FLORIDA INTERNATIONAL UNIVERSITY

OFFICIAL UNIVERSITY POLICY

Information Blocking # 1660.170

INITIAL EFFECTIVE DATE:	LAST REVISION DATE:	RESPONSIBLE UNIVERSITY DIVISION/DEPARTMENT
November 7, 2023	August 11, 2025	University Office of Compliance and Integrity

POLICY STATEMENT

The HIPAA Privacy Rule provides a federal floor of privacy protection for individually identifiable health information held by a covered entity, covered component, or by a Business Associate of a covered entity or covered component Florida has implemented statutes that expand patient rights and access to their PHI and, therefore, are more stringent than HIPAA. These Florida state statutes, although contrary to the HIPAA Privacy Rule, are not superseded by HIPAA.

It is the policy of FIU to place patients at the center of their healthcare through provisions that remove the obstacles they encounter when trying to access their Electronic Health Information (EHI). (Also known as Electronic Protected Health Information (ePHI)).

Florida International University ("FIU") is committed to protecting the privacy of Protected Health Information in compliance with all applicable federal and Florida state laws, regulations and rules. For purposes of compliance with the Health Insurance Portability and Accountability Act (HIPAA), FIU has determined that it is a "Hybrid Covered Entity" and has designated the facilities and programs that constitute HIPAA Hybrid Components (Components).

The FIU Health Insurance Portability and Accountability Act (HIPAA) Hybrid Designated Healthcare facility and program Workforce members (Actors) will refrain from Practices that are likely to Interfere with the Access, Exchange, or Use of EHI, except when the Practices are required by law (including HIPAA and Florida state statutes) or meet an Information Blocking Rules Exception. In other words, when a disclosure of EHI is permitted by applicable law, including HIPAA and Florida state statute, the Information Blocking Rules require the disclosure unless an Information Blocking Rules Exception applies, or the Workforce member (Actor) can otherwise demonstrate that the Practice complies with the Information Blocking Rules.

1. When considering requests for EHI or other Practices impacting the Access, Exchange, or Use of EHI, the facility or program Workforce members, through the FIU Division

of Information Technology and the Office of Compliance and Integrity, Director of Compliance and Privacy for Health Affairs, shall confirm that the Practice complies with applicable law and FIU privacy and security policies and procedures.

a. For example:

i. Requests for EHI must comply with HIPAA, including the minimum necessary standard, where applicable. (See FIU Policy and Procedure #1660.120 (Minimum Necessary).

ii. Most single-patient and multi-patient EHI requests will follow FIU's HIPAA Policy and Procedure for receipt and processing of third-party requests for Protected Health Information (PHI). For example, patients and patient Representatives can access much of their EHI in electronic format using patient portals made available by FIU or they may submit HIPAA access requests through other methods supported by FIU.

2. Requests for EHI must be processed by the facility or program Medical Records Manager, or designee.

3. The facility or program Medical Records Manager, or designee must promptly evaluate all requests to Access, Exchange, or Use of EHI.

4. The facility or program Medical Records Manager, or designee may ask third parties requesting Access, Exchange, or Use EHI to clarify the content, manner, and/or purpose of the request to assist the Medical Records Manager, or designee with confirming:

(**NOTE:** Content and Manner are commonly known as Form and Format)

a. that the potential Access, Use or Exchange is permitted or required by law;

b. whether the facility or program can furnish the requested EHI; and

c. whether the facility or program Medical Records Manager, or designee can provide the EHI in the manner requested. Alternatives to the content and/or manner requested will be identified and offered when necessary.

(NOTE: Item 3 immediately above does not apply to patient access requests under HIPAA and Florida state statutes to the extent such requests for clarification would be inconsistent with FIU Policy and Procedure #1660.050 (Patient Access to Protected

Health Information) or applicable law governing the right of patients to access their Protected Health Information (PHI)).

5. The facility or program Medical Records Manager, or designee must ensure that any Practice that may Interfere with the Access, Use or Exchange of EHI is structured, when feasible, to meet an Information Blocking Exception. If an Information Blocking Exception does not apply or cannot fully be met, the Medical Records Manager, or designee must refer the concern to the Director of Compliance and Privacy for Health Affairs to confirm the Practice is consistent with the Information Blocking Rules and FIU Policy and Procedure.

6. Complaints received alleging Information Blocking should immediately be escalated to the Director of Compliance and Privacy for Health Affairs.

The facilities and programs will implement this Policy and Procedure and inform its Workforce members as it applies to their individual roles.

The facilities and programs will review existing internal policies and procedures for receiving, processing, and responding to requests to Access, Exchange, or Use EHI and revise them as necessary to ensure compliance with the Information Blocking Rule requirements, HIPAA, and Florida state statutes.

It is the Policy of FIU that the facilities and programs will:

1. Coordinate with health IT vendors to identify and implement (if not already in place) health IT solutions that the facility or program uses or could use to support responses to access requests or otherwise comply with the Information Blocking Rule requirements;

2. Not charge fees to individuals (persons or entities that they designate) who request electronic access to their EHI through internet-based methods, such as personal health apps, standalone/untethered personal health records, and email;

3. Ensure that for fees charged to individuals (persons or entities that they designate) who request their EHI in physical media (such as paper copies), CD, or flash drive formats, comply with the HIPAA Privacy Rule and Florida State statutes;

4. Review data use and other agreements governing the sharing of EHI to ensure compliance with Information Blocking Rule requirements;

5. Conduct an inventory of how the facility or program EHI is stored and transmitted.

6. As necessary, develop policies and procedures for responding to requests for EHI from patients, providers, third-party apps, health IT vendors, and others. This may include creating forms for receiving, processing, and responding to such requests and procedures specifying how access to EHI may be provided.

Unless otherwise indicated in FIU Privacy or Security Rule Policy and Procedure, the facility and program Medical Records manager, or designee may maintain Information Blocking Rule and 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.

It is FIU's policy to comply fully with The Information Blocking Rule, the HIPAA's and Florida state statute requirements. To that end, all FIU Workforce members shall receive mandatory HIPAA Privacy and Security Rule training, as well as state law and/or regulation training in support of FIU's commitment to the proper use, disclosure, and safeguarding of PHI/ePHI from any intentional, unintentional, or incidental use or disclosure to unauthorized individuals.

Workforce members who fail to adhere to this policy and procedure may be subject to civil and criminal penalties as provided by law, and/or administrative and disciplinary action, including, but not limited to termination of employment or expulsion. Violations will be handled through FIU disciplinary policies applicable to employees and students. FIU may also refer suspected violations of applicable law to appropriate law enforcement agencies. (See 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. This policy and procedure will also change should it become necessary and appropriate to comply with changes in federal and state law, including the standards, requirements, and implementation specifications of HIPAA and the Information Blocking Rules. This policy and procedure are designed to be implemented in conjunction with a set of comprehensive privacy policies and procedures, and any ambiguities between this policy and procedure and the other policies and procedures should be harmonized consistent with the requirements of HIPAA, the Information Blocking Rules, and Florida state laws and regulations.

SCOPE

This Policy applies to FIU's HIPAA Hybrid Designated Healthcare facilities and programs.

REASON FOR POLICY

Information Blocking Rules prohibit actions that interfere with Access, Exchange, or Use of Electronic Health Information (EHI) in order to promote value-based healthcare through transparency and coordinated care among patients, healthcare providers, and others. This Policy and Procedure establishes:

(i) Florida International University and the healthcare facilities and programs are committed to preventing and avoiding engagement in practices that constitute Information Blocking according to applicable federal regulations, and

(ii) how Florida International University and the healthcare facilities and programs applies allowable exceptions and meets all conditions of such exceptions before engaging in a practice that may otherwise constitute Information Blocking.

DEFINITIONS

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

HIPAA Policies Definitions

RELATED RESOURCES

References

- 45 CFR §170 and §171 (Health IT Standards, Implementation Specifications and Certification Criteria and Information Blocking) promulgated by the Office of the National Coordinator for Health Information Technology ("ONC") in order to implement Section 4004 of the 21st Century Cures Act of 2016.
- See Public Law 104-191, §264(c)
- 45 CFR §171.103
- 42 USC §300jj
- 45 CFR §164.502
- 45 CFR §164.504
- 45 CFR §164.514
- 45 CFR §164.524
- 45 CFR §164.526
- 45 CFR §164.528
- 45 CFR §164.530

- F.S. §456.057
- F.S. §95.11

Related Policies

- FIU Policy and Procedure# 1610.005 (Designated Components of the FIU Hybrid Covered Entity)
- FIU Policy and Procedure #1660.001 (Representative)
- FIU Policy and Procedure #1660.015 (Business Associates)
- FIU Policy and Procedure #1660.040 (Verification)
- FIU Policy and Procedure #1660.050 (Patient Access to PHI)
- FIU Policy and Procedure #1660.070 (Designation of HIPAA Privacy Officer and Component Privacy and Security Coordinators)
- FIU Policy and Procedure #1660.080 (Policies and Procedures, Changes to Policies and Procedures, and Documentation)
- FIU Policy and Procedure #1660.085 (Sanctions)
- FIU Policy and Procedure #1660.105 (Class of Jobs and/or Job Titles of Workforce Members Who Require Access to PHI/ePHI and the Categories of PHI/ePHI Necessary to Carryout Job Functions and Responsibilities)
- FIU Policy and Procedure #1660.115 (Destruction/ Disposal of PHI)
- FIU Policy and Procedure #1660.120 (Minimum Necessary)

CONTACTS

For further information concerning this policy, please contact the Director of Compliance and Privacy for Health Affairs at (305) 348-0622 or hipaaprivacy@fiu.edu, or contact the appropriate Component Privacy Coordinator.

HISTORY

Initial Effective Date: November 7, 2023
Review Dates *(review performed, no updates)***:** N/A
Revision Dates *(updates made to document)***:** November 7, 2023; August 11, 2025.

Information Blocking # 1660.170a

INITIAL EFFECTIVE DATE:	LAST REVISION DATE:	RESPONSIBLE UNIVERSITY DIVISION/DEPARTMENT
November 7, 2023	August 11, 2025	University Office of Compliance and Integrity

PROCEDURE

1. The FIU HIPAA Hybrid Designated Healthcare Components (hereinafter facilities and programs) Workforce members shall prohibit and avoid engaging in practices that constitute Information Blocking and shall engage in practices that otherwise constitute Information Blocking only after meeting all conditions justifying an exception as outlined in this Policy and Procedure.

2. The facility or program Medical Records Manager, or designee shall make Electronic Health Information (EHI) available to patients in a reasonable and permissible timeframe unless an allowable exception applies and shall further make EHI available upon request in electronic or other Form and Format unless an allowable exception applies. (Also see FIU Policy and Procedure #1660.050) (Patient Access to Protected Health Information)

3. **Preventing Harm Exception.** (Also see FIU Policy and Procedure #1660.050) (Patient Access to Protected Health Information) and (FIU Policy and Procedure #1660.001) (Representatives) The facility and program healthcare professionals shall only undertake a practice likely to interfere with the Access, Exchange, or Use of EHI in order to prevent harm when the following conditions are met:

   a. **Reasonable belief.** The healthcare professional must hold a reasonable belief that the practice will substantially reduce a risk of harm to a patient or another person that would otherwise arise from the Access, Exchange, or Use of EHI affected by the practice.

   3.2 **Practice breadth.** The practice is no broader than necessary to substantially reduce the risk of harm.

   3.3 **Type of risk.** The risk of harm:

   (a) Has been determined on an individualized basis in the exercise of professional judgment by a licensed FIU healthcare professional who has a current or prior healthcare professional-patient relationship with the patient whose EHI is affected by the determination; or

(b) Has arisen from data that is known or reasonably suspected to be misidentified or mismatched, corrupt due to technical failure, or erroneous for another reason.

3.4 **Type of harm.** The type of harm serves as grounds for denying Access in one of the following circumstances:

(a) A licensed FIU healthcare professional has determined, in the exercise of professional judgment, that the Access requested is reasonably likely to endanger the life or physical safety of the patient or another person, and the practice is likely to, or in fact does, interfere with the patient's Access, Exchange, or Use of the patient's own EHI or the practice is likely to, or in fact does, interfere with a legally permissible Access, Exchange, or Use of EHI, regardless of whether the risk of harm the practice is intended to reduce is consistent with Section 3.3: **Type of Risk** of this section; or

(b) The PHI makes reference to another person (unless the other person is a Healthcare Provider) and a licensed FIU healthcare professional has determined, in the exercise of professional judgment, that the Access requested is reasonably likely to cause substantial harm to the other person, and the practice is likely to, or in fact does, interfere with the patient's or their legal representative's Access to, Exchange, or Use of information that references another person and the practice is implemented pursuant to an individualized determination of **risk of harm** consistent with Section 3.3(a) of this section; or

(c) The request for Access is made by the patient's legally authorized representative and an FIU licensed healthcare professional has determined, in the exercise of professional judgment, that the provision of Access to the legally authorized representative is reasonably likely to cause substantial harm to the patient or another person, and the practice is likely to, or in fact does, interfere with Access, Exchange, or Use of the patient's EHI by the legally authorized representative and the practice is implement pursuant to an individualized determination of **risk of harm** consistent with Section 3.3(a) of this section.

3.5 **Right to request review.** Where the risk of harm has been determined on an individualized basis in the exercise of professional judgment by an FIU licensed healthcare professional who has a current or prior healthcare provider-patient relationship with the patient whose EHI is affected by the determination, the individual who made the request for Access, Exchange, or Use has the right to have the denial reviewed by a licensed healthcare professional designated by FIU to act as a reviewing official and who did not participate in the original decision to deny Access, Exchange, or Use. (Also see FIU Policy and Procedure #1660.050) (Patient Access to Protected Health Information).

3.6 **Policy or specific determination.** The practice is either consistent with:

(a) An FIU written policy that is based on relevant clinical, technical, and other appropriate expertise, is implemented in a consistent and non-discriminatory manner, and meets all other applicable conditions; or

(b) A determination based on facts and circumstances known or reasonably believed by the FIU healthcare professional at the time of the determination and while the practice remains in use and based on expertise relevant to implementing the practice in a way that meets all other applicable conditions.

4. **Privacy Exception.** (Also see FIU Policy and Procedure #1660.050 (Patient Access to Protected Health Information). The facility or program Medical Records Manager, or designee shall only undertake a practice likely to interfere with the Access, Exchange, or Use of EHI in order to protect an individual's privacy when the following conditions are met:

4.1 **Precondition not satisfied.** (Also see FIU Policy and Procedure #1660.040) (Verification), (FIU Policy and Procedure #1660.020) (Authorization for Uses and Disclosures of Patient Protected Health Information), and (FIU Policy and Procedure #1660.001) (Representatives). Florida state statutes or Federal law, such as the HIPAA Privacy Rule, requires one or more preconditions for providing Access, Exchange, or Use of PHI that have not been satisfied and:

(a) the facility or program practice is tailored to the applicable precondition not satisfied, is implemented in a consistent and non-discriminatory manner, and either conforms to written FIU Policies and Procedures that specify the criteria to be used to determine when the precondition would be satisfied and the steps to take to satisfy the precondition or the facility or program has supporting case-by-case documentation identifying the criteria used to determine when the precondition would be satisfied, any criteria that were not met, and the reason why the criteria were not met; or

(b) If the precondition required consent or authorization from an individual (e.g., the patient or legally authorized representative) and the facility or program Medical Records Manager, or designee has received consent or an authorization, but it does not satisfy all the required elements of the precondition required under applicable law, the facility or program Workforce member(s) has:

- Used reasonable efforts within its control to provide the individual with a consent or authorization form that satisfies all required elements of the precondition or has provided other reasonable assistance to the individual to satisfy all required elements of the precondition; and

- Not improperly encouraged or induced the individual to withhold the consent or authorization.

4.2 **Denial of an individual's request for his/her EHI** consistent with 45 C.F.R. §164.524 (Access of individuals to Protected Health Information). If an individual requests EHI under the Right of Access provision of the HIPAA Privacy Rule and Florida state statutes, the facility and program Workforce members shall adhere to applicable requirements. (See FIU Policy and Procedure #1660.050 (Patient Access to Protected Health Information).

4.3 **Respecting an individual's request not to share information.** (See FIU Policy and Procedure #1660.045) (Right of Patients to Request Restrictions Regarding the Use and Disclosure of their Protected Health Information). Unless otherwise required by law, the facilities and programs may elect not to provide Access, Exchange or Use of an individual's EHI if:

(a) The individual requests such restriction without any improper encouragement or inducement by the facility or program Workforce member(s);

(b) The facility or program Medical Records Manager, or designee must document the request as required by HIPAA, federal law, and Florida state statutes, and FIU Policy and Procedure;

(c) The facility or program practice is implemented in a consistent and non-discriminatory manner; and

(d) The facility or program terminates an individual's request for such restriction only if:

- The individual agrees to the termination in writing or requests it in writing;
- The individual orally agrees to the termination and the oral agreement is documented by the facility or program Medical Records Manager, or designee; or
- The facility or program Medical Records Manager, or designee informs the individual that it is terminating its agreement to the restriction except that such termination is not effective to the extent prohibited by applicable HIPAA and Florida state statutes and only applicable to EHI created or received after the facility or program Medical Records Manager, or designee has informed the individual of the termination.

5. **Security Exception.** The FIU facilities and programs shall only undertake a practice likely to interfere with the Access, Exchange, or Use of EHI in order to protect the security of EHI when the following conditions are met:

5.1 The practice directly relates to safeguarding the confidentiality, integrity, and availability of EHI;

5.2 The practice is tailored to the specific security risk being addressed;

5.3 The practice is implemented in a consistent and non-discriminatory manner; and

5.4 The practice either:

(a) Implements a written FIU security policy that has been prepared on the basis of, and is directly responsive to, security risks identified and assessed by or on behalf of the FIU facility or program, aligns with one or more applicable consensus-based standards or best practice guidelines, and provides objective timeframes and other parameters for identifying, responding to, and addressing security incidents; or

(b) Does not implement an FIU security policy and FIU has made a determination in each case, based on the particularized facts and circumstances, that the practice is necessary to mitigate the security risk to EHI and there are no reasonable and appropriate alternatives to the practice that address the security risk that are less likely to interfere with, prevent, or materially discourage Access, Exchange, or Use of EHI.

6. **Infeasibility Exception.** The FIU facilities and programs shall only undertake a practice of not fulfilling a request to Access, Exchange, or Use EHI due to the infeasibility of the request when one or more of the following conditions are met:

6.1 **Conditions.** One of the following:

(a) **Uncontrollable events.** The FIU facility or program cannot fulfill the request due to natural or humanmade disaster, public health emergency, public safety incident, war, terrorist attack, civil insurrection, strike or other labor unrest, telecommunication or internet service interruption, or act of military, civil or regulatory authority;

(b) **Segmentation.** (Also see FIU Policy and Procedure #1660.050) (Patient Access to Protected Health Information). The FIU facility or program cannot fulfill the request because the facility or program Medical Records Manager, or designee cannot unambiguously segment the requested EHI from EHI that either cannot be made available due to an individual's performance, cannot be made available

by law, or may be withheld in accordance with the **Preventing Harm Exception** in Section 3 above.

(c) **Infeasible under the circumstances.** The FIU facility or program demonstrates, prior to responding to the request as required by this Policy and Procedure, through a contemporaneous written record or other documentation, its consistent and non-discriminatory consideration of the following factors that led to its determination that complying with the request would be infeasible under the circumstances, and in determining whether the circumstances were infeasible, the Facility and program has not considered whether the manner requested would have facilitated competition with the facility or program and whether the manner requested would have prevented the facility or program from charging a fee or resulted in a reduced fee:

- The type of EHI and the purposes for which it may be needed;
- The cost to the FIU facility or program in complying with the request;
- The financial and technical resources available to the facility or program;
- Whether the facility or program practice is non-discriminatory, and the facility or program provides the same Access, Exchange, or Use of EHI to its patients, suppliers, partners, and other persons with whom it has a business relationship;
- Whether the facility or program owns or has control over a predominant technology, platform, Health Information Exchange, or Health Information Network through which EHI is Accessed or Exchanged; and
- Why the facility or program was unable to provide Access, Exchange, or Use of EHI consistent with the **Content and Manner Exception** in Section 8 below.

6.2 **Responding to requests.** (See FIU Policy and Procedure #1660.050) (Patient Access to Protected Health Information). If an FIU facility or program does not fulfill a request for Access, Exchange, or Use due to infeasibility, the facility or program Medical Records Manage, or designee must, within **ten (10) business days** of receipt of the request, provide to the requestor in writing the reasons why the request is infeasible.

7. **Health IT Performance Exception.** The FIU facilities and programs shall only undertake a practice implemented to maintain or improve health IT performance and that is likely to interfere with the Access, Exchange, or Use of EHI when one of the following conditions are met, as applicable to the particular practice and the reason for its implementation:

7.1 **Maintenance and improvements to health IT.** When FIU, a facility or a program implements a practice that makes health IT under FIU's, the facility's or program's control temporarily unavailable, or temporarily degrades the performance of health IT, in order to perform maintenance or improvements to the health IT, the practice must be:

(a) Implemented for a period of time no longer than necessary to complete the maintenance or improvements for which the health IT was made unavailable or the health IT's performance degraded;

(b) Implemented in a consistent and non-discriminatory manner; and

(c) If the unavailability or degradation is initiated by a health IT developer of certified health IT, Health Information Exchange, or Health Information Network, the unavailability or degradation, whether planned or unplanned, is consistent with applicable existing service level agreements.

7.2 **Assured level of performance.** FIU may not take action against a third-party application that is negatively impacting the health IT's performance, provided that the practice is:

(a) For a period of time no longer than necessary to resolve any negative impact(s);

(b) Implemented in a consistent and non-discriminatory manner; and

(c) Consistent with existing service level agreements, where applicable.

7.3 **Practices that prevent harm.** If the unavailability of health IT for maintenance or improvements is initiated by FIU, a facility or a program in response to **risk of harm** to a patient or another person, the facility or program does not need to satisfy the requirements of the **Health IT Performance Exception** but must comply with all requirements of the **Preventing Harm Exception** at all relevant times to qualify for an exception.

7.4 **Security-related practices.** If the unavailability of health IT for maintenance or improvements is initiated by FIU, a facility or program in response to a security risk to EHI, FIU, the facility or program does not need to satisfy the requirements of the **Health IT Performance Exception** but must comply with all requirements of the **Security Exception** at all relevant times to qualify for an exception.

8. **Content and Manner Exception.** (See FIU Policy and Procedure #1660.050) (Patient Access to Protected Health Information). The FIU facility and program Medical Records Manager, or designee shall only undertake a practice of limiting the content of its

response to or the manner in which it fulfills a request to Access, Exchange, or Use of EHI when the following conditions are met:

8.1 **Content condition.** The facility or program Medical Records Manager, or designee must respond to a request to Access, Exchange, or Use EHI.

8.2 **Manner condition.** The facility or program is technically unable to fulfill the request or cannot reach agreeable terms with the requestor to fulfill the request.

(a) **Manner requested.** When the facility or program Medical Records Manager, or designee fulfills a request in any manner requested, any **fees charged** must comply with HIPAA, and Florida state statues, whichever rules charge the lesser fee.

(b) **Alternative manner.** If the facility or program Medical Records Manager, or designee does not fulfill a request in any manner requested because it is technically unable to fulfill the request or cannot reach agreeable terms with the requestor to fulfill the request, the Medical Records Manager, or designee shall fulfill the request in an alternative manner as follows:

- Without unnecessary delay in the following order of priority:
  - o using technology certified according to applicable regulation that is specified by the requestor,
  - o using content and transport standards specified by the requestor and published by the Federal Government or a standards developing organization accredited by the American National Standards Institute,
  - o using an alternative machine-readable format, including the means to interpret the EHI, agreed upon with the requestor.
- Any fees charged in relation to fulfilling the request are required to satisfy the **Fee Exception**.
- Any license of Interoperability Elements granted by FIU in relation to fulfilling the request is required to satisfy the **License Exception**.

9. **Fees Exception.** The FIU facilities and programs shall only undertake a practice of charging fees as permitted and limited by the HIPAA Privacy Rule and Florida state statute.

9.1 **Basis for fees condition.** The fees the FIU facilities and programs charges must be based on:

- objective and verifiable criteria that are uniformly applied for all similarly situated classes of persons or entities and request.

(a) The fee charges must not be based on:

- whether the requestor or other person is a competitor, potential competitor, or will be using the EHI in a way that facilitates competition with the FIU facility or program.

10. **Licensing Exception.** The provision does not apply to FIU because FIU does not engage in a practice to license Interoperability Elements for EHI Access, Exchange, or Use.

11. To ensure all relevant conditions of an allowable exception apply, Workforce Members shall contact the Director of Compliance and Privacy for Health Affairs with the University Compliance & Integrity and/or the HIPAA Security Officer with the FIU Division of Information Technology, for advice and guidance when considering FIU facilities and programs engagement in a new, not previously reviewed, practice that may interfere with Access, Exchange, or Use of EHI.

Record Retention

FIU facilities and programs must maintain patient Protected Health Information in either paper or electronic form, provided that any format is sufficiently protected to ensure it will be retrievable throughout the required retention period of seven (7) years from the date of its creation, or the last effective date, whichever is later. (See FIU Policy and Procedure #1660.080) (Policies and Procedures, Changes to Policies and Procedures, and Documentation).