FLORIDA INTERNATIONAL UNIVERSITY

OFFICIAL UNIVERSITY POLICY

Information Blocking # 1660.170

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

POLICY STATEMENT

The HIPAA Privacy Rule provides a federal floor of privacy protections for individually identifiable health information held by a covered entity, covered component, or by a Business Associate of a covered entity or 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 These Florida state statutes, although contrary to the HIPAA Privacy Rule, are not superseded by HIPAA.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)).

The FIU Health Insurance Portability and Accountability Act (HIPAA) Hybrid Designated Healthcare Components/Units (Components/Units) 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 Component/Unit 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 Personal 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 Component/Unit Medical Records Manager, or designee.

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

4. The Component/Unit Medical Records Manager, or designee may ask third parties requesting to 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 Component/Unit can furnish the requested EHI; and

   c. whether the Component/Unit 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 Component/Unit 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 Components/Units will implement this Policy and Procedure and inform its Workforce members as it applies to their individual roles.

The Components/Units 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 Components/Units will:

1. Coordinate with health IT vendors to identify and implement (if not already in place) health IT solutions that the Component/Unit 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 Component's/Unit's 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 Component/Unit 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. 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 and state law and regulation.

SCOPE

This Policy applies to FIU's HIPAA Hybrid Designated Healthcare Components/Units.

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 Components/Units 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 Components/Units applies allowable exceptions and meets all conditions of such exceptions before engaging in a practice that may otherwise constitute Information Blocking.

DEFINITIONS	
TERM	**DEFINITIONS**
Access	Ability or means necessary to make Electronic Health Information (EHI) available for Exchange or Use.
Actor	A Health Care Provider, HIE/HIN or Health IT Developer of Certified Health IT. (Also see Healthcare Provider/Professional)
Availability	Means the property that data or information is accessible and useable upon demand by an authorized person.
Business Associate	Generally, an entity or person who performs a function involving the use or disclosure of Protected Health Information (PHI) on behalf of a covered entity (such as claims processing, case management, utilization review, quality assurance, billing) or provides services for a covered entity that require the disclosure of PHI (such as legal, actuarial, accounting, accreditation). **NOTE:** A business associate relationship exists when an individual or entity, acting on behalf of an FIU HIPAA Component(s), assists in the performance of a function or activity involving the creation, use, disclosure, or access of PHI. This includes, but not limited to, claims processing or administration, data analysis, utilization review, quality assurance, billing, benefit management or repricing. **NOTE:** A Business Associate may include any individual or entity that receives PHI from a HIPAA Component in the course of providing legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, software support, or financial services. A Business Associates does not, however, include HIPAA Component workforce members.
Patient	The person who is the subject of PHI.

Code of Federal Regulations	Also known as CFR
Component	Means a component or combination of components of a hybrid entity designated by the hybrid entity (Florida International University). Those programs designated by FIU that must comply with the requirements of the Health Insurance Portability and Accountability Act of 1996, hereinafter referred to as "Components". Components of FIU are required to comply with the Administrative Simplification provisions of HIPAA because the Components perform a covered function.
Confidentiality	Means data or information is not made available or disclosed to unauthorized persons or processes.
Covered Entity	An entity that is subject to HIPAA. 1. a health plan; 2. a health care clearinghouse; and/or 3. a health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.
Disclosure	Means the release, transfer, provision of access to, or divulging in any other manner of protected health information outside of the entity holding the information.
Designated Record Set	A group of records maintained by or for a covered entity that may include patient medical and billing records; the enrollment, payment, claims, adjudication, and cases or medical management record systems maintained by or for a health plan; or information used in whole or in part to make care-related decisions.
Electronic Access	Means an internet-based method that makes EHI available at the time the EHI is requested and where no manual effort is required to fulfill the request.
Electronic Protected Heath Information (ePHI)	PHI in electronic form. See also: PHI. Electronic Protected Health Information (ePHI) to the extent that it would be included in Florida International University Healthcare Components/Units Designated Record Set, regardless of whether the group of records are used or maintained by Florida International University Healthcare Components/Units. EHI does not include: • Psychotherapy Notes; or • Information complied in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding.

	Any Protected Health Information that is produced, saved, transferred or received in an electronic form, including payment information or demographic information collected from an individual.
Electronic Health Information (EHI)	Means electronic Protected Health Information to the extent that it would be included in a Designated Record Set, regardless of whether the group of records are used or maintained by or for a Covered Entity, but EHI does not include: (1) Psychotherapy Notes; or (2) information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding. EHI excludes de-identified information (as defined in the model policy attached to the Patient Privacy Program Requirements Policy, IP.PRI.001). Examples of EHI include electronic Protected Health Information found in medical records, billing records and other information used to make decisions about patients. EHI for the purposes of the information blocking definition is limited to the data elements represented in the USCDI standard. Beginning October 6, 2022, the EHI definition was expanded and represents the same EPHI that a patient would have the right to request a copy of pursuant to the HIPAA Privacy Regulation.
Exchange	Ability for EHI to be transmitted between and among different technologies, systems, platforms, or networks.
Florida Statutes	Also known as F.S. is a permanent collection of state laws organized by subject area into a code made up of titles, chapters, parts, and sections.
Health Care Component	See "Component"
Health Care Operations	Means any of the following activities: 1. quality assessment and improvement activities, including case management and care coordination; 2. competency assurance activities, including provider or health plan performance evaluation, credentialing, and accreditation; 3. conducting or arranging for medical reviews, audits, or legal services, including fraud and abuse detection and compliance programs; 4. specified insurance functions, such as underwriting, risk rating, and reinsuring risk; 5. business planning, development, management, and administration; and

	6. business management and general administrative activities of the entity, including but not limited to: a. de-identifying protected health information, b. creating a limited data set, and c. certain fundraising for the benefit of the covered entity.
Health Care Provider/Professional	Means a provider of medical or health services and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business. The Final Rule generally speaks in terms of "actors," of which one type is a healthcare provider. The term "healthcare provider" includes a hospital, skilled nursing facility, nursing facility, home health entity or other long term care facility, healthcare clinic, community mental health center, renal dialysis facility, blood center, ambulatory surgical center, emergency medical services provider, Federally qualified health center, group practice, a pharmacist, a pharmacy, a laboratory, a physician, a practitioner, a provider operated by, or under contract with, the Indian Health Service or by an Indian tribe, tribal organization, or urban Indian organization, a rural health clinic, a covered entity under the 340B Drug Pricing Program, an ambulatory surgical center, and a therapist.
U.S. Department of Health and Human Services	Also known as HHS is a federal agency with the mission of to enhance the health and well-being of all Americans, by providing for effective health and human services and by fostering sound, sustained advances in the sciences underlying medicine, public health, and social services.
Health Information	Means any information, whether oral or recorded in any form or medium, that is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and relates to the past, present, or future physical or mental health or condition of an patient/client; the provision of health care to an patient/client; or the past, present, or future payment for the provision of health care to an patient/client.
Health Information Exchange/Health Information Network	An individual or entity that determines, controls, or has the discretion to administer any requirement, policy, or agreement that permits, enables, or required the use of any technology or services for Access, Exchange, or Use of EHI: (1) Among more than two unaffiliated individuals or entities (other than the individual

	or entity to which this definition might apply) that are enabled to Exchange with each other; and (2) That is for treatment, payment, or health care operations purposes regardless of whether such individuals or entities are subject to the requirements of 45 CFR parts 160 and 164.
Health Information Technology	Health Information Technology: Hardware, software, integrated technologies or related licenses, intellectual property, upgrades, or packaged solutions sold as services that are designated for or support the use by health care entities or patients for the electronic creation, maintenance, Access, or Exchange of health information.
Health IT Developer of Certified Health IT	Health IT Developer of Certified Health IT: An individual or entity, other than a Health Care Provider that self-developed health IT for its own use, that develops or offers Health Information Technology and which has, at the time it engages in a practice that is the subject of an Information Blocking claim, one or more Health IT Modules certified under a program for the voluntary certification of Health Information Technology that is kept or recognized by the National Coordinator pursuant to 42 U.S.C. 300jj-11(c)(5) (ONC Health IT Certification Program).
HIPAA	Means the Health Insurance Portability and Accountability Act of 1996.
Hybrid Covered Entity	Means a single legal entity that performs both covered and non-covered functions. The entity has a defined health care component that engages in HIPAA electronic transactions.
Information Blocking	"Information blocking" by a healthcare provider means a Practice that: (i) Except as required by law or covered by an exception set forth in federal regulations, is likely to interfere with Access, Exchange, or use of EHI; and (ii) The healthcare provider knows is unreasonable and is likely to interfere with, prevent, or materially discourages Access, Exchange, or Use of EHI. "Information blocking" by a health IT developer, health information network or health information exchange means a practice that (i) except as required by law or covered by an exception set forth in federal regulations, is likely to interfere with access, exchange, or use of EHI; and (ii) the developer, network or exchange knows, or should know, is likely to interfere with, prevent, or materially discourage access, exchange, or use of EHI.
Interfere with or Interference	Means to prevent, materially discourage, or otherwise inhibit.

Practice	Means an act or omission by an actor.
Privacy Coordinator	Means an FIU Workforce member, appointed by the director, manager, or supervisor of a HIPAA Designated Component to conduct and/or coordinate with necessary and appropriate Workforce members all HIPAA Privacy Rule activities and actions within the Component, including but not limited to tracking HIPAA training activities; coordinating HIPAA Privacy Rule implementation; participating in HIPAA Privacy and Security Rule violation investigations, as necessary and appropriate, communicating with the Director of Compliance and Privacy for Health Affairs, the HIPAA Security Officer, and the Office of General Counsel, as necessary and appropriate, regarding HIPAA Privacy and Security Rule activities and concerns; conducting and reporting monitoring activities; participate in assessments; and responding to, tracking and documenting HIPAA Privacy Rule activities. Maintain ongoing communication with the Director of Compliance and Privacy for Health Affairs and the HIPAA Security Officer.
Protected Health Information (PHI)	Means any individually identifiable health information collected or created in the course of the provision of health care services by a covered entity, in any form (written, verbal or electronic). PHI relates to the past, present, or future physical or mental health or condition of an individual or the past, present, or future payment for the provision of health care to an individual. Protected Health Information however specifically excludes: 1. Education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. § 1232g ("FERPA"); 2. Records described at 20 U.S.C. § 1232g(a)(4)(B)(iv); and 3. Employment records held by a covered entity in its role as an employer.
Privacy Rule	The regulations at 45 CFR 160 and 164, which detail the requirements for complying with the standards for privacy under the administrative simplification provisions of HIPAA.
Standard	Means a rule, condition, or requirement: 1. Describing the following information for products, systems, services, or practices: a. Classification of components. b. Specification of materials, performance, or operations; or c. Delineation of procedures; or 2. With respect to the privacy of protected health information.

The United States Core Data for Interoperability (USCDI)	The United States Core Data for Interoperability (USCDI) is a standardized set of health data classes and constituent data elements for nationwide, interoperable health information exchange.
Use	With respect to patient/client identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information. Ability for EHI, once Accessed or Exchanged, to be understood and acted upon.
Workforce	Means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity (FIU HIPAA Component) or business associate, is under the direct control of such covered entity or business associate, whether or not they are paid by the covered entity or business associate.

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 (FIU HIPAA Hybrid Designation)
- 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 (Component Privacy Coordinators)
- FIU Policy and Procedure #1660.080 (Record Retention and Complaints)
- FIU Policy and Procedure #1660.085 (Sanctions)
- FIU Policy and Procedure #1660.105 (Class of Workforce members Who Require Access to PHI)
- FIU Policy and Procedure #1660.115 (Destruction and Disposal of PHI)
- FIU Policy and Procedure #1660.120 (Minimum Necessary)

CONTACTS

For further information concerning this policy, please contact the FIU Office of Compliance & Integrity at (305) 348-2216, the appropriate Component/Unit Privacy Coordinator, or at hipaaprivacy@fiu.edu.

HISTORY

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

Information Blocking # 1660.170a

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

PROCEDURE

1. The FIU HIPAA Hybrid Designated Healthcare Component/Unit (Component/Unit) 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 Component/Unit 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 Component/Unit 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 Component/Unit 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 (Representative))*. 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 Component/Unit 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 Component/Unit 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 Component/Unit 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 Component/Unit 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 Component/Unit 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.** *(Also 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 Components/Units 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 Component/Unit Workforce member(s);

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

(c) The Component/Unit practice is implemented in a consistent and non-discriminatory manner; and

(d) The Component/Unit 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 Component/Unit Medical Records Manager, or designee; or
- The Component/Unit 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 Component/Unit Medical Records Manager, or designee has informed the individual of the termination.

5. **Security Exception.** The FIU Components/Units 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 Component/Unit, 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 Components/Units 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 Component/Unit 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 Component/Unit cannot fulfill the request because the Component/Unit 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 Component/Unit 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 Component/Unit has not considered whether the manner requested would have facilitated competition with the Component/Unit and whether the manner requested would have prevented the Component/Unit 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 Component/Unit in complying with the request;
- The financial and technical resources available to the Component/Unit;
- Whether the Component/Unit practice is non-discriminatory, and the Component/Unit 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 Component/Unit 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 Component/Unit 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.** *(Also see FIU Policy and Procedure #1660.050 (Patient Access to Protected Health Information).* If an FIU Component/Unit does not fulfill a request for Access, Exchange, or Use due to infeasibility, the Component/Unit 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 Components/Units 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 or a Component/Unit implements a practice that makes health IT under FIU'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 or the Component/Unit in response to **risk of harm** to a patient or another person, the Component/Unit 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 or the Component/Unit in response to a security risk to EHI, FIU or the Component/Unit 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.** (Also see FIU Policy and Procedure #1660.050 (patient Access to Protected Health Information)). The FIU Component/Unit 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 Components/Units Medical Records Manager, or designee must respond to a request to Access, Exchange, or Use EHI.

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

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

(b) **Alternative manner.** If the Component/Unit 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 Component/Unit 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 by the FIU Component/Unit 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 Components/Units 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 Components/Units 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 Components/Units.

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 Components/Units engagement in a new, not previously reviewed, practice that may interfere with Access, Exchange, or Use of EHI.

Record Retention

FIU Components/Units 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)).