireless PDA's, within the University. Network and computer resources include PHI data, PHI printouts, PHI software (applications and databases), PHI hardware, facilities and telecommunications that permit access to PHI.

Policy:

It is the policy of the University to prohibit unauthorized access, disclosure, use, duplication, modification, diversion, destruction, storage, loss, misuse, or theft of medical (hard copy or electronic) records, information, software or hardware as relates to PHI. Any such unauthorized activities or misuse will be cause for disciplinary action to be taken to the fullest extent of the law, in accordance with university policies and collective bargaining agreements when applicable.

Definitions Access

The ability of clinical and technical users with authorization and a need to know to access systems and medical records (physical and electronic formats) which contain PHI or the ability of University workforce members that work in various areas to have contact with PHI.

Risk Management and Oversight

The University will have in place a formal structure that will govern risk management and assessment of the University PHI data management structure. This structure will have oversight of the privacy and security (hard copy and electronic) of the University PHI and communication infrastructure environment that stores or transmits such information.

Employee Responsibility Users

Users are expected to follow all policies and procedures related to PHI security and privacy of medical record data in both physical and electronic format. University workforce members will comply with policies and procedures at the University (global) and departmental (local) levels for security of printing, copying and faxing PHI, this includes transmission, viewing and distributing PHI. University workforce members are expected to not only be aware of all existing security and privacy policies, but also to comply with all future policy changes as they arise. Only authenticated University workforce members will be given access to the communication infrastructure as related to PHI in a capacity limited to meet the ability to perform their duties appropriately and with a need to know level of access only.

All University workforce members who have been determined to no longer need access to the communication infrastructure or specific areas of the network and applications will be removed from access lists, including terminated employees, employees on extended leave, retired or transferred employees with new duties and responsibilities. All University workforce members with PHI access capabilities must attend HIPAA specific training sessions, which will provide information on current policies, procedures and regulations relating to PHI security and privacy compliance.

Confidentiality

The University, in accordance with Federal and State laws, is required to protect and preserve the confidentiality of PHI. All University workforce members must sign a Workforce & Electronic Information Confidentiality Acknowledgement Statement to be granted access honoring all the legal and ethical requirements for protecting and preserving the confidentiality and privacy of patients at Student Health Services, University Hospital and the Long Island State Veterans Home (LISVH). This includes pre-employment and any subsequent additional requirements or changes in access to PHI, either for hard copy or electronic format.

Administrators/Department Heads

Administrators and Department Heads are responsible for ensuring that PHI data privacy and information security measures are being followed for their areas. They must maintain a current working knowledge of the University policies pertaining to PHI security and privacy and identify necessary process improvement changes when new policies are approved.

The Department Head is responsible for ensuring the PHI security and privacy of all department/agency data stored as either physical paper records or electronic records on departmental computer servers. Department Heads will work with the appropriate network and information security administration to ensure PHI security. The Department Head may assign responsibility to someone within the department/agency who will oversee the day-to-day implementation of the PHI security and privacy policies and procedures for their departments. Department Heads must ensure that all employees in their area of responsibility are trained in the most current University policies and procedures as related to PHI security and privacy. Department Heads will ensure that all employees under their supervision will have appropriate access to PHI and will review such on a regular basis.

Information Security Officer

The designated Information Security Officer of each University division is responsible for oversight and monitoring maintenance and compliance of the University PHI systems. This position may be assigned at the University or at divisional levels.

Privacy Officer

The Privacy Officer of each University division is responsible for overseeing the development and implementation of policies, procedures and systems for protecting the privacy of PHI maintained by that University division or its business associates that has the potential to reveal the identity of patients. This position may be assigned at the University or at divisional levels.

Security Committee

A committee will be established to monitor the electronic security structure of the University, and interpret and implement changes in applicable regulations. To further the protection of the University PHI infrastructure, the committee will consist of not only the Information Security Officers, but representatives from all local University divisions that have access or input capabilities to PHI, and any other relevant department(s). This committee will authorize appropriate audits and maintain records for compliance with this policy and University, University Hospital, Health Sciences Center and LISVH policies that relate to PHI and the security of systems.

Privacy Committee

A committee will be established to monitor HIPAA Privacy compliance and will interpret and implement changes in applicable regulations. The committee will also review new or revised health care laws, regulations and standards pertaining to the privacy of PHI, to determine whether the establishment of new policies and procedures or modification of existing policies and procedures are needed. To further the protection of PHI the committee will consist of representatives, as necessary, from all University divisions that have access or input capabilities to PHI, as well as other relevant departments. The committee will review suspected violations and/or incidents on a case-by-case basis.

Functional Requirements Authentication

The ability to authenticate the users of every University computer network and application that accesses PHI is required. No application or hardware

that prevents authentication and identification of users on the University network infrastructure will be permitted. All users on the University computer network will be authenticated by a Human Resources personnel database (i.e., PeopleSoft and/or the Medical Staff Directory). Authentication will allow access to systems with PHI by role and on a need to know basis and will be verified by a department director/manager. Access levels to systems with PHI will be managed by the appropriate System Administrator and an alternate.

Access

Access is the ability of an authenticated user to access systems with PHI. Methods of access will be by a unique user name (alternate methods such as biometrics or tokens can be used) for identifying and tracking. All passwords used by a user will consist of a minimum of eight alpha/numeric characters and will be changed on a regular basis, but not to exceed 120 days. System administrator passwords will be changed on a regular basis, but not to exceed 60 days.

Acceptable Use

The PHI communication infrastructure and physical records are the property of the University and the governance of its use are restricted to further the legitimate interests of the University. Actions and activities that directly or indirectly threaten the integrity of the University PHI communication infrastructure, including circumvention of established security mechanisms, constitutes a violation of this policy. Any violation of this acknowledgement or University policies and procedures is strictly prohibited and will be subject to disciplinary action.

Physical/Technical Security

Servers, networking equipment and other computers storing or transmitting University PHI data and physical records must be located in secured areas. Access is restricted to authorized personnel. PHI data will be backed up appropriately and tested to ensure the backup is an exact copy as per University policies. Any PHI that is on electronic or magnetic media will be controlled to prevent unauthorized access and will be destroyed in an appropriate manner as per University policies. Additional measures for the safeguarding of PHI, such as the development of individual system disaster recovery plans, firewalls, intrusion detection systems, virus and other intrusion scanning, use of UPS (Uninterruptible Power Supplies) and offsite storage of backups, will be implemented as required by HIPAA.

Authorization for Services on the Internet/Network

The Communication Infrastructure Security Committee must approve all services that will be made available on the Internet. All servers connected to the University network system must be documented appropriately. Any unauthorized servers on the University network system will be disconnected and appropriate disciplinary action will be taken. The latest encryption technology will be utilized for all University network system communications by external vendor services, business associates/partners and individuals with access to PHI.

Training/Orientation

All departments will provide appropriate staff training. The University will provide HIPAA training sessions, as needed, for all workforce members.

Updated Software

Software used on the PHI communication infrastructure will be kept current through the use of the latest version(s) that have the most current updates, service packs or "patches". New versions of software, especially operating systems, will not be supported by the University until a determination of the acceptability of the PHI security of that software is determined. University and University Hospital Information Security Administration, together with the appropriate network/client support, will review all new applications that effect PHI. System administrators will maintain a record of the most current updates, service packs or "patches".

Waste Disposal

All departments must prevent the disposal and destruction of PHI that may directly or indirectly breach PHI confidentiality. Examples include unsecured disposal of hard copies of medical records, computer media, or documents containing network IP addresses, or usernames and passwords. Disposal of sensitive documentation and storage media will follow applicable University policy.

Verbal Security Breaches/Social Engineering

All University workforce members who have access to the PHI network shall communicate sensitive information about the network only to appropriate personnel. Release of such information in any form to individuals not properly identified is a violation of this policy.

Minimum Necessary Standards

All University workforce members are expected to limit their use and disclosures of PHI. Requests for PHI should be kept to the minimum amount of information necessary to perform their duties. Each department will implement policies and procedures, identifying the persons, or groups of persons within the department who will be permitted to access and use PHI to carry out their respective duties. Departmental policies should specify what categories of PHI each person or group may access and use and under what conditions. The determination should be consistent with individual job responsibilities. For example, individuals involved in treatment may be permitted to access the entire record as needed. As a guide for assigning access levels, the following factors should be considered:

- Who may access PHI?
- Which types of PHI may be accessed?
- In the record of which patients?
- During what time period or for what activities?

There must be a specific justification for using or requesting the entire physical medical record or accessing the entire electronic medical record.

Public Viewing/Hearing

Many customary health care communications and practices play an important role in ensuring that patients receive prompt and effective health care. Due to the nature of these communications and practices, as well as the various environments in which patients receive health care services, the potential exists for PHI to be disclosed incidentally. For example, a Student Health Services, Hospital or LISVH visitor may overhear a health care provider's confidential conversation with another provider or patient. The Privacy Rule permits certain incidental uses and disclosures of PHI when the University has in place reasonable safeguards and minimum necessary policies and procedures to protect an individual's privacy. Reasonable safeguards for University workforce members include:

- Speaking quietly or talking apart from others when discussing a patient's condition with family members in semi-private patient rooms and waiting rooms;
- Isolating or locking file cabinets or records rooms;
- Isolating or screening from public view and access computer terminals, printers and fax machines containing PHI;
- Providing additional security, such as ID and passwords on computers maintaining PHI;

- Safeguarding PHI from inappropriate public viewing and hearing and refraining from discussing PHI in public areas, such as elevators or reception areas, unless doing so is necessary to providing treatment to patients; and
- Ensuring that confidential databases are exited upon leaving workstations so that PHI is not left on a computer screen where it may be viewed/accessed by individuals who are not authorized to see the information.

Incident Reporting

All reports of incidents of HIPAA PHI violations will be reported to the designated Privacy Officer. Privacy violations will be appropriately reported up the chain of command. Electronic PHI security violations will be reported to the appropriate Information Security Administration unit for the University and University Police in accordance with policy. Warnings and reports of external PHI security threats will be monitored and distributed by each University division. All hardware will be handled in accordance with incident reporting and investigation policies. All PHI violations will be properly investigated and reported.

Penalties

The University will not tolerate the intentional or unintentional breach of PHI security. Any violation of this policy or other applicable University division policy or procedure is strictly prohibited and will be subject to disciplinary action and/or dismissal and could include additional penalties in accordance with federal, state and local laws.

Definitions:

None

Contact:

Additional information about this policy is available here:

Enterprise Risk Management
180 Administration Building
Stony Brook, NY 11794
(631) 632-9500

Relevant Standards, Codes, Rules, Regulations, Statutes and Policies:

- SUNY Notice of HIPAA Privacy Practices