NOVA SOUTHEASTERN UNIVERSITY

HIPAA Security Plan:
Guidelines, Policies & Procedures

Effective April 20, 2005

Reviewed and Updated: April 20, 2007

Updated: March 29, 2012

Updated 9/29/2015

Updated August 21, 2017

Updated July 16, 2018

The Institute for Neurology Immune Medicine (NIM)

Table of Contents

Definitions

Unless otherwise provided, the definitions set forth below apply to all of the HIPAA Security Policies and Procedures.

1. Business Associate. A "Business Associate" is a person or entity, not considered to be a part of NSU's Workforce, that creates, receives, maintains, or transmits protected health information for a function, activity, or service performed on behalf of NSU. For example, a Business Associate may include service providers such as billing, practice management, cloud vendors, claims processing or administration, accounting, consulting, legal, or any other service that may involve or require the disclosure of protected health information to that person or entity.

2. Deputy Security Officer. A "Deputy Security Officer" is a designated individual by the Security Officer who will assist the Security Officer with specified tasks related to the development and implementation of the HIPAA Security Policies and Procedures.

3. Breach. "Breach" is defined as the acquisition, access, use, or disclosure of protected health information not permitted by HIPAA Privacy Rule, which compromises the security or privacy of the protected health information.

4. Electronic Media. "Electronic Media" means electronic storage media on which data is or may be recorded electronically, including, for example devices in computers (i.e. hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disc, optical disc, or digital memory card. It also includes transmission media that is used to exchange information already in electronic storage media. Transmission media may include the Internet, extranet or intranet, leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media, excluding telephone calls and paper to paper facsimiles, if the information being exchanged did not exist in electronic form immediately before the transmission.

5. Email. "Email" is a means or system for transmitting written messages electronically between terminals linked by telephone lines, cable networks, or other relays.

6. Electronic Protected Health Information. "Electronic Protected Health Information" or "EPHI" means individually identifiable health information that is either transmitted by electronic media or maintained in electronic media.

7. Encryption. "Encryption" involves the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key. For purposes of these policies, encryption must be consistent with the methods described in NIST Special Publication 800-111 which can be found at **http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-111.pdf**.

8. Health Care Component. NSU has designated itself as a hybrid entity. Meaning, NSU is an entity whose business activities include both covered and non-covered functions under HIPAA. Covered functions are certain functions performed by NSU that makes NSU a health care provider requiring compliance with HIPAA. As a result, a "Health Care Component" is a component or combination of components that perform covered functions or activities that would create a business associate relationship if the components were separate entities. Each Health Care Component will include workforce members providing health care services or providing support services to it, which requires the use of PHI.

9. HIPAA Security Rule. The "HIPAA Security Rule" refers to the regulations at 45 CFR Part 160 and Parts A and C of 45 CFR Part 164, which contain the standards for the security of electronic protected health information pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

10. Individually Identifiable Health Information. "Individually Identifiable Health Information" is information, including demographic information collected from an individual that is created or received by NSU and which relates to the past, present, or future physical or mental health or condition of an individual, provision of health

care to an individual, or the past, present or future payment for the provision of health care to an individual. Information is considered PHI where the information identifies the individual or where there is a reasonable basis to believe the information can be used to identify an individual.

11. NSU Owned. In reference to equipment, workstations, devices, or hardware/software, the term "NSU owned" shall be used to describe NSU property regardless of whether the property is owned, leased, administered, managed, or maintained by NSU, or is otherwise under the custody and control of NSU.

12. Protected Health Information. "Protected Health Information" or "PHI" means individually identifiable health information transmitted or maintained in any form or medium, including oral, written and electronic.

13. Security Officer. The Security Rule regulations require that NSU assign security responsibilities to an identified individual. The person designated by NSU as the Security Officer shall be responsible for the development and implementation of the policies and procedures required by the Security Rule.

14. Unsecured Protected Health Information. "Unsecured Protected Health Information" is protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of technology methodology specified by the Secretary of the Department of Health and Human Services in the guidance issued under section 13402(h)(2) of Public Law 111-5. Essentially, secured protected health information is encrypted or has been destroyed beyond the ability to recover (i.e. shredded).

15. User. According to the Security Rule regulations, a "User" is defined as a person with authorized access.

16. Workforce Member. "Workforce Members" shall mean employees, faculty, volunteers, students, trainees, physicians, researchers, or any other individual whose conduct in the performance of work for NSU is under the direct control of NSU whether or not they are paid by NSU or a Health Care Component.

17. Workstation. "Workstation" means an electronic computing device such as a laptop, desktop computer or any other devices, including tablet or mobile devices that perform similar functions, and electronic media stored in its immediate environment.

Policy 1
Security Management Policy and Procedure

Policy:

17.1 Risk Analysis

Risk analysis is a process that can be used to identify possible threats and vulnerabilities to the confidentiality, integrity, or availability of protected health information ("PHI"). Once the risk baseline is determined through an initial analysis, the risk management process allows for the application of policy and technology in order to reduce, mitigate, or manage the risk. Thus, a covered entity uses the risk analysis and risk management processes to identify and reduce risk to organizationally accepted levels. The acceptable level depends on a number of factors, including for example, the size, complexity, capabilities, technical infrastructure, hardware, and software security capabilities of the covered entity; the costs of security measures; and the probability and criticality of potential risks to electronic protected health information (EPHI). This includes putting in place safeguards and security measures to reasonably reduce the risk of inappropriate use or disclosure of PHI whenever Workforce Members take action.

NSU has conducted risk analyses, including a survey of all computer and information systems in order to determine where EPHI is stored, how it is transmitted, and which Workforce Members currently have access. NSU has also identified the type of information contained on each system and the impact to daily activities that would be caused by a loss of this information. It is the policy of NSU to make good faith efforts to repeat or update the risk analysis at least annually or whenever there is a significant change in the environment, including, but not limited to:

- Introduction of new systems;
- Significant upgrades to existing systems;
- Retirement or disposal of systems;
- Physical relocation of IT assets;
- Introduction of new lines of business (e.g., new clinics or other Health Care Components); or
- Reorganization of NSU's management or business structure.

Special focus will be given to any areas in which corrective actions were taken for weaknesses identified in previous risk analyses and any new or modified systems or facilities.

NSU shall maintain a person appointed as the Information Security Officer ("ISO"), also known as the "Security Officer." The Security Officer shall be responsible for the development and implementation of the security policies and procedures required by the HIPAA Security Rule. The Security Officer has the authority to designate certain individuals as "Deputy Security Officer(s)" for the purpose of assisting him/her with carrying out the responsibilities set forth below.
The Security Officer will be responsible for making good faith efforts to:

- Maintain an inventory of all systems within NSU that store, process, or transmit EPHI and a diagram of the flow of EPHI, including all software, hardware, PDCs and servers;
- Identify components of the organization that handle EPHI and the physical location of IT assets that contain EPHI and review the Hybrid Entity Designation to determine whether all such components are appropriately identified as Health Care Components and that systems are included on the inventory referenced above;
- Identify Workforce Members with information relevant to the risk analysis and include them in the process as applicable, or necessary, including, for example:
    - NSU HIPAA Privacy Officer
    - Executive Director(s) of Information Systems
    - Legal Counsel
    - VP of Human Resources
    - Facilities Maintenance
    - Representatives from affected business and clinical areas;
- Identify the criticality of the identified systems and their data;
- Identify threats and vulnerabilities of the identified systems;

- Analyze the controls that have been implemented, or are planned for implementation;
- Identify the probability that a vulnerability may be exploited;
- Identify the impact of a successful threat;
- Assess the level of risk;
- Identify additional controls to mitigate risks;
- Organize and catalog all information gathered for ease of reference for future reviews;
- Document the results of the risk analysis in a risk analysis for review, approval and finalization by legal counsel and NSU management; and,
- Ensure that documentation exists that would reasonably support the risk analysis process, which shall be a direct input to the risk management process.

17.2 Risk Management

Risk management validates the effectiveness of chosen policy and/or solutions serving to balance the protection of confidentiality, integrity and availability of EPHI with the operational needs of patient care and related health care processes. NSU recognizes the importance of the risk analysis and risk management functions. As such, it has focused time and resources to develop an effective risk management process involving individuals at all levels of the organization. Risk Management includes three (3) components:

a. Risk Analysis - the process to determine level of risk (see above 1.1)
b. Risk Mitigation - the process to decrease the determined level of risk
c. Evaluation and Assessment – the process to monitor and take action to maintain the decreased level of risk, which shall include an ongoing evaluation of security measures, in response to environmental or operational changes, that affect the security of EPHI.

The Security Officer will be responsible for:

a. Methodical evaluation and determination of processes and/or technical solutions designed to address each Security requirement, while balancing the confidentiality, integrity, and availability of PHI.
b. Managing a realistic implementation of the processes and/or technical solutions.
c. Documenting in policy and procedure form all processes/technical solutions.
d. Incorporating any necessary information in training materials
e. Managing the necessary workforce training.
f. Creating and performing on going audits or evaluations of the chosen processes and/or technical solutions in order to continually assess the effectiveness of NSU's ability to balance the confidentiality of the PHI with its integrity and availability.

Where solutions are deemed to require an expenditure of resources, it will be the responsibility of the Security Officer to gather information and present this information to the appropriate decision makers within NSU so that determinations can be made based upon the risks to the and the costs associated with mitigating these risks. Such decisions will be documented in the risk analysis documents.

17.3 Workforce Member Sanctions

All violations of the NSU HIPAA Privacy Policies or the NSU HIPAA Security Policies or breach of the HIPAA Privacy or Security Regulations will be handled in accordance with **NSU HIPAA Privacy Policy No. 14 – Sanctions**.

Where a breach or violation involves EPHI, or non-compliance with the NSU HIPAA Security Policies, the Security Officer may be asked to participate in discussions related to the appropriateness of Sanctions. In such situations, the Security Officer will be informed of the final outcome of the disciplinary decision and will be responsible for documenting the end result of any disciplinary action and/or retaining any such documentation.

17.4 Information System Activity Review

The Security Officer will determine which reports the various Health Care Components' information systems and software programs are capable of generating, including, but not limited to audit logs, access reports, and security incident tracking reports.

The Security Officer will implement procedures to regularly review records of information system activity, such as audit logs, access reports and security incident tracking reports.

17.5 Business Associate Contracts and Other Arrangements

NSU is required to assure that any Business Associate with whom it shares PHI, including electronic protected health information ("EPHI") or has PHI or EPHI created on behalf of NSU, handles the information in accordance with the HIPAA Security Rule (for electronic PHI) and the HIPAA Privacy Rule (for all PHI). In the event NSU permits an individual or entity, outside of its workforce, to create, receive, transmit or maintain EPHI on its behalf, the individual or entity is deemed to be a Business Associate of NSU. As a result, NSU must obtain satisfactory assurances that the Business Associate will properly safeguard the information. In the event of such an arrangement, all Business Associates who meet this definition will be required to sign a business associate agreement in accordance with NSU's HIPAA Privacy Policy No. 8, Business Associate Policy. Additionally, the implementation process, enforcement of the contract, and procedures outlined in the HIPAA Privacy Policy No. 8, shall be followed.

Procedure:

1. The Security Officer will work with HIPAA Security legal counsel to conduct periodic updates to the risk analysis. Reports will be marked "– Subject to Attorney Client Privilege." Final reports must be approved by HIPAA Security legal counsel and appropriate management and will be maintained by the Security Officer and HIPAA Security legal counsel.
2. The Security Officer will make good faith efforts to conduct such periodic risk analyses on an annual basis, or whenever there are material changes to clinical systems, software, hardware or the flow of EPHI.
3. The Security Officer will confer with Administration, including legal counsel, with respect to determining which security solutions may be implemented (based upon a cost/benefit analysis).
4. All Workforce Members who intend to contract with or engage the services of an individual or entity that would be deemed a Business Associate as described in this policy must comply with HIPAA Privacy Policy No. 8 to ensure that a proper written agreement is in place prior to permitting access, use of PHI, or creation of PHI on behalf of NSU, including EPHI, by the individual or entity.
5. All violations of the NSU HIPAA Privacy Policies or the NSU HIPAA Security Policies or non-compliance with the HIPAA Privacy or Security Regulations of which the Security Officer becomes aware will be handled in accordance with HIPAA Privacy Policy No. 14 – Sanctions. The Security Officer will consult with the Privacy Officer and legal counsel as appropriate.
6. The Security Officer will take all reasonable and necessary actions following the outcome of any disciplinary matter and will document the outcome and retain in accordance with NSU Record Retention guidelines but no less than six (6) years.
7. The Security Officer will be responsible for listing all reports related to information system activity review and the frequency with which each report should be run routinely, as well as any events that will trigger the running of the report.
8. The Security Officer will be responsible for setting a schedule for the routine information system activity reviews as well as maintaining all related reports for a period of at least six (6) years.
9. If the Security Officer identifies suspicious activity based upon the reports, it will be investigated, the results of such investigation documented, and appropriate actions taken.

Policy 2
Workforce Security Policy and Procedure

Policy:

2.1 Authorization and/or Supervision

It is the policy of NSU that all Workforce Members will be assigned a specific job title based upon their detailed job description. Job titles and access levels will be assigned by the administrator in the applicable Health Care Component. Access will be given to EPHI only to the extent that it is reasonable and appropriate for the individual's role and responsibilities and will be consistent with the access to paper PHI as set forth in the Minimum Necessary Rule, HIPAA Privacy Policy No. 4A, and based upon a spreadsheet maintained by the NSU Department of Clinical Information Systems ("CI").

The granting of remote access will be given special consideration and will only be granted if the Security Officer, in conjunction with the HIPAA Liaison of the Health Care Component, determines that it is reasonable and appropriate for a Workforce Member to have such access.

Workforce Members who are not authorized to access EPHI, but who have an occasional need to access EPHI, will be supervised by a designated Workforce Member(s) while accessing EPHI. The HIPAA Liaison will determine which employees should be responsible for supervising Workforce Members on such occasions.

2.2 Workforce Clearance Procedures

The Security Officer will work with legal counsel and the NSU's Human Resources Department to determine reasonable and appropriate background checks for various levels of Workforce Members requiring access to EPHI based on position and level of access.

At a minimum, NSU will make good faith efforts to ask any new Workforce Members if they have ever been disciplined for breaching security at a previous job or facility. If so, in the event the person is hired, the Office of Innovation and Information Technology ("OIIT") may review such Users' activity more frequently and intensively than others to ensure compliance with the HIPAA Security Policies.

The Office of Legal Affairs, when reviewing business associate agreements, will determine what, if any, background investigations or representations and warranties should be obtained from affiliates, vendors or other business associates.

2.3 Termination/Modification of Access Procedures

When a Workforce Member, contractor, or any individual previously entitled to access EPHI ceases to have such privileges by virtue of termination of employment at NSU or affiliation with NSU, termination or expiration of contract or through any other means by which the relationship ends (through termination, resignation, retirement, disenrollment, graduation, completion of program/work or any other means) or changes positions requiring a different level of access, Human Resources will be responsible for communicating the termination, resignation, or change to the Security Officer or a designee of the Security Officer and the following steps will be taken:

- The individual's access to all computer systems will be disabled or deleted, or altered as appropriate.

In the event of termination for any reason, Human Resources will be responsible for determining that the Workforce Member's keys, keycards, or other means of obtaining access to NSU's Health Care Components are returned and that the Workforce Member's name badge has been returned.

Human Resources is responsible for alerting the Security Officer of situations that might raise concern regarding a threat to security (for example, the Workforce Member makes threats, has a history of sabotage, or leaves under hostile circumstances). The Security Officer, with input from the HIPAA Liaison, will make a determination as to any special security measures that should be taken, such as:

- Alerting security personnel
- Changing locks on doors
- Changing key code access or passwords to gain entrance to the facility if such passwords are known to all Workforce Members

When a student is terminated from an NSU program, it is the responsibility of the faculty member responsible for supervising that student in the clinical setting to notify the Security Officer or a HIPAA Liaison as soon as the decision is made to terminate the student, so that access can be terminated immediately.

Procedure:

1. Access levels will be assigned based upon role based permissions as determined by the assigned HIPAA Liaison or designee working with the leadership of the clinical department, and will be maintained by the Clinical Informatics group and consistent with the Minimum Necessary Rule, HIPAA Privacy Policy No. 4A.
2. Business associate agreements, affiliation agreements and other similar agreements will be reviewed by legal counsel to determine whether representations related to clearance are sufficient.
3. Those Workforce Members who are not authorized to access EPHI will be supervised if they need to obtain temporary access (supervision will be provided by a designated Workforce Member deemed to be appropriate by the HIPAA Liaison as set forth above).
4. Before Workforce Members are given access to EPHI, the clearance procedures set forth in Paragraph 2.2 above shall be followed.
5. Termination procedures in Paragraph 2.3 shall be followed for all NSU employees and other Workforce Members.

Policy 3
Information Access Policy and Procedure

Policy:

3.1 Access Authorization/ Authentication

It is the policy of NSU to establish mechanisms to protect all electronic protected health information ("EPHI") from unauthorized access by password protecting all systems containing EPHI, and using other techniques if appropriate. Each Workforce Member who needs access to a system will be given a unique user name for that system, will authorize an appropriate level of access pursuant to HIPAA Workforce Security Policy and Procedure No. 2, and will be required to develop a password and comply with NSU's Enterprise Username and Password Policy.

3.2 Access Establishment and Modification

(a) Access Establishment for Workforce Members

Based on the various job duties or roles in the organization, the NSU Department of Clinical Information Systems ("CI"), in conjunction with the HIPAA Liaison where appropriate, will make certain determinations as to which Workforce Member or other individuals are authorized to access EPHI and the types of EPHI that they may access based upon job titles and job functions provided by the applicable Health Care Component.

Access will be established based on job function taking into account the "Minimum Necessary Rule" discussed in HIPAA Privacy Policy No. 4A which generally requires covered entities to take reasonable steps to limit the use or disclosure of, and requests for, protected health information to the minimum necessary to accomplish the intended purpose. Spreadsheets describing the access levels will be maintained by CI. Spreadsheets will be periodically reviewed and updated by HIPAA Liaisons with input by supervisors, as appropriate, to determine that the assigned levels are appropriate for the individuals.

(b) Remote Access

It is the policy of NSU that remote access to systems containing EPHI is strictly controlled. The Security Officer, with the assistance of the HIPAA Liaison for the applicable Health Care Component, will establish a list of each Workforce Member by job function or roles that require remote access. Any User intending to connect to departmental networks remotely (i.e., via internet, dial-in, etc.) must first obtain permission from the HIPAA Liaison who will determine whether the individual has a job function that has been approved for remote access. If there has not been a decision made with respect to the level of access permitted for a particular job function, the HIPAA Liaison will seek approval from the Security Officer.

It is the responsibility of all Users with dial-in or VPN access privileges to prevent dial-in connections to the network by unauthorized individuals attempting to gain access to Department system resources. Any Users who are granted dial-in or VPN access privileges must remain constantly aware that dial-in or VPN connections between their locations and NSU are literal extensions of NSU's network, and that they provide a potential path to NSU's most sensitive information. All dial-in or VPN Users must take every reasonable measure to protect EPHI. All precautions required for workstation security apply to Users utilizing dial-in or VPN access (i.e., Users must treat their remote access locations as though they were on-site at NSU and take appropriate security precautions).

(c) Wireless Access

Access to NSU resources (systems containing EPHI) via the wireless network is prohibited with the exception of connections approved for remote access use (see above) and must also be in accordance with HIPAA Security Mobile Device Policy No. 15. This applies to all wireless data communication devices (e.g., personal computers, cellular phones, PDAs, tablets etc.) connected to any of NSU's internal networks, including any form of wireless communication device capable of transmitting packet data. The only authorized wireless connection to NSU resources that contain EPHI shall be through secured, encrypted wireless networks as approved by the Security Officer.

(d) Student Access

Students will be provided with access to clinical systems including remote access during the time period that the student is participating in clinical training at NSU to the extent that such access is necessary for the training program. This access will be terminated automatically when the student graduates from or disenrolls from NSU in accordance with the termination procedures in NSU HIPAA Security Policy 2.3.

(e) Fictitious Charts for Training Purposes

Where appropriate, NSU educators may set up fictitious medical records or training applications for students or other trainees to use to learn documentation or computer skills. Such medical records will not be based on real patients or names and to avoid any appearance of impropriety will not contain names of real persons, (e.g., celebrity names).

3.3 Workforce Responsibilities Related to Access

All Workforce Members and others given access are responsible for complying with the access levels and restrictions that apply to their positions and may only seek access to additional EPHI if granted permission by the HIPAA Liaison. Users are not permitted to access specific EPHI, even though they may be capable of doing so, which is beyond their authority. For example, a User who is given access to a system to review a specific patient's electronic record may not use that access to review other patients' records. The HIPAA Liaison must notify the CI of any necessary changes, temporary or otherwise, in User's access levels.

Procedure:

1. CI will maintain documentation of the level of access granted to Workforce Members, taking into account each individual's job title or function as forth in the Minimum Necessary Policy, HIPAA Privacy Policy No. 4A. All Workforce Members will be responsible for notifying the HIPAA Liaison of the Health Care Component if they feel that they have a higher or lower level of access than is necessary to perform their job, and the HIPAA Liaison may consult with the Security Officer if there is any doubt as to the appropriateness of the access level requested.
2. HIPAA Liaisons will be responsible for approving requests for remote access. The Security Officer or his or her designee will maintain a list of Workforce Members with remote access.
3. Workforce Members with remote access are responsible for complying with all NSU policies and procedures, including HIPAA Privacy and Security Policies and Procedures, while accessing information remotely.

Policy 4
Security Awareness and Training Policy and Procedure

Policy:

4.1 Security Training

The NSU Security Officer coordinates the following HIPAA Security Training Program:

- Within approximately 30 days of starting work and before being provided access to PHI, all new Workforce Members, including new hires and/or students rotating in a Health Care Component are provided basic security training, including:
  - Identification and contact information for the NSU HIPAA Security Officer and/or Deputy Security Officers, the HIPAA Liaison of their Health Care Component, and the OIIT;
  - General security safeguards that have been enacted by NSU including rules on passwords, rules on email and the internet, and log-in monitoring;
  - Rules on remote accessing of EPHI;
  - Discussion of how to protect against viruses, malicious software and other threats to the security and integrity of EPHI;
  - Authorized users and limitations on accessing and disclosing PHI;
  - How to report security incidents, including breaches and concerns regarding security; and
  - The HIPAA Confidentiality and Need to Know Agreement (HIPAA Privacy Forms, Exhibit 19).
- The NSU HIPAA Security Officer may also provide annual re-education sessions for certain, existing Workforce Members that covers HIPAA security and privacy education and updates; for example, whenever environmental or operational changes affect the security of EPHI, such as new or updated policies or procedures, new or updated software or hardware, new security technology; or changes to the HIPAA Security Rule. NSU, at its option, may incorporate this training with other yearly training such as general compliance.

4.2 Security Reminders

Workforce Members who receive HIPAA Privacy training pursuant to NSU HIPAA Privacy Policy No. 13 will also receive HIPAA Security training. In addition to this formal training, periodic security reminders will be communicated by the Security Officer, Deputy Security Officers or HIPAA Liaison. Examples of ways in which security reminders may be communicated, include, but are not limited to:

- Security newsletters
- Security reminders to HIPAA Liaisons to be communicated during clinic or departmental meetings
- Email reminders

The topics to be addressed in these communications will be determined by the Security Officer. The issues that the Security Officer may consider when determining appropriate content for reminders should include, without limitation, the following:

- Security issues brought to the attention of the Security Officer (such as non-compliance with the security policies)
- Questions raised by staff
- New guidance from the government regarding steps necessary for compliance with the HIPAA Security Rule
- New policies and procedures implemented by the practice

If HIPAA Liaisons become aware of topics on which their Health Care Component needs reminders or extra training, the HIPAA Liaison will notify the Security Officer who will arrange for or conduct such training.

4.3 Protection from Malicious Software

It is the policy of NSU that every NSU-owned Workstation has anti-virus software installed to constantly monitor and safeguard the Workstation against malicious software. If a User suspects that a NSU-owned Workstation does not have anti-virus software installed or activated, the Security Officer, a HIPAA Liaison, or a Security Deputy should be notified immediately. It is the Security Officer's responsibility to make good faith efforts to work with all HIPAA Liaisons to confirm that all NSU-owned Workstations have appropriate, updated, active anti-virus software. Anti-virus software shall be updated at least weekly (if not as soon as updates become available) to ensure that the library of detectable malicious software is as complete as possible as new viruses appear every day. Any computing device that is found to have security vulnerabilities or other software deficiencies cannot be used to access EPHI until the problems are resolved and the computing device is cleared by the Security Officer.

As part of NSU's efforts to protect the security and integrity of EPHI, all users are required to comply with the following guidelines:

- Do not open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your deleted items folder.
- Delete spam, chain, and other junk email without forwarding it.
- Do not download files from unknown or suspicious sources.
- Avoid direct disk sharing with read/write access unless there is absolutely a business requirement to do so. If storage media is shared between Workstations, anti-virus software should scan the media before allowing its contents to be accessed by the NSU-owned Workstation. Unless the OIT instructs otherwise, Users should assume that portable storage media are not automatically scanned by each NSU owned-Workstation.
- If system software (such as lab programs, etc.) conflicts with anti-virus software, notify the HIPAA Liaison, who will in turn consult with the OIIT to develop an appropriate solution.

In addition, all Workforce Members are required to adhere to the following guidelines:

- Individuals are not permitted to add, remove or download software programs to any NSU-owned Workstation without first obtaining the permission of the Chief Information Officer ("CIO") and/or Security Officer, in accordance with the NSU Organization Software Policy.
- Individuals are not permitted to open attachments on NSU-owned Workstations associated with personal e-mail (for example, jokes, video clips, links, etc.) since these types of attachments carry significant risk of spreading viruses and other malicious software.
- Individuals should not open e-mail attachments from individuals or organizations who they do not know.
- Individuals are expected to alert the Security Officer if they receive suspicious or unusual e-mail.
- Individuals are not permitted to disable anti-virus or similar software installed on any NSU owned Workstation.
- Individuals must notify the Strategic Support Services (SSS) group at extension 20777 or by emailing SSS at sss@nova.edu in the event they are unable to login to a program or if they receive an unusual error message when trying to login.
- Any computing device that is found to have security vulnerabilities or other software deficiencies cannot be used to access EPHI until the problems are resolved and the computing device is cleared by Security Officer.

4.4 Log-in Monitoring

It is the policy of NSU for Workforce Members to monitor log-in attempts and to report any log-in discrepancies as a potential security incident (see HIPAA Security Policy No. 5, Security Incidents). The Security Officer will review the capabilities of each system that contains EPHI and will implement log-in monitoring and reporting procedures and safeguards based on the capabilities of the system. Such safeguards may include, for example:

- Notification displays upon log-in stating that the system must only be accessed by an authorized NSU Workforce Member
- Review and removal of any help messages that could assist an unauthorized user
- Implement limitations on the number of unsuccessful log-in attempts
- Removal of statements that tell which part of the log-in information is correct or incorrect if there is an error
- Removal of identifying information that is visible prior to successfully completing the log-in process, information system or application
- Limitations on the time allowed for the log-in procedure
- Record and limit number of failed log-in attempts with lockout periods
- Displaying the date and time of the previous successful login by the Workforce Member after successful login

If Workforce Members are unable to log-in to a system for any reason, or encounter anything suspicious during the login process, they shall immediately contact the HIPAA Liaison and the HIPAA Security Officer or a designated Deputy Security Officer.

4.5 Password Management

Any Workforce Member who is provided with a password to access EPHI through one of NSU's systems will be required to comply with the NSU Enterprise Username and Password Policy.

Procedure:

1. The Security Officer will work with those Workforce Members at NSU who are responsible for hiring new Workforce Members and providing access to students to set up a training program.
2. The Security Officer will be responsible for establishing content and timing of initial security training and security reminders.
3. Workforce Members will be responsible for reviewing the guidelines set forth in Paragraph 4.3 above and any new policies that are developed with respect to malicious software.
4. All Workforce Members will be responsible for alerting the Security Officer of any log-in failures in accordance with Paragraph 4.4 above.
5. OIIT will be responsible for loading anti-virus software on all NSU-owned Workstations. All Workforce Members are responsible for notifying OIIT if there is a problem with their anti-virus software or it is lacking.
6. All Workforce Members are responsible for complying with NSU Enterprise Username and Password Policy, pursuant to Paragraph 4.5, above.

Policy 5
Security Incidents Policy and Procedure

Policy:

5.1 Identification and Reporting of Security Incidents

Pursuant to the HIPAA Security Rule, a Security Incident is defined as "the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system."

The Security Officer will implement procedures for detecting and responding to known or suspected Security Incidents that may affect systems that maintain or transmit EPHI.

Certain Security Incidents may be detected by Workforce Members and should be immediately reported to the Security Officer by calling the Security Officer at (954) 262-0448 or the HIPAA Security/IT Security Team Hotline (954) 262-0448. Examples of Security Incidents that must be identified and reported include, without limitation:

- Passwords that have been lost, stolen, shared, or used by persons other than the individual to whom the password was assigned
- Introduction of viruses, worms, Trojan horses or other malicious software into the organization's computer systems
- Unauthorized access to networks, computer systems, or facilities/equipment rooms housing the computer systems, including physical break-ins leading to the theft of media containing EPHI
- Destruction of electronic protected health information
- Failure to terminate the account of a former Workforce Member that is then used by an unauthorized user to access information systems with EPHI
- Complaints from patients that relate to security

In order to assess the security of systems, and to the extent consistent with current technological capabilities of the systems, the Security Officer will work with the OIIT to implement mechanisms regarding tracking failed log-in attempts. Any User who becomes aware of failed log-in attempts of a suspicious nature must report immediately to the OIIT. Individuals must be aware that the Department reserves the right to monitor system access and activity of all system Users.

5.2 Documentation of Security Incident and Response

When the Security Officer receives a report of a Security Incident, it will be the responsibility of the Security Officer to document the Security Incident, the outcome of the investigation and NSU's response to the Security Incident. The Security Officer will be responsible for maintaining this documentation.

An individual may report a known or suspected Security Incident directly to the Security Officer or may call the HIPAA Security Hotline at 954-262-0448.

The Security Officer will also maintain documentation of any Security Incidents detected.

5.3 Breach Notification

A breach is the acquisition, access, use, or disclosure of PHI in a manner not permitted under the HIPAA Privacy Rule, which compromises the security or privacy of the PHI, excluding certain exceptions identified under the Breach Notification Rule.

When a Security Incident involves an unauthorized use or disclosure of EPHI, the Security Incident will be treated as a suspected breach of EPHI and will be handled in accordance with the HIPAA Privacy Policy No. 10, Breach Notification Policy and Procedure, in coordination with the NSU HIPAA Privacy Officer.

All complaints, reports, or discovery of potential breaches of EPHI shall be immediately reported to the HIPAA Security Officer. Please note: The HIPAA Breach Notification Rule requires NSU to notify affected individuals in the event of a breach without unreasonable delay and in no case later than 60 days following the discovery of a breach. If applicable, other federal or state law may require that NSU provide notification of a breach to affected individuals, the appropriate governmental agency, or other entities within a shorter timeframe. For these reasons, complaints or reports of a potential breach of EPHI must be immediately reported to the HIPAA Security Officer upon discovery. Delay in submitting complaints or reports regarding potential breaches or security incidents could result in significant regulatory penalties against NSU and may result in disciplinary action against Workforce Members involved.

5.4 Mitigation

The Security Officer will make recommendations regarding the steps that should be taken, if any, to mitigate harm as a result of a confirmed security breach. The NSU HIPAA Security Officer may consult with others in the field or expert consultants in addressing potential mitigation options and, depending on the severity of the issue, may coordinate with legal counsel with regard to the matter prior to making any final recommendations or taking any actions. The steps taken will be documented and retained by the Security Officer.

5.5 Non-retaliation

It is the policy of NSU that retaliation against those who report or complain about security breaches or incidents is strictly prohibited.

Procedure:

1. The Security Officer will be responsible for implementing and overseeing Security Incident detection efforts.
2. All Workforce Members will be responsible for understanding the definition of a "Security Incident" and a "Breach" and their responsibility for promptly reporting such Security Incidents and Breaches involving EPHI to the Security Officer.
3. The Security Officer will be responsible for documenting all Security Incidents, including breaches of EPHI, the results of investigations, the response and steps taken to reduce harmful effects. The Security Officer will be responsible for maintaining such documentation for at least six (6) years, unless there is an ongoing investigation or litigation, in which case the Security Officer may be asked by risk management or legal counsel to retain the information for a longer time period.
4. The Security Officer will be responsible for determining what, if any, steps can be taken to mitigate the harmful effects of the breach. The Security Officer will also be responsible for taking such steps either personally or through delegation and documenting the steps taken. All documentation related to mitigation of harmful effects of a breach must be maintained for at least six (6) years.
5. The HIPAA Privacy Policy No. 10, Breach Notification Policy and Procedure, will be followed when there is a potential or actual breach of EPHI.

Policy 6
Contingency Plan Policy and Procedure

Policy:

6.1 Applications and Data Criticality Analysis

The Security Officer, with assistance from the HIPAA Liaison from the Health Care Component, will be responsible for identifying software applications (data applications that store, maintain, or transmit EPHI) and determining which is considered "critical" for NSU operations based upon the needs of the Health Care Component, in order to prioritize for data backup, disaster recovery, and emergency operations plans.

Criticality will be determined on both a long term and a short term basis. Information is critical on a short term basis if daily operations could not be continued without this information. Information is critical on a long term basis if the Health Care Component would have liability exposure if the information was permanently lost or unavailable for a long term period.

6.2 Data Backup, Business Continuity and Disaster Recovery Plan

Data, including all PHI, will be backed up based upon a schedule determined by OIIT with input from the Security Officer where appropriate and shall take into account the criticality of the data stored on each information system.

The Security Officer will work with Deputy Security Officers, designated OIIT personnel and clinical leadership to, update and implement a Business Continuity and/or Disaster Recovery Plan.

In the event of a disaster that may impact NSU's systems containing EPHI, the Security Officer, Deputy Security Officers and other designees from OIIT will be responsible for overseeing the recovery of data and restoration of operations as set forth in the Disaster Recovery Plan.

6.3 Emergency Mode Operation Plan

The data that is deemed to be most critical to daily operations will be restored first (to the extent that it does not impair the potential for recovery of information that is critical from a long term perspective). The Security Officer shall make and test a plan to continue operations while information systems and data are being restored.

Alternative procedures will be followed during the time period while systems are down.

6.4 Testing and Revision Procedures

The Security Officer will meet with the Deputy Security Officers and other individuals from OIIT periodically to determine whether personnel understand their roles for restoring data and emergency mode operations as set forth in the Business Continuity and/or Disaster Recovery Plan. The Business Continuity and/or Disaster Recovery Plan will be tested periodically by the Security Officer with the assistance of Deputy Security Officers and OIIT. Testing methods will be determined in a manner that will provide the least disruption to daily operations while still allowing the Security Officer and others to discover potential flaws in the plan.

Procedure:

1. The Security Officer, with the assistance of HIPAA Liaisons from Health Care Components, will identify software applications that store, maintain or transmit EPHI and determine the criticality of same for data backup, disaster recovery, and emergency operations purposes.
2. The Security Officer will take responsibility for documenting and implementing the Business Continuity and/or Disaster Recovery Plan.
3. The Security Officer will make good faith efforts to assemble appropriate personnel including Deputy Security Officers and designated individuals from OIIT to test the Business Continuity and/or Disaster Recovery Plan on a periodic basis, and to make revisions to such plans as necessary.

Policy 7
Facility Access Controls Policy and Procedure

Policy:

7.1 Contingency Operations

In the event of a disaster, certain individuals within a Health Care Component will require access to the facility to minimize losses and restore data. A list of individuals, as well as procedures for gaining access to the buildings and/or facilities as necessary for restoring data will be included in the Business Continuity and/or Disaster Recovery Plan as set forth in HIPAA Security Contingency Plan Policy and Procedure No. 6.

7.2 Facility Security Plan/Access Control and Validation

OIIT will maintain lists of individuals who are permitted access to areas where sensitive data is housed (e.g., the data center). An individual's level of access to such facilities will be determined based upon the individual's role or function within the Health Care Component. The Security Officer will regularly review this list to determine whether the access is appropriate and the list is up to date. If an individual with special access to sensitive data is terminated or ceases to be affiliated with NSU, the Security Officer will work with OIIT and the maintenance department to determine whether special modifications are required (e.g., locks changed, etc.).

Lists of individuals with special access to the facilities of Health Care Components (e.g., with after-hours access) will be maintained by each Health Care Component's HIPAA Liaison. If a Workforce Member with special access to the facility is terminated or ceases to be affiliated with NSU, the HIPAA Liaison must take steps to ensure that keys or key cards are obtained prior to termination or keys and codes changed, if deemed necessary.

NSU has a Public Safety Department that protects the physical security of the Health Care Components that are part of the NSU Campus. All Workforce Members of NSU Health Care Components are expected to wear a name badge at all times.

The Security Officer shall implement other facility safeguards to be in place during the activation of a Restoration Plan, Disaster Recovery Plan, or Emergency Mode Operations Plan, as appropriate.

7.3 Visitor Control

Visitors to the data center will be monitored via camera and will be required to sign a visitor log, and will only be provided entry if the purpose and process of the visit is within parameters set by the Security Officer.

Access points to areas with access to EPHI housed within Health Care Components will be locked or monitored. All visitors (e.g., drug reps, repairmen, etc.) will be required to sign a visitor sign in sheet and will be given a visitor badge when present in a Health Care Component. These individuals will not be permitted to have access to EPHI. Any Workforce Member witnessing a visitor attempting to gain access to EPHI should immediately report such activity to the HIPAA Liaison and HIPAA Security Officer.

7.4 Maintenance Records

HIPAA Liaisons will be responsible for overseeing documentation of any maintenance that is performed on the Health Care Components' premises that would relate to security of the Health Care Components, such as repair or replacement of doors, windows, walls or locks.

Procedure:

1. OIIT will maintain lists of individuals permitted access to the data center and other areas where sensitive data is housed.
2. The HIPAA Liaison of each Health Care Component will maintain a list of individuals who require after-hours access and will monitor the termination of such employees.
3. The data center will be monitored via camera and a log of visitors will be kept.
4. All Workforce Members will be trained on appropriate methods of supervising visitors as set forth in this policy. The HIPAA Liaison will monitor compliance with this policy.
5. If the HIPAA Liaison thinks that a door, window or lock poses a Security Risk, the HIPAA Liaison will be responsible for contacting maintenance to address such issue and will document steps taken.
6. HIPAA Liaisons will be responsible for documenting any maintenance issues reported or corrected that would impact the physical security of a Health Care Component.

Policy 8
Workstation Use and Security Policy and Procedure

Policy:

It is the policy of NSU that all Users of computer systems are required to comply with the NSU Acceptable Use of Computing Resources Policy. In addition, any Workforce Member with access to EPHI must comply with the following safeguards set forth below.

The following general rules are intended to safeguard both the integrity and availability of NSU's computer network. They apply to every person that is authorized to access the network.

- Individuals who access systems with EPHI must do so through a unique user ID in accordance with HIPAA Security Information Access Policy and Procedure No. 3 and must set up a password in accordance with the NSU Enterprise Username and Password Policy.
- Individuals are not permitted to add, remove or download software programs to any NSU-owned Workstation without first obtaining the permission of the Chief Information Officer ("CIO") and/or the HIPAA Security Officer, in accordance with the NSU Organization Software Policy.
- Individuals are not permitted to open attachments on NSU-owned Workstations associated with personal email (for example, jokes, video clips, links, etc.) since these types of attachments carry significant risk of spreading viruses and other malicious software.
- Individuals should not open e-mail attachments from individuals or organizations who they do not know.
- Individuals are expected to alert the HIPAA Security Officer immediately if they receive suspicious or unusual email.
- Individuals are not permitted to disable anti-virus or similar software installed on any NSU-owned Workstation.
- Individuals must notify the NSU Strategic Support Services ("SSS") group by contacting them at extension 20777 or by emailing SSS at sss@nova.edu in the event they are unable to login to a program or if they receive an unusual error message when trying to login.
- If individuals have portable NSU-owned Workstations such as laptops or smart phones, or personally owned devices that are used to access NSU-related EPHI, they must comply with the NSU HIPAA Security Mobile Device Policy and Procedure No. 15.
- To the extent reasonable, individuals utilizing NSU-owned Workstations in areas where visitors and others may see the screen should turn or relocate the screen or use auxiliary equipment such as a screen protector to minimize unauthorized observation of EPHI.
- Individuals should not eat or drink at NSU-owned computer Workstations.
- Individuals should log off before leaving the Workstation for an extended period of time.
- Unless the NSU HIPAA Security Officer has granted a specific documented exception for patient care or other valid reasons, each NSU-owned Workstation should have a screen saver enabled that will automatically activate and require a password before further use if the Workstation is idle for more than ten (10) minutes.
- Individuals are responsible for reporting any Security Incidents of which they become aware to the HIPAA Security Officer in accordance with HIPAA Security Incidents Policy and Procedure No. 5.
- Individuals are responsible for password-protecting any NSU-owned or personally owned Workstation, laptop, smart phone or other mobile device that is used to access EPHI in accordance with the NSU Enterprise Username and Password Policy and the NSU Security Mobile Device Policy and Procedure No. 15.

- Any computing device that is found to have security vulnerabilities or other software deficiencies cannot be used to access EPHI until the problems are resolved and the computing device is cleared by the Security Officer.
- Individuals who have been granted remote use will not store EPHI on a personally owned device and will not leave a Workstation or mobile device unattended if they are logged into an NSU system.
- Individuals may not store EPHI in cloud storage services such as Dropbox, SkyDrive, or iCloud, unless they have received prior approval from the Security Officer as set forth in Cloud Storage Policy No. 14.

Procedure:

1. Workstation use will be included in HIPAA Security Training and will be the topic of security reminders where deemed necessary by the Security Officer.
2. The HIPAA Liaison will be responsible for observing Workstation use within the Health Care Component, retraining Workforce Members as necessary, and reporting issues to the Security Officer or Deputy Security Officer.

Policy 9
Device and Media Controls Policy and Procedure

Policy:

9.1 Disposal of Electronic Media, Data Backup and Storage

It is the policy of NSU that the following procedures must be undertaken in the event of disposal of computer hard drives, devices in computers, systems or removable/transportable media containing EPHI:

- All disks, tapes, CDs, USB thumb drives and other portable storage media that may contain EPHI should be destroyed or erased prior to disposal, in such a manner rendering the media unusable and/or inaccessible;
- When media are disposed of, the Deputy Security Officer is responsible for consulting with the Security Officer to determine the best manner in which to destroy or erase EPHI;
- Prior to erasing any media, a duplicate copy should be made of any EPHI that the Deputy Security Officer in consultation with the Health Care Component determines should be retained; and
- Where an outside vendor provides disposal services, a certificate of destruction that verifies an approved disposal method(s) by OIIT was used by outside vendor shall be received and maintained by OIIT.
- Any leased devices with media (e.g. copier or fax machines) must have its media erased or destroyed prior to being returned.

9.2 Media Re-Use

Electronic media is defined by the regulations as electronic storage media on which data is or may be recorded electronically, devices in computers (hard drives) and any removable or transportable digital memory medium like magnetic tape or disk, optical disk, or digital memory card. Before re-using, donating, selling, or disposing of used electronic media, all EPHI previously stored on such media must be properly removed.

Thumb Drives or other types of removable/transportable storage devices that can be reused must be encrypted with approved methods prior to reuse. While in use, such storage devices must be encrypted in accordance with the NSU Mobile Device Security Policy No. 15.

It is the policy of NSU that any CDs or DVDs containing EPHI that are no longer needed must be destroyed according to Department of Defense Standards, and pursuant to Paragraph 9.1, above.

9.3 Offsite Use of Media

Videotapes, DVD, audio or video files and similar media containing EPHI must not be removed from NSU without written authorization from the Security Officer or Deputy Security Officer and only after the Security Officer or Deputy Security Officer has determined that such removal is being accomplished in compliance with the HIPAA Privacy Regulations. After obtaining such permission from the HIPAA Privacy Officer, all media must be signed out in a log-book maintained by the Security Officer and persons who have received authorization to remove media containing EPHI must sign an acknowledgment that the media will be kept secure and private. Any media that contains data such as data DVDs or CDs must be transferred to a format that is encrypted in accordance with the NSU Mobile Device Security Policy and Procedure No. 15.

Individuals may not store EPHI in cloud storage services such as Dropbox, SkyDrive, or iCloud unless they have received approval from the Security Officer as set forth in the Cloud Storage Policy No. 14.

9.4 Accountability

As part of the risk management process, the Security Officer will work with OIIT to maintain an inventory of all Workstations within NSU and will document the removal of any Workstation. OIIT will also maintain an inventory of all NSU-owned portable devices, such as laptops or tablets. Where possible, serial numbers, or other identifying characteristics will be recorded to differentiate such devices from other similar devices. The HIPAA Liaison for each Health

Care Component will be responsible for keeping a log of any portable media, such as USB memory sticks that are used to transfer, transport or store EPHI from the Health Care Component and will identify individuals who are responsible for safeguarding that portable media.

9.5 Data Backup and Storage

The Security Officer shall create and implement procedures to assure that a retrievable, exact copy of EPHI is created, when needed, before movement of equipment.

Procedure:

1. All Workforce Members will receive information related to appropriate disposal of EPHI in their HIPAA Security training.
2. HIPAA Liaisons will be responsible for observing appropriate procedures within their Health Care Component.
3. The Security Officer, with the assistance of Security Deputies and the OIIT, will make arrangements for disposal of hard drives and other equipment containing EPHI and may use outside vendors.
4. Where outside vendors are used, the OIIT Department will retain certificates of destruction to verify proper destruction/deletion of EPHI.
5. Media that is reused or used offsite must comply with the NSU Mobile Device Security Policy and Procedure No. 15, where applicable.

Policy 10
Technical Access Control Policy and Procedure

Policy:

10.1 Unique User Identification Policy

Each Workforce Member in a Health Care Component who is authorized to access EPHI will be assigned a unique username for the various systems containing EPHI or that allow access to EPHI. Assigned usernames may not be changed without the approval and assistance of the Security Officer, an assigned Deputy Security Officer or other Designee of the Security Officer.

Passwords are used for various purposes at NSU. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins. Users must develop and update passwords in accordance with the NSU Enterprise Username and Password Policy.

10.2 Emergency Access Procedure

Workforce Members who have not been granted access to EPHI, but who may occasionally need access, or who may require access during emergencies, should contact the HIPAA Liaison for their Health Care Component or a designated Deputy Security Officer. The Deputy Security Officer will confirm the need with appropriate management of the Health Care Component to verify that the requested access is necessary.

Clinical Informatics, upon request from clinical leadership, will have the ability to generate a username and password for limited temporary use. Whenever granting emergency access, special consideration should be given to the level of access actually needed by a User and precautions taken to prevent Users from accessing EPHI not necessary for their job functions. Whenever possible, Users requiring emergency access should be granted the lowest level of access possible that will allow them to perform their job functions. If it is not possible to limit access in this way during emergencies, the HIPAA Liaison, in consultation with the Security Officer, should determine whether alternatives exist to protect EPHI, including assigning a different User to a required task who has the clearance to access appropriate EPHI levels.

Any Users who access or attempt to access EPHI beyond their clearance levels will be subject to disciplinary action.

10.3 Automatic Logoff

All individuals with access to NSU systems will receive awareness training of the fact that logging into a NSU-owned Workstation using an appropriate username and password creates an open doorway to NSU's systems. Accordingly, it is the policy of the NSU that all Users remain responsible for their NSU-owned Workstations whenever they leave them unattended. As a general practice, Users should log off the system they are working on when their Workstation is to be left unattended. However, there may be times when Users may inadvertently forget, or may not have time, to log off a Workstation. Therefore, unless an individual or Health Care Component has received a specific documented exception based upon patient care needs and low risk of access, each NSU-owned Workstation should have a screen saver enabled that will automatically activate and require a password before further use if the workstation is idle for more than a certain period of time as determined appropriate by the Security Officer based upon the environment where the Workstation is being used. Generally, the timeframe will be ten (10) minutes, but this may be shorter as deemed appropriate by the Security Officer. For example, screen savers on NSU-owned Workstations that are in the most publicly accessible environments may be set to activate after 60 seconds of inactivity.
It is the policy of NSU that OIIT will periodically confirm that the screen saver features on each NSU-owned Workstation is active and set to work after the assigned period of inactivity. Users intentionally disabling these features, or who lengthen the period of in activity required to trigger the screen saver without approval of the Security Officer, will be subject to disciplinary action.

Workforce Members who feel that they have a need for longer or shorter duration, or to disable the screen saver for patient care or other legitimate reasons, should request such extension or waiver from the HIPAA Liaison for the Health Care Component, who must consult with and seek written approval from the Security Officer or Deputy Security Officer.

10.4 Encryption and Decryption

It is the policy of NSU that all data in motion and at rest will be encrypted where NSU has the current resources to encrypt such data (e.g., where settings can be changed with regard to existing software). In situations where NSU requires additional technology or other resources to encrypt data, then NSU will analyze options as part of the risk management process and will develop an IT strategy for managing identified risks. If encryption is not deemed reasonable, the Security Officer will document the reasons why and what compensating controls are in place to provide similar protections if reasonable and appropriate.

For mobile devices, all Workforce Members and any other individuals who access NSU-related EPHI must comply with the NSU Mobile Device Security Policy and Procedure No. 15.

For email communications, NSU will require all Workforce Members to comply with the NSU HIPAA Security Policy No. 13A, Electronic Mail Containing PHI and OIIT will install and implement technology for Workforce Members as necessary to allow Workforce Members to comply with that policy.

10.5 Firewalls

To oversee that NSU's systems containing EPHI are appropriately secured, the following policies and procedures apply:

- All systems and applications containing EPHI that are accessible outside of NSU must have perimeter security and access control with a firewall approved by the Security Officer.
- Firewalls must be configured to support the following minimum requirements:
    - Limit network access to only authorized Workforce Members and entities (e.g., Business Associates);
    - Limit network access to only legitimate or established connections (an established connection is return traffic in response to an application request submitted from within the secure network);
    - Console and other management ports must be appropriately secured or disabled;
    - Mechanisms must be present to log failed access attempts; and
    - Servers and other devices containing firewalls must be located in a physically secure environment allowing access to only necessary users (i.e., those people that must have access).

Procedure:

1. For all systems that can be used to access EPHI, Users will be given a unique login and will be required to develop a password that complies with the NSU Enterprise Username and Password Policy.
2. The Security Officer, a Security Deputy, or other Designee of the Security Officer may authorize the use of a temporary login in situations where an individual needs emergency access.
3. All Workstations, unless there is a documented exception, must incorporate automatic logoff or an automatic screensaver. The appropriate timeframe for the screensaver or automatic logoff will be determined by the Security Officer or a Security Deputy and will be dependent on the location of the Workstation.
4. Data at rest and in motion will be encrypted as determined feasible and necessary by the Office of Innovation and Information Technology (OIIT). Emails containing PHI will be encrypted in accordance with the NSU Electronic Mail Containing EPHI Policy No. 13A. Mobile Devices will be encrypted in accordance with the NSU Mobile Device Security Policy and Procedure No. 15.
5. OIIT will be responsible for configuring firewalls in accordance with this policy.

Policy 11
Audit Control Policy and Procedure

Policy:

It is the policy of NSU to periodically review User activity in order to monitor NSU systems for security issues. Information systems used to access EPHI shall have logging facilities in operation that record events and persons accessing EPHI. These logs shall be retained on a schedule set by the Security Officer to assure their availability for reviews of system activity as described above.

Procedure:

- With regard to the computer patient demographic and billing system, the Security Officer, with assistance of the HIPAA Liaisons for each NSU Health Care Component, will maintain a list of all Users within the NSU Health Care Components using the system who have access to the system, including the privileges based on job title. The list is reviewed and updated periodically and whenever there is a change in staff or change in position of a Workforce Member.
- The Security Officer or Deputy Security Officer may periodically select Users on a random basis and review those Users' activity to determine whether they are acting in compliance with these Security Policies and within the limitations of their access authority. Violations will be handled in accordance with the HIPAA Privacy Policy No. 14 – Sanctions (see Security Management Policy and Procedure 1.3, Workforce Member Sanctions).
- The Security Officer may periodically conduct selective, focused audits to system operations, including analysis of logs, without respect to specific Users to determine that security measures are in place and performing as intended.
- The Security Officer will, whenever technically possible, maintain any reports or logbook information generated by the audits on a separate system accessible only by OIIT, the Security Officer and, at the discretion of the Security Officer, the HIPAA Liaison.
- At each network log-in, Users should receive a notice that their activity is subject to administrative monitoring and that they should have no expectation of privacy.
- In reviewing network activity, OIIT may look for, among other things:
    - Account creations/deletions;
    - High volumes of unsuccessful log-in attempts;
    - Unusually high Internet gateway activity;
    - Unusually high volumes of database access or file creation, modification, or deletion;
    - Unusually high access records for specific accounts;
    - Inappropriate or unauthorized network use by staff members or outsiders;
    - Virus infestation notices; and
    - Irregular Workstation behavior, including unusual slowdowns, slow response times, or display errors.
- The Security Officer will periodically review audit logs from various information systems related to "red flag" behaviors using Security Event Information Management Technology.
- The Security Officer will periodically review reports from email monitoring systems in order to track and investigate potential misuse of email for sending of unencrypted PHI.

Policy 12

Integrity/Authentication of Electronic Protected Health Information Policy and Procedure

Policy:

It is the policy of NSU to identify and implement technology that will corroborate that data containing EPHI has not been altered or destroyed in an unauthorized manner.

Procedure:

1. Through the risk management process, the Security Officer will address which data must be authenticated and will evaluate which data authentication methods are available for each system to corroborate that data containing EPHI has not been altered or destroyed in an unauthorized manner (e.g., error correcting memory, magnetic disc storage).
2. The Security Officer will make good faith efforts to activate or turn on any capabilities that are available on each system which requires data authentication and to acquire and use facilities to carry out data authentication and corroboration as described above, where reasonable.

Policy 13
Transmission Security Policy and Procedure

Policy:

NSU shall ensure the confidentiality and integrity of EPHI with regard to technical security measures to guard against the unauthorized exposure and modification of EPHI during transmission. This policy shall apply to the transmission (data in motion) of EPHI across public networks and portable media. Public networks include the Internet and open environments that do not require confidentiality and integrity of information. Portable media includes, but is not limited to, removable hard drives, CDs, floppy disks, USB memory sticks, and mobile devices or smart phones capable of storage. This policy does not apply to private lease line or dial-up phone connections, including facsimile transmissions.

Workforce Members are responsible for the transmission of EPHI in accordance with this policy and Policy 13A. Failure to comply with this policy, including Policy 13A, shall result in disciplinary action up to and including termination or employment or expulsion from the program. The Security Officer shall be responsible for providing the technical assistance requested from individuals in order to comply with the encryption requirements.

General Transmission Guidelines:

- Internal transmissions within NSU is considered secure as there are authentication and encryption security mechanisms implemented on NSU networks, including NSU's secure wireless networks.
- When transmitting EPHI outside of those networks, additional and appropriate security measures must be implemented in accordance with this policy and Policy 13A. Pursuant to Policy 13A, EPHI shall not be transmitted to patients except in limited circumstances for the purpose of compliance with the HIPAA Privacy Rule and patient's right of access (i.e., patient's right to request an electronic copy of their records to be sent electronically) or as specifically permitted by NSU.
- All transmissions of EPHI across public infrastructures must either encrypt the information or encrypt the connection between the sending and receiving entities.
- All transmissions of EPHI across public networks must also ensure that EPHI is not improperly modified without detection while in transit.

Procedures:

1. When transmitting confidential information, including EPHI, the sending party must comply with the following requirements depending on the nature of the transmission:

   <u>EPHI Transmissions to Non-NSU Individuals/Entities</u>

   - All transmissions of PHI from NSU networks to an outside network must utilize an encryption mechanism between the sending and receiving entities or the file, document, folder containing EPHI must be encrypted before transportation.
   - Prior to transmission of EPHI from NSU network to an outside network, Workforce Members must take reasonable precautions to ensure the identity of the receiving party.
   - All transmissions of EPHI shall include only the minimum amount of PHI (See HIPAA Privacy Policies) and a legitimate need for transmittal of the confidential information.
   - See HIPAA Security Policy, Electronic Mail Containing PHI Policy, No. 13A.

   <u>EPHI Transmissions Using Electronic Removable Media</u>

   - Use an encryption mechanism to protect against unauthorized access or modification.
   - Transmit only the minimal amount of confidential information necessary to comply with the request or use.
   - Store and transport the media in a secure environment.

   <u>EPHI Transmission Using Email</u>

   - See HIPAA Security Policy, Electronic Mail Containing PHI Policy, No. 13A.

Policy 13A
Electronic Communications Containing PHI Policy and Procedure

Introduction:

The Health Insurance Portability and Accountability Act ("HIPAA") privacy and security standards establish mandatory standards for protecting patient's Protected Health Information ("PHI"), which includes electronic protected health information ("EPHI"). EPHI is PHI that is transmitted or maintained in electronic media. This policy sets the rules for the use and disclosure, including transmission, of PHI electronically through email and text messaging. NSU policies and procedures relating to PHI apply equally to all Workforce Members granted access privileges to any NSU information resource with the capacity to receive, maintain or transmit PHI through electronic media.

NSU supports the timely email communication of PHI where necessary to promote patient health and safety and efficient customer service while balancing the need for patient privacy. As such, email communication involving PHI is allowed only under specific circumstances and shall occur according to NSU policies and procedures. All electronic mail (email) created, received, stored or sent on computers owned, leased, administered, or maintained by NSU, or otherwise under the custody and control of NSU, shall be considered to be the property of NSU.

At this time, NSU does not have an "organizational-wide" secure email messaging system for email communication involving PHI. However, NSU does have encryption solutions available for individuals who have a need to send PHI electronically as part of their job. NSU Workforce Members who have a need to communicate information containing PHI through email are required to obtain approval in advance from the HIPAA Security Officer who will also be responsible for setting up any solutions for secure email exchange with encryption technology that may be deemed necessary to protect communications. Email sent via the Internet, between servers, or through other unsecure means can be intercepted and accessed by individuals other than the intended recipient. This unauthorized access poses a risk to our patients and to NSU.

With respect to text messaging, due to concerns, among other things, about the security of this medium and the ability to incorporate a text message if necessary into a patient's electronic medical record, NSU prohibits any use of text messaging by NSU Workforce Members to access, use, store, or transmit PHI.

All NSU Workforce Members, including employees, students, contractors and researchers who may receive, maintain or transmit EPHI are expected to comply with this policy. Failure to comply with this policy will result in sanctions in accordance with HIPAA Privacy Policy Number 14 - Sanctions (See Security Management Policy and Procedure 1.3 Workforce Member Sanctions).

Definitions:

Email: A means or system for transmitting written messages electronically between terminals linked by telephone lines, cable networks, or other relays.

Protected Health Information (PHI): PHI means individually identifiable health information transmitted or maintained in any form or medium, including oral, written and electronic. Individually identifiable health information is information, including demographic information collected from an individual that is created or received by NSU and which relates to the past, present, or future physical or mental health or condition of an individual, provision of health care to an individual, or the past, present or future payment for the provision of health care to an individual. Information is considered PHI where the information identifies the individual or where there is a reasonable basis to believe the information can be used to identify an individual.

Text messaging: Any means of transmitting written messages electronically between cellular phones, pagers, or other handheld or mobile devices sent through SMS (short message service) or similar service.

Policy:

13.1 Sending Email Containing EPHI within NSU

a) Emails containing PHI may only be sent from one nova.edu address to another nova.edu address.
b) The email containing EPHI content should be limited to the minimum necessary to meet the requester's needs, should use de-identified health information whenever possible, and should be sent only to individuals who have a need to know the information, in accordance with NSU's HIPAA Privacy Policy 4A (Minimum Necessary/Need to Know Policy).
c) The sender of any email containing PHI is responsible for ensuring that the recipient's address is within the nsu.edu email system and the name and email address of the recipient must be verified as correct before the message is sent.
d) Email and email accounts that include, or could potentially include, EPHI may not be manually forwarded or auto-forwarded to non-nsu.edu accounts and any unsecure email accounts, including but not limited to personal and commercial email accounts such as Gmail, Yahoo, Hotmail, etc.
e) No distribution list may be used for email that contains PHI.
f) Access to any NSU administered email accounts (i.e. nsu.edu accounts) through the Internet must be by secure (SSL) connections.
g) The following message should be included in all email transmissions containing PHI:
"This communication may contain information that is legally protected from unauthorized use or disclosure. If you are not the intended recipient, any dissemination, distribution or copying of this communication is strictly prohibited. If you have received this message in error, you should notify the sender immediately by telephone or by return email and delete this email from your computer."
h) The following are situation-based questions and answers to help you apply these guidelines:

Question	Answer
Can I put the patient's name in the "subject" line of the email?	In order to maintain patient confidentiality, you should not put the patient's name in the subject line of the email. As an alternative, you can put the words "patient specific information."
What should I do if I receive an email containing EPHI in error?	Send a "reply" email to the sender noting that you received the email in error and that the sender should check that he/she has the correct email address for the individual who should have received the message. Before replying to the sender, strip the content of the email to avoid any further errors. Notify the HIPAA Security Officer at 2-0448 of the error for appropriate follow up.

13.2 Email Communication with Patients

It is the policy of NSU that Health Care Components may not exchange clinically-relevant information with patients via email, except in response to a patient's specific written request that an electronic copy of the patient's medical records be sent via email. Such a request must be documented on the NSU Authorization for Use or Disclosure of Protected Health Information, HIPAA Privacy Forms Exhibit 7, including Addendum to Authorization as discussed in Paragraph 13.3 of this Policy.

13.3 Email Copies of Medical Records in Response to Patient Requests

The HIPAA Privacy Rule, as amended by the Final Omnibus Rule, gives patients the right to request a copy of their PHI in a form and format of their choosing. This has been interpreted by the Office of Civil Rights to include a requirement that a patient, upon request, must be permitted to request an electronic copy of his or her medical record or billing record to be sent through email. The patient can also request, in writing, that an electronic copy of his or her medical record be sent to an individual designated by the Patient (e.g., the patient's doctor or a family member). Note that this right to electronic access only extends to information that is maintained in electronic form by NSU.

An electronic copy of a patient's medical record or billing record, or any portion of these records, may be sent through email to the patient or a person that the patient designates only when necessary to comply with this new legal requirement. In order to request the electronic transmission of any PHI, including medical or billing records, the patient must complete and sign an Authorization for Use or Disclosure of Health Information form (HIPAA Privacy Forms Exhibit 7), which shall include the Addendum to Authorization for Email Communications, and clearly designate the individual who should receive the medical records as well as the email of the intended recipient (written twice for confirmation).

Only the HIPAA Liaison for the Health Care Component or his/her designee, utilizing a secure email program approved by the Security Officer, may send the email providing the patient, the patient's personal representative, or the patient's designee with any PHI, including a copy of the patient's medical or billing records in response to the patient's request for the electronic transmission of electronically maintained PHI.

Procedures:

a) It is the responsibility of NSU Workforce Members within a Health Care Component to make sure a patient requesting an electronic copy of his/her medical or billing record to be sent by email is provided the NSU Authorization for Use and Disclosure of Health Information (Authorization), HIPAA Privacy Policies Exhibit 7, which shall include the Addendum to Authorization for Email Communications ("Addendum").
b) NSU personnel must obtain the completed and signed Addendum from the patient before sending an electronic copy of the patient's medical or billing records by email.
c) In addition to the Addendum, it is the responsibility of the NSU personnel to obtain the completed and signed Authorization from the patient, in accordance with the HIPAA Privacy Policy before sending an electronic copy of the patient's medical or billing records by email.
d) The patient or recipient's name and email address must be verified before the medical records are sent.
e) If the patient is requesting that the information be sent to a designee, the form must clearly state the designee's name as well as the email address for the designee.
f) The following message must be included in all email transmissions containing PHI:
"This communication was sent from an unmonitored email account at NSU. If you have treatment-related or any other questions, please contact The Eye Care Institute to address the matter at (954) 262-4200, or make an appointment, as appropriate. If you are experiencing an eye emergency please call (954) 262-4200 immediately. This communication may contain information that is legally protected from unauthorized use or disclosure. If you are not the intended recipient, any dissemination, distribution or copying of this communication is strictly prohibited. If you have received this message in error, you should notify the sender immediately by telephone at (954) 262-4200 and delete this email from your computer."
OIIT or a Deputy Security Officer will set up separate accounts for the HIPAA Liaison or his/her designee to use for the purpose of sending copies of medical records pursuant to this policy. The email will have a generic name indicating the Health Care Component but not an individual (e.g., healthcarecomponent1@nsu.edu). Where possible, OIIT or a Deputy Security Officer will help the HIPAA Liaison to set up an autoreply response that contains the following language:
"You have reached an unmonitored email account at NSU. If you have treatment-related or any other questions, please contact the Eye Care Institute to address the matter at 954-262-2273, or make an appointment, as appropriate. If you are experiencing an emergency please call "911" immediately."
g) If an individual receives an email from a patient that relates to the patient's medical care, the individual is responsible for notifying the patient that the Health Care Component does not communicate clinical information by email and that the patient should call the office to address the matter or make an appointment, as appropriate. The only exception involves providing a patient his/her medical or billing records in an electronic form provided those records are maintained by NSU in an electronic form. In that event, the patient must provide NSU with specific written authorization to do so as described above.
h) If email messages are received by NSU Health Care Component Workforce Members (e.g., faculty, staff, and students) from patients that relate to their health care and would otherwise constitute part of the medical record, the email should be printed and kept in the patients' medical record. In addition, the NSU Workforce Members are responsible for notifying the patient that the NSU Health Care Component does not communicate medical or treatment-related information by email and that the patient should call the NSU Health Care Component to address the matter, or to make an appointment, as appropriate. Please note that the prohibition on communicating via email includes, but is not limited to, appointment scheduling.

13.4 Email Communication Containing PHI with External Entities (e.g., Vendors, Insurance Companies).

NSU policy prohibits email communications containing PHI with any external individual or entity. There are approved means by which the information may be sent (see below).

Question	Answer
I need to send an Excel Spreadsheet containing PHI to a collection agency, but I don't have encryption. What should I do?	1. "Burn" the spreadsheet to a CD, password protect the file, mail the CD, and then call the recipient and provide the password to the file; or 2. Fax the spreadsheet according to the NSU faxing guidelines (Please see HIPAA Privacy Policy No. 7B).

13.5 Email Communication between NSU Health Care Providers and Non-NSU Health Care Providers

NSU policy prohibits email communications containing PHI with any non-NSU health care provider. There are approved means by which the information may be sent (see below).

Question	**Answer**
I need to send an Excel Spreadsheet file containing research data containing PHI to a collaborating researcher at another University, but I don't have encryption. What should I do?	1. "Burn" the spreadsheet to a CD, password protect the file, mail the CD, and then call the recipient and provide the password to the file; or 2. Fax the spreadsheet according to the NSU faxing guidelines, (Please see HIPAA Privacy Policy No. 7B).
Can I respond via email to a patient's primary care physician's (PCP) unsecure email requesting my opinion after I saw the patient in the clinic on a referral basis?	No. Even though the PCP initiated the email, you should not respond using unsecure email. Contact the PCP by phone to communicate the information and follow up the conversation with a letter/note.

13.6 Email Monitoring

No Workforce Members shall have the expectation of privacy in anything they create, receive, maintain or transmit using NSU's email system. NSU reserves the right to periodically access, monitor and disclose the contents of email messages. Access and disclosure of individual employee messages may only be done with the approval of NSU officials and/or its legal counsel.

13.7 Forwarding Email

To prevent the unauthorized or inadvertent disclosure of sensitive information such as PHI, automatic email forwarding, and the potentially inadvertent transmission of sensitive information by all Users, is prohibited. It is the policy of the Health Care Component and NSU that email should not be automatically forwarded to any destination external to NSU.

13.8 Distribution Lists

No distribution list may be used for email that contains PHI.

13.9 Use of Text Messaging

It is the policy of NSU that NSU Workforce Members are prohibited from using text messaging on any device in order to access, use, store, or transmit PHI. This prohibition applies to communications within NSU and to non-NSU entities and individuals.

NSU Workforce Members may not communicate with NSU patients (including the patient's family, the patient's personal representative, or the patient's designee) via text messaging, including but not limited to any communications with regard to scheduling, appointments, treatment or diagnosis. NSU Workforce Members may not disclose any contact information to NSU patients that would enable the patient to contact the NSU Workforce Member via text messaging. NSU Workforce Members are encouraged to educate and remind NSU patients of the approved channels through which they can communicate with NSU Workforce Members.

Policy 13 B
Email Communications between NSU Providers and Patients Policy
The Institute for Neurology Immune Medicine (NIM)

Policy:

NSU supports the timely email communication of protected health information (PHI) to promote patient health and safety while balancing the need for patient privacy and confidentiality. Email communication entails the use of the Internet, which can be intercepted and read or accessed by unauthorized individuals. This poses a risk to NSU as well as our patients. For these reasons, email communication involving PHI is allowed only under specific circumstances and shall occur only upon compliance with NSU guidelines. (Refer to HIPAA Security Policy 13 A, Electronic Mail Containing PHI Policy).

Pursuant to section 13.2 of Policy 13 A, NSU does not permit its Health Care Components to exchange clinically relevant information, including PHI, with patients through email, except in response to a patient's specific written request for an electronic copy of his/her medical. Given the circumstances involved with the clinical services in The Institute for Neurology Immune Medicine (NIM), NSU is willing to authorize specific NSU providers in NIM to communicate with NSU patients via email provided strict compliance with this policy, procedures and guidelines set forth below.

Procedures:

1. Patient or Patient Representative Authorization. You must obtain the patient or patient's representative's prior written authorization before communicating clinically relevant information, including PHI via email. (Attached NSU Patient – Provider Email Communication Form)
2. Secure Encryption Solution. Prior to conducting any communications with patients via email, NSU provider must ensure that he/she has obtained a secure file transfer solution from Strategic Support Services (sss@nova.edu). Sending emails without such a secure solution, is strictly prohibited and sending emails to patients from personal accounts is likewise prohibited (e.g. use of unsecure email accounts such as Yahoo, Gmail, Hotmail).
3. Patient Consent. Prior to beginning an email relationship with a patient, the NSU provider should have a discussion with the patient about the possible risks associated with email communication involving PHI, ensure that patient has provided the correct email address, ask the patient to send a "test" email message to verify correct email address, and ensure that the patient signed the consent, Form (see #1 above), a copy of which should be placed in the patient's medical record. These steps shall be documented in the patient's medical record.
4. Provider Choice. NSU providers reserve the right to deny a patient's request to communicate with him/her via email. The provider must use his/her best professional judgment and if circumstances would make it not in the patient's best interest, then email communication with the patient should not occur. For example, highly confidential information (e.g. mental illness, HIV/AIDS testing or treatment, substance abuse) may be types of information that a NSU provider chooses not to communicate to a patient via email.
5. Medical Record. Any communication that occurs between NSU provider and NSU patients that involves clinical care communication must become part of the patient's medical record. Clinical care information means all communications containing clinically relevant information, treatment, care management, medications or any other form of medical care. All email communications between NSU provider and NSU patient must be printed, scanned and incorporated in the respective NSU patient's medical record. The Health Care Component, in this case NIM, is solely responsible to ensure that this occurs.

Other Recommended Guidelines Relating to Email Usage with Patients

- Subject line should state, "Confidential: Physician-Patient Information For Authorized Individuals Only"
- Standard privacy disclaimer language is recommended and should be automatically attached to all NSU outgoing email messages.
- When out of the office for any period of time (e.g. vacation, sickness, business travel), NSU provider shall create an automatic "out of office" replay message that will provide proper notification that you will be unavailable until a certain date and state whether you will be checking your email account during your absence. NSU provider must also provide instructions that if the sender is a patient, that he/she should contact an alternate number for immediate assistance until your return.

Enforcement

Non-compliance with this policy and/or its related procedures may be cause for disciplinary action up to and including termination. (Refer to HIPAA Privacy Policy No. 14, Workforce Sanction Policy) Depending on the circumstances, federal law or state law may involve civil or criminal action, including restitution, fines, penalties or other sanctions for actions that result from violation of this policy.

Policy 14
Cloud Storage Policy

Introduction:

The Health Insurance Portability and Accountability Act ("HIPAA") Privacy and Security Rules set standards and mandatory requirements that for protecting patient's Protected Health Information ("PHI"), which includes electronically maintained or transmitted PHI ("EPHI"). This policy sets the rules for the storage of EPHI in cloud storage service models ("Cloud Storage"). This policy applies equally to all Workforce Members granted access privileges to any NSU information resource with the capacity to receive, maintain or transmit EPHI.

All NSU Workforce Members, including employees, students, contractors and researchers who may create, receive, maintain, or transmit EPHI are expected to comply with this policy. Failure to comply with this policy will result in sanctions in accordance with HIPAA Privacy Policy Number 14 – Sanctions (See Security Management Policy and Procedure 1.3 Workforce Member Sanctions).

Policy:

14.1 Use of Cloud Storage Prohibited Without Preapproval

For purposes of the NSU HIPAA Security Policies, Cloud Storage is any service model in which data is maintained, stored, managed or backed up remotely and made available to Users over a network (typically, the Internet). Although there may be others, common examples of Cloud Storage include SkyDrive, Dropbox and iCloud.

It is the policy of NSU that EPHI may not be stored using a Cloud Storage service model unless the service model has been approved in writing and in advance of the use by the Security Officer.

In evaluating requests for approval for the use of Cloud Storage service models, the Security Officer will consult with the Chief Information Officer ("CIO") to determine whether appropriate security and encryption of data is in place. The Security Officer will also determine whether the requestor has a legitimate need that justifies any risks associated with the Cloud Storage service model chosen. In the event a legitimate need is justified, the Security Officer will ensure that an appropriate Business Associate Agreement is in place with the Cloud Storage vendor in accordance with HIPAA Privacy Policy No. 8, Business Associate Policy.

Upon the effective date of this policy, it will be the responsibility of all Workforce Members to review their current practices with regard to the storage of EPHI. If individuals are currently using a Cloud Service model that meets the definition of Cloud Storage, such individuals are responsible for immediately contacting the Security Officer, ceasing to upload any additional EPHI to the Cloud Storage, and immediately removing all EPHI from Cloud Storage unless written approval for Cloud Storage use is obtained from the Security Officer and an appropriate Business Associate Agreement or other arrangement is in place in accordance with the HIPAA Privacy Policies. Should any Workforce Members have any question as to what may constitute Cloud Storage, the individual shall consult with the Security Officer.

Policy 15
HIPAA Security Mobile Device Policy and Procedure

POLICY STATEMENT

NSU seeks to protect NSU-owned mobile devices and NSU-related data stored on such devices, from unauthorized access, use, disclosure, alteration, modification, deletion, destruction and/or removal. Because of the inherent risks associated with mobile device access to NSU-related data, access to NSU-related data will not be permitted on personally owned (i.e. non-NSU-owned) mobile devices unless the device has been enrolled on the OIIT provided Mobile Device Management (MDM) solution. The use of Mobile Device Management ("MDM") will be implemented as of June 2014 to manage risks inherent with device use to NSU-owned and personally owned mobile devices that connect to NSU email and NSU sensitive data systems. All requirements must be complied with in order to use, access, store or transmit NSU/PHI confidential data on NSU-owned or personally owned mobile devices. Random/periodic checks/audits of devices to ensure compliance will be performed.

Installation of MDM Software will be required prior to using NSU-owned or personally owned mobile devices to access, use, transmit or store NSU-related Confidential or Personal Information, Electronic Protected Health Information ("EPHI") or Research Related Health Information ("RRHI"). Permission must be obtained from an appropriate individual as described in this policy AND the device must be secured in advance by the Office of Innovation and Information Technology ("OIIT").

PURPOSE

This policy describes the minimum security policy for all NSU-owned or personally owned mobile devices used to access, use, store, or transmit NSU-related Confidential or Personal Information, EPHI or RRHI. Mobile devices must be appropriately secured to:

- Prevent NSU-related Confidential or Personal Information, EPHI and RRHI from being lost or compromised
- Reduce the risk of spreading viruses; and
- Mitigate other forms of abuse of NSU's computing and information infrastructure

SCOPE

This policy applies to users of any NSU-owned or personally owned mobile devices that connects to NSU's network / resources or is otherwise used to store or transmit NSU-related information. The access, use, transmission or storage of NSU-related Confidential or Personal Information, EPHI, or RRHI, including but not limited to taking or storing NSU patient-related images, with a personally owned (i.e. non-NSU-owned) mobile device is prohibited.

DEFINITIONS

1. **Encryption:** The use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key. For purposes of this policy, encryption must be consistent with the methods described in NIST Special Publication 800-111 which can be found at **http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-111.pdf**.

2. **HIPAA Security Rule**: The HIPAA Security Rule refers to the regulations at 45 CFR Part 160 and Parts A and C of 45 CFR Part 164, which contain the standards for the security of EPHI pursuant to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").

3. **Mobile Devices:** These include, but are not limited to, Personal Digital Assistants (PDAs), notebook computers, Tablet PCs, iPhones, iPads, iPods, Palm Pilots, Microsoft Pocket PCs, RIM Blackberry devices, MP3 players, text pagers, smart phones, compact discs, DVD discs, memory sticks, USB drives, floppy discs and other similar devices**.**

4. Research Related Health Information or RRHI: RRHI means information collected during a research study that does not include a diagnostic or therapeutic intervention, and does not acquire health related facts about a person by copying them from a medical record, the confidentiality of which must be protected pursuant to the Federal Policy for the Protection of Human Subjects ("the Common Rule").

5. **User:** Anyone with authorized access to NSU's business information systems. This includes all Workforce Members, permanent and temporary employees, students, faculty, physicians, third-party personnel such as temporaries, contractors, or consultants, and other parties with valid company access accounts.

6. **Screen Lock:** A password-protected mechanism used to hide data on a visual display while the device continues to operate. Screen locks can be activated manually or in response to rules.

7. **Screen Timeout:** A mechanism that turns off a device display after the device has not been used for a specified time period.

8. **Personal Information:** The term "Personal Information" means an individual's first name, first initial and last name or any middle name and last name, in combination with any one or more of the following unencrypted data elements: (a) social security number; (b) driver's license number or state identification card number; (c) account number, credit card number, or debit card number, in combination with any required security code, access code or password that would permit access to an individual's financial account.

9. **Confidential Information:** Confidential Information is any information that is the property of NSU and may cause financial, reputational or other harm to the NSU if disclosed to unauthorized persons, either because of legal or business concerns. If there is a question as to whether information is considered confidential, individuals should consult with their supervisor or other superior and may also consult with the Chief Information Security Officer (CISO).

10. **Electronic Protected Health Information or EPHI:** Protected Health Information is any information that (a) is created or received by a provider and relates to the past, present or future physical or mental health 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 (b) either identifies the individual or could reasonably be used to identify an individual. Protected health information becomes "electronic" protected health information when it is maintained in electronic media or transmitted by electronic media.

ENFORCEMEN
T

Non-compliance with this policy and/or its resulting procedures, including but not limited to any use or attempted use of a personally owned mobile device to access, use, store, or transmit NSU-related Confidential or Personal Information, EPHI or RRHI, may be cause for disciplinary action up to and including termination. Actionable conduct includes, but is not limited to, taking or storing NSU patient-related images with a personally owned (i.e. non-NSU-owned) mobile device or NSU-owned mobile device that has not been enrolled in the MDM service. Depending on the circumstances, federal or state law may permit civil or criminal litigation and/or restitution, fines, and/or penalties for actions that would constitute a violation of this policy.

RESPONSIBILITY

1. All mobile device users are responsible for following this policy.
2. Anyone observing what appears to be a breach of security, violation of this policy, violation of state or federal law, theft, damage, or any action that might place company resources at risk must immediately report the incident to the Chief Information Security Officer, the NSU HIPAA Security Officer at 954-262-0448, by email at itsecurity@nova.edu, and/or Toll Free Hotline: 888-609-Nova (6682).
3. Managers, supervisors and HIPAA Liaisons and Deputy Security Officers are jointly responsible for communicating this policy to all individuals in their area so that all mobile device users in their area are aware of and understand this policy and all related procedures.
4. With regard to RRHI, it is the responsibility of the Institutional Review Board (IRB) to inform mobile device users of this policy during the research review process.

PERMISSION FOR ACCESSING, STORING, OR USING EPHI, RRHI, or NSU RELATED CONFIDENTIAL INFORMATION OR INFORMATION ON MOBILE DEVICES

EPHI, RRHI, and NSU-related Confidential Information and/or Personal Information should not be used, stored or accessed on a mobile device unless it is necessary for a legitimate business purpose and appropriate approval has been obtained. Those individuals designated to grant approval shall maintain documentation of those Workforce Members granted permission. All Workforce Members, including but not limited to students, faculty, researchers, and physicians must obtain permission from the following individuals, as applicable:

Type of Information	**Who May Grant Permission**
Electronic Protected Health Information (EPHI)	The HIPAA Liaison for the clinical area/covered component
Research Related Health Information (RRHI)	The IRB
Other NSU Related Personal Information	Immediate supervisor
Other NSU Related Confidential Information	Immediate supervisor

NSU-owned or Personally owned (i.e. non-NSU-owned) mobile devices that have not been enrolled in the MDM service may not be used under any circumstance to access, use, store, or transmit NSU-related Confidential or Personal Information, EPHI or RRHI, including but not limited to taking, storing, or transmitting NSU patient-related images, and any request for permission to do so without the MDM service being setup will be denied.

NSU-OWNED MOBILE DEVICES AND NSU PATIENT IMAGES

An NSU-owned mobile device may not be used by Workforce Members to create, store, or transmit images of NSU patients unless the mobile device has been secured with MDM Software, the Workforce Member's immediate supervisor has approved this specific use as necessary for carrying out clinical operations, and permission has been granted by the HIPAA Liaison for that Workforce Member's clinical area or covered component. Those individuals designated to grant permission shall maintain documentation of those Workforce Members granted such permission.

A Workforce Member may only transmit a patient image to the secured NSU system. The Workforce Member may not transmit a patient image to the patient (for example, via e-mail or text message). The Workforce Member may not use a personal e-mail account to transmit a patient image. A patient image may not be transmitted or stored by NSU Cloud Storage.

ENCRYPTION

Once permission is granted to access, use, transmit, or store EPHI, RRHI, or NSU Related Confidential Information or Personal Information on a NSU-owned or personally owned mobile device, the device must be secured in the following manner:
The Office of Innovation and Information Technology (OIIT) must properly register the mobile device with MDM software. In addition, OIIT will encrypt all existing mobile devices with an encryption product determined by OIIT to be the best encryption solution for the device at issue. Devices will be encrypted and secured in order of priority based upon the risk that the device may be used to access, use, store, or transmit EPHI or RRHI or upon request of individuals who have a need to access, use, store, or transmit EPHI or RRHI.**DESTRUCTION/DISPOSAL**

All NSU-related Confidential or Personal Information, RRHI, or EPHI contained on an NSU-owned or personally owned mobile device must be "wiped" or securely deleted at the conclusion of the stated purpose for having such information on the mobile device, upon termination of employment with NSU, or upon termination of affiliation with NSU.

If you have questions, please contact the Chief Information Security Officer, the NSU HIPAA Security Officer at 954-262-0448, or email at itsecurity@nova.edu.

NSU-owned and personally owned mobile devices will be disposed of or wiped in accordance with NSU's policies.

PROCEDURE:

1. There must be a legitimate business purpose to access, use, store, or transmit EPHI, RRHI, or NSU-related Confidential or Personal Information on a mobile device and prior approval as set forth in this policy must be obtained. In order to transmit PHI (including patient images) by electronic media, you must also comply with HIPAA Security Policy No. 13A, Electronic Mail Containing PHI Policy. Specific approval must be obtained to create, store, or transmit images of NSU patients using an NSU-owned or personally owned mobile device. Patient images may be transmitted from an NSU-owned mobile or personally owned device only via the secure NSU email system, and may not be transmitted using a non-MDM-secured personally-owned mobile device or personal e-mail account or transmitted to Cloud Storage that is not provided for such use by OIIT, consistent with HIPAA Security Policy No. 14, Cloud Storage Policy.
2. A mobile device used to store, access or use EPHI, RRHI or NSU-related Confidential or Personal Information must be encrypted in accordance with this policy.
3. Whenever possible, and whenever necessary to secure a device in accordance with this policy, all mobile devices must be password protected. Most devices allow for a 4-digit PIN number to be selected by the user, which must be enabled. The password must not be "1234" or "4321" or all 4 of the same number (such as "1111" or "2222 etc.). The password must also not be an address number or digits in a telephone number associated with the user. The PIN number chosen should be changed at least once per year.
4. For devices that can support a longer password, the NSU Enterprise Username and Password Policy must be followed, which can be found at **https://www.nova.edu/portal/oiit/policies/forms/enterprise-username-policy.pdf.**
5. The physical security of mobile devices is the responsibility of the user to whom the device has been assigned. Mobile devices shall be kept with the user whenever possible. Whenever a device is being stored, it shall be stored in a secure place, preferably out-of-sight in a locked cabinet or desk drawer. Mobile devices should not be left in unlocked vehicles under any circumstances. Mobile devices should be removed from locked vehicles whenever possible and should always be hidden from view.
6. If a mobile device is lost or stolen, you must immediately report the incident to the Chief Information Security Officer, the NSU HIPAA Security Officer at 954-262-0448, by email at itsecurity@nova.edu and/or Toll Free Hotline: 888-609-Nova (6682). This report should include the serial number if the device has one. (If your mobile device has a serial number, record it now.)
7. Mobile devices must be appropriately "wiped" or disposed of in accordance with this policy at the conclusion of the stated purpose for having such information on the mobile device, upon termination of employment with NSU, termination of affiliation with NSU, or prior to selling, exchanging or otherwise disposing of the device.
8. Mobile device options and applications that are not in use should be disabled.
9. ALL mobile devices must have screen locking and screen timeout functions enabled. Screen lock and/or timeout after ten (10) minutes of inactivity.
10. All users of NSU-related Confidential or Personal Information, EPHI or RRHI on mobile devices will be asked to sign an attestation agreeing to safeguard applicable mobile devices as required by this policy, including an attestation that they will follow appropriate procedures for wiping/destroying such devices.

HIPAA Security Officer Designation Form

DESIGNATION FORM

The NSU Hybrid Entity has designated the following individual to serve as the NSU HIPAA Security Officer:

Name: Robin Supler	*Date: April 20, 2005*
Name: Andrew Tuck, Information Security Officer:	*Date: May 2, 2011*
Name: John Christly, Chief Information Security Officer:	*Date: November 17, 2012*
Name: Charles Rodholm, Chief Information Security Officer:	***Date: July 25, 2016 - Present***

The NSU Hybrid Entity has designated the following individual to serve as NSU Deputy HIPAA Security Officer: Name:

Dr. Marlon R Clarke, Director IT Security	*Date: May 1, 2015*
Name: Marisol Suarez, Healthcare IT Security Analyst	*Date: May 1, 2015*
Name: Gisandre Mardy, Manager Healthcare IT Security	***Date: May 1, 2015 - Present***