FLORIDA INTERNATIONAL UNIVERSITY

OFFICIAL UNIVERSITY POLICY

HIPAA Privacy and Security: Faxing Protected Health Information: Steps to Minimize Privacy Risks # 1660.210

INITIAL EFFECTIVE DATE:	LAST REVISION DATE:	RESPONSIBLE UNIVERSITY DIVISION/DEPARTMENT
September 23, 2025	September 23, 2025	Office of Compliance and Integrity

POLICY STATEMENT

Florida International University (FIU) Health Insurance Portability and Accountability Act (HIPAA) Hybrid Designated Health Care Components (hereinafter facilities and programs) are committed to safeguarding Protected Health Information (PHI) and to operating in a manner consistent with applicable federal laws and Florida state statutes.

Facilities and programs will exercise special care regarding the location and operation of facsimile (fax) machines.

Facility and program Workforce members who have access to, maintain or transmit PHI will protect the privacy and confidentiality of this information when transmitting or receiving it via facsimile (fax).

Facility and program Workforce members should exercise appropriate care when faxing PHI. In addition, the faxing of sensitive PHI, such as mental health, substance misuse, sexually transmitted diseases, HIV or other highly personal information (Super-Confidential PHI), should be avoided whenever possible.

Any suspected or known violations where incoming or outgoing faxes have compromised a patient's right to privacy must be reported immediately to the Director of Compliance and Privacy for Health Affairs (HIPAA Privacy Officer) and/or the HIPAA Security Officer. (FIU Policy and Procedure #1660.095 (Reporting of HIPAA Incidents and Notification in the Case of a Breach) and (FIU Policy and Procedure # 1670.020) (Duty to Report Security Incidents Involving Protected Health Information Policy).

Facilities and programs are expected to develop procedures or protocols supplementing this policy and procedure when facility or program-specific procedures are needed. As a University-wide policy and procedure approved by the HIPAA Steering Committee, facility and program Privacy and Security Coordinators, the Office of Compliance and Integrity, and the Office of General Counsel, this policy and procedure takes precedence over any facility and program-specific policies, procedures, or protocols that conflicts with this policy and procedure, unless prior approval is obtained from the Office of Compliance and Integrity.

(FIU Policy and Procedure #1660.080) (Policies and Procedures, Changes to Policies and Procedures, and Documentation)

Facilities and programs may maintain HIPAA documentation in either paper or electronic form, provided that any format is sufficiently protected to ensure it will be retrievable throughout the required retention period. Unless otherwise indicated in the FIU Privacy or Security Rule Policy and Procedure, each facility and program Privacy Coordinator will be responsible for maintaining all HIPAA documentation relevant to his/her facility or program. (FIU Policy and Procedure #1660.080) (Policies and Procedures, Changes to Policies and Procedures, and Documentation)

All Facility and program Workforce members shall receive mandatory HIPAA Privacy and Security Rule training. (FIU Policy and Procedure # 1660.075) (HIPAA Privacy and Security Rule Training)

Facility and program Workforce members who fail to adhere to this policy and procedure may be subject to criminal and civil penalties as provided by law, and/or administrative and disciplinary action. (FIU Policy and Procedure #1660.085) (Sanctions)

FIU reserves the right to amend, change or terminate this policy and procedure at any time, either prospectively or retroactively, without notice. Any ambiguities between this policy and procedure and the other policies and procedures should be accordingly made consistent with the requirements of HIPAA, Florida state statutes and regulations, and the Information Blocking Rules. (FIU Policy and Procedure 1660.080) (Policies and Procedures, Changes to Policies and Procedures, and Documentation)

SCOPE

This policy applies to FIU's Health Care Components (hereinafter facilities and programs) contained within FIU's HIPAA Hybrid Designation (Policy and Procedure #1610.005), its Workforce members and Business Associates as defined in this policy and FIU Policy and Procedure #1660.015 regarding Business Associate Agreements.

REASON FOR POLICY

To provide the policy and procedures that should be followed when sending or receiving facsimile (fax) containing Protected Health Information (PHI) or FIU restricted information to ensure FIU's compliance with the Health Information Portability and Accountability Act of 1996 (HIPAA), the Health Information Technology for Economic and Clinical Health Act (HITECH Act) 2009, the Omnibus Rule of 2013, and the Standards for Privacy of Individually Identifiable Health Information and to safeguard restricted, confidential, sensitive PHI and other information as protected by Florida state statutes, federal law or FIU policy.

DEFINITIONS

Please refer to the following link for a complete list of definitions pertaining to all HIPAA policies.

HIPAA Policies Definitions

ROLES AND RESPONSIBILITIES

I. **Compliance Oversight:** The Director of Compliance and Privacy for Health Affairs:

- Evaluates all federal and state healthcare privacy laws, regulations, rules and ordinances (Rules) to ensure compliance with the Rules.
- Develops and maintains all required University-wide Privacy Rule policies and procedures.
- Develops and maintains HIPAA health care Privacy Rule training modules.
- Performs audits and assessments of the facilities and programs to ensure their compliance with the Privacy Rules and associated FIU Policies and Procedures.
- Partners with the Division of Information Technology HIPAA Security Officer to ensure compliance with all federal and Florida state healthcare privacy and security laws, regulations rules, and ordinances.

II. **HIPAA Components (Facilities and Programs):**

- Each FIU HIPAA Hybrid Designated Component (hereinafter facility and program) must designate a Privacy Coordinator responsible for overseeing and ensuring the Facility and program's implementation and compliance with the HIPAA Privacy Rule, FIU's associated HIPAA Privacy Policies and Procedures, and any applicable federal laws and Florida state statutes governing the confidentiality, integrity and availability of PHI and electronic PHI (ePHI), including, but not limited to the sending and receiving of facsimiles containing PHI.

RELATED RESOURCES

I. **References**

- 45 CFR §164.502
- 45 CFR §164.504
- 45 CFR §164.514
- 45 CFR §164.530
- Florida Statute §456.057

II. Related Policies

- FIU Policy # 1610.005 (Designated Health Care Components of FIU Community)
- FIU Policy and Procedure #1610.015 (Sanctions)
- FIU Policy and Procedure #1610.020 (Business Associate Agreements)
- FIU Policy and Procedure #1640.010 (HIPAA Privacy and Security Rule Training)
- FIU Policy and Procedure #1660.005 (Right of Patients to Request Confidential Communications Regarding the Use and Disclosure of Their Protected Health Information)
- FIU Policy and Procedure #1660.015 (Designation of HIPAA Privacy Officer and Component Privacy and Security Coordinators)
- FIU Policy and Procedure #1660.040 (Verification)
- FIU Policy and Procedure #1660.085 (Policies and Procedures, Changes to Policies and Procedures, and Documentation)
- FIU Policy and Procedure #1660.095 (Reporting of HIPAA Incidents and Notification in the Case of a Breach)
- FIU Policy and Procedure # 1670.020 (Duty to Report Security Incidents Involving Protected Health Information Policy)

CONTACTS

For further information concerning this policy, please contact the FIU Office of Compliance and Integrity at (305) 348-2216, compliance@fiu.edu, hipaaprivacy@fiu.edu, or the appropriate Facility and program Privacy Coordinator.

HISTORY

Initial Effective Date: September 23, 2025
Review Dates (*review performed, no updates*): N/A
Revision Dates (*updates made to document*): September 23, 2025.

FLORIDA INTERNATIONAL UNIVERSITY

OFFICIAL UNIVERSITY PROCEDURE

HIPAA Privacy and Security: Faxing Protected Health Information: Steps to Minimize Privacy Risks # 1660.210a

INITIAL EFFECTIVE DATE:	LAST REVISION DATE:	RESPONSIBLE UNIVERSITY DIVISION/DEPARTMENT
September 23, 2025	September 23, 2025	Office of Compliance and Integrity

PROCEDURE STATEMENT

Each Florida International University (FIU) Health Insurance Portability and Accountability Act (HIPAA) Hybrid Designated Health Care Component (hereinafter facility and program) must designate a HIPAA Privacy Coordinator responsible for overseeing and ensuring the facility's or program's implementation and compliance with the HIPAA Privacy Rule, FIU's associated HIPAA Privacy Policies and Procedures, and any applicable Florida state statutes governing the confidentiality, integrity and availability of Protected Health Information (PHI) and electronic PHI (ePHI), including, but not limited to the sending and receiving of facsimiles containing PHI. Privacy Coordinators may delegate and share duties and responsibilities as necessary and appropriate but retain oversight responsibility. The facilities and programs must also designate a HIPAA Security Coordinator responsible for overseeing and ensuring the facilities and programs implementation and compliance with the HIPAA Security Rule, FIU's associated HIPAA Security Policies and Procedures, and any applicable Florida state statutes governing the confidentiality, integrity, and availability of electronic PHI (ePHI), including, but not limited to the sending and receiving of facsimiles containing PHI. (FIU Policy and Procedure #1660.070) (Designation of HIPAA Privacy Officer and Component Privacy and Security Coordinators)

Each HIPAA facility and program must notify the Director of Compliance and Privacy for Health Affairs, Office of Compliance and Integrity (HIPAA Privacy Officer), and the HIPAA Security Officer, Division of Information Technology, the name and title of their designated HIPAA Privacy and Security Coordinator.

I. The Director of Compliance and Privacy for Health Affairs and the HIPAA Security Officer will ensure that facsimiles are sent and received in compliance with the HIPAA Privacy and Security Rules, other federal laws and Florida state statutes.

A. Sending Facsimiles (Faxes).

Workforce members may transmit PHI via facsimile when the transmission is time-sensitive and delivery by regular mail will not meet the reasonable needs of the sender or recipient or when the patient approves of transmission via facsimile.

Workforce members will take reasonable steps to ensure that any facsimile transmission which includes PHI is sent to and received by the intended recipient. These reasonable steps may include, but are not limited to, the following:

1. Confirming with the intended recipient that their receiving facsimile machine is located in a secure area or that the intended recipient is waiting by the facsimile machine to receive the transmission.

2. Pre-program the facsimile numbers of those recipients to whom PHI is frequently sent so errors associated with misdialing can be minimized or avoided.

   (**NOTE:** Pre-programmed facsimile numbers will be tested frequently to confirm they are still valid)

3. When a facsimile number is entered manually (because it is not one of the pre-programmed numbers), visually check the recipient's facsimile number on the facsimile machine prior to starting the transmission.

4. Use a standard facsimile cover sheet that contains a statement to the following effect:

   This facsimile is intended only for the use of the named addressee and may contain health information, the privacy and confidentiality of which are protected by federal and state law. If you are not the intended recipient, or you are not the employee responsible for delivering the facsimile to the intended recipient, you are hereby notified that any dissemination, distribution or copying of this facsimile is strictly prohibited. If you have received this facsimile in error, please notify the sender immediately and destroy, as appropriate.

5. Include the name, business affiliation, telephone number and facsimile number of the intended recipient as well as the number of pages contained in the transmission on the cover sheet.

6. Check the facsimile confirmation report to confirm the material was faxed to the intended fax number. If the intended recipient notifies the sender that the facsimile was not received, the sender will use best efforts to determine whether the facsimile was inadvertently transmitted to an incorrect facsimile number by checking the facsimile confirmation report and/or the facsimile machine's internal logging system.

7. If a Workforce member becomes aware that a facsimile was sent to an incorrect facsimile number, the Workforce member will immediately attempt to contact the unintended recipient by facsimile and/or telephone and request that the faxed documents, and any copies of the documents, be immediately returned or destroyed. The Workforce member is responsible for immediately notifying his/her immediate supervisor, the Director of Compliance and Privacy for Health Affairs, or the HIPAA Security Officer of the misdirected facsimile. (FIU Policy and Procedure #1660.095 (Reporting of HIPAA Incidents and Notification in the Case of a Breach) and (FIU Policy and Procedure # 1670.020 (Duty to Report Security Incidents Involving Protected Health Information Policy)

8. Recipients who regularly receive FIU patient PHI via facsimile will be periodically reminded to notify the FIU facility and/or program of any change to the recipient's facsimile number.

9. Facsimile confirmation reports will be attached to and maintained with all faxed materials.

10. Sensitive PHI (Super-Confidential PHI) such as HIV/AIDS status and/or test results, or substance abuse and mental health treatment records should never be sent via facsimile absent urgent need for the information as determined by the health care provider. (FIU Policy and Procedure #1660.150) (Use and Disclosure of Super-Confidential Protected Health Information)

11. When faxing PHI, Workforce members will comply with all other Florida International University Privacy and Security Policies and Procedures.

B. <u>Receiving Faxes.</u>

Workforce members who are intended recipients of facsimiles containing PHI will take reasonable steps to minimize the possibility those facsimiles are viewed or received by unintended recipients. These reasonable steps may include, but are not limited to, the following:

1. Facsimile machines that receive facsimiles containing PHI will be located in a secured area. If a Workforce member receives a facsimile containing PHI on a facsimile machine that is not in a secure area, the recipient of the facsimile will promptly advise the sender that the receiving facsimile machine should not be used for the transmission of such information.

2. Facsimile machines will be checked on a regular basis to minimize the amount of time incoming facsimiles containing PHI are left on the machines. Workforce members who monitor the facsimile machines, or Workforce

members who see a facsimile unattended on the facsimile machine, will promptly remove the incoming facsimiles and places them in a secured location or deliver them to the intended recipient.

3. If a Workforce member receives a facsimile addressed and intended for another FIU Workforce member, the unintended recipient will promptly notify the intended recipient and deliver or make arrangements for delivery of the misdirected facsimile to the intended recipient.

4. If a Workforce member receives a facsimile addressed and intended for a person NOT affiliated with FIU, the unintended recipient will promptly notify the sender and destroy or return the facsimile as directed by the sender.

5. Workforce members who routinely receive facsimiles containing PHI from other individuals or organizations (either internal or external sources) will promptly advise those regular senders of any changes to the facility's or program's facsimile number.

6. Workforce members who receive facsimiles containing sensitive PHI (Super-Confidential PHI) such as HIV/AIDS status, results, or substance abuse and mental health treatment records will promptly advise the senders of such facsimiles that it is the policy of FIU not to accept transmissions of sensitive PHI by facsimiles absent urgent need for this information as determined by the health care provider. (FIU Policy and Procedure #1660.150) (Use and Disclosure of Super-Confidential Protected Health Information)

II. Record Retention

If a communication, action, activity, or designation is required to be documented in writing, the document or record owner will maintain such writings, or an electronic copy, for seven (7) years from the date of its creation or the last effective date, whichever is later. (FIU Policy and Procedure #1660.080) (Policies and Procedures, Changes to Policies and Procedures, and Documentation)