SCOPE
This policy applies to Florida Atlantic University’s Covered Components and those working on behalf of the Covered Components for purposes of complying with the privacy provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

POLICY STATEMENT
FAU’s workforce providing health care services, performing health care operations or handling PHI in the course or scope of their employment or engagement must make reasonable efforts to limit the use, disclosure and request for protected health information (PHI) to the minimum necessary to accomplish the intended purpose of the use, disclosure or request.

REASON FOR THE POLICY
To establish that FAU will make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure or request.

DEFINITIONS
Authorization – Permission given by the individual to use and/or disclose protected health information about the individual. The requirements of a valid authorization are defined by the HIPAA regulations.

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).

Covered Component – health care components of a Hybrid Entity, named and designated by the Hybrid Entity, that engage in Covered Functions, and any component that engages in activities that would make it a Business Associate of a Covered Component if the two components were separate legal entities.

Covered Entity – A health plan, a health care provider, or a health care clearinghouse who transmits any health information in electronic form in connection with a transaction covered by the Privacy Rule.
**Disclose or Disclosure**: The release, transfer, provision or access to, or divulging in any other manner of information outside the entity holding the information.

**Health Care Operations** – Any of the following activities of a covered entity that relate to its covered functions:
1. Conducting Quality Assessment and Improvement activities, including the following: outcomes evaluation and development of clinical guidelines; patient safety activities, population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination; and contacting health care providers and patients with information about treatment alternatives;
2. Reviewing the competence or qualifications of health care professionals including the following: evaluating practitioner and provider performance; conducting training programs; accreditation; certification; licensing; or credentialing activities;
3. Underwriting (except as prohibited under 45 CFR §164.502 (a)(5)(i)(e.g., involving genetic information)), enrollment, premium rating, and other activities related to the creation, renewal, or replacement of a contract of health insurance of health benefits, and ceding, securing or placing a contract for reinsurance of risk relating to claims for health care;
4. Conducting or arranging for medical review, legal services and auditing functions including fraud and abuse detection and compliance programs;
5. Business planning and development such as conducting cost-management and planning-related analyses related to managing and operating the entity; and
6. Business management and general administrative activities including the following: management activities relating to implementation of and compliance with the requirements of the privacy regulations; customer service; resolution of internal grievances; the sale, transfer, merger, or consolidation of all or part of the covered entity; and creating de-identified health information or a limited data set; and fundraising for the benefit of the covered entity.

**Legally Authorized Representative** – A person authorized either by state law or by court appointment to make decisions, including decisions related to health care, on behalf of another person, including someone who is authorized under applicable law to consent on behalf of a prospective subject to the subject’s participation in the procedure involved in the research.

**Minimum Necessary** – Reasonable efforts made to limit the use, disclosure, or request for PHI to the minimum necessary to accomplish the intended purpose.

**Payment** – The activities undertaken by a:
1) Health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; or
2) Covered health care provider or health plan to obtain or provide reimbursement for the provision of health care.
**Protected Health Information (PHI)** – Individually identifiable health information collected from an individual that is: 1) transmitted by electronic media; 2) maintained in electronic media; or 3) transmitted or maintained in any other form or medium by a Covered Entity.

PHI encompasses information that identifies an individual or might reasonably be used to identify an individual and relates to: the individual’s past, present or future physical or mental health or condition of an individual; the provision of health care to the individual; or the past, present or future payment of health care to an individual.

PHI excludes individually identifiable health information in: a) education records covered by the Family Educational Rights and Privacy Act (FERPA); b) records described at 20 U.S.C. §1232g(a)(4)(B)(iv); c) employment records held by a covered entity in its role as employer; and d) regards to a person who has been deceased for more than 50 years.

**TPO** – Treatment, payment and health care operations. The HIPAA Privacy Rule permits disclosure of PHI only for TPO or when a regulatory exception applies (e.g., public health reporting).

**Treatment** – The provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one provider to another.

**Use** – The sharing, employment, application, utilization, examination, or analysis of individually identifiable information within an entity that maintains or holds such information.

**APPLICABILITY**

Minimum necessary applies when FAU uses or discloses PHI or when FAU requests PHI from another covered entity or business associate. A covered entity or business associate must make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure or request.

**EXEMPTIONS**

“Minimum Necessary” does not apply to the following uses, disclosures or requests:

1. Disclosures to or requests by a health care provider for treatment;
2. Uses or disclosures made to the individual or the individual’s legally authorized representative;
3. Uses or disclosures made pursuant to an authorization signed by the individual or the individual’s legally authorized representative;
4. Disclosures made to the Secretary of Health and Human Services to determine FAU’s compliance with the Privacy Rule;
5. Uses or disclosures that are required for compliance with HIPAA regulations; or
6. Uses or disclosures that are required by law.
LIMITATIONS
Identifying persons, classes and categories relating to minimum necessary use
FAU will identify the persons or classes of persons in its workforce who need access to PHI to carry out their duties and responsibilities and will make reasonable efforts to limit the access of such persons or classes of persons to a category or categories of PHI to which access is needed and establish any conditions appropriate to such access. Departments should develop and maintain a list of categories of persons and organizations to which PHI is routinely disclosed or from which information is routinely requested, the purpose of the disclosures and requests and the minimum information needed for each purpose.

Limitations related to disclosures
Routine disclosures should only be for the purposes of treatment, payment and health care operations. Non-routine disclosures should be reviewed carefully and authorized to the extent reasonably necessary to achieve the purpose of the disclosure.

Limitations related to requests
Routine requests for PHI should be constructed to limit the PHI requested to the amount reasonably necessary to accomplish the purpose for which the request is made. FAU must limit any request for PHI to that which is reasonably necessary to accomplish the purpose for which the request is made, when requesting such information from other covered entities. Non-routine requests should be reviewed carefully to determine the minimum necessary information needed to fulfill the purpose. Any PHI requested from another person or organization that is not specifically for treatment should be made only with the patient’s authorization.
This policy does not cover authorizations and the process of review, approval or waiver by an institutional review board for research purposes. Refer to the Division of Research and their policies for conditions under which FAU faculty, staff, students, residents, post-doctoral fellows and non-employees may obtain, create, use or disclose PHI for research purposes.

In General
The entire health record should not be used, disclosed or requested unless it is specifically required for the intended purpose or for treatment of the patient.

All access to PHI must be documented and all staff must be educated about their department’s minimum necessary procedures.

Retention
FAU’s Covered Components will retain any related documentation for a minimum period of 6 years.

PROCEDURES
FAU Covered Components will identify and define the following:
1. The persons or classes of persons in the FAU Personnel who need access to PHI to carry out their duties based on their role(s). (e.g., clinicians, administration, billing staff, etc.)

2. The category or categories of PHI to which access is needed, based on their role(s).

3. Each Covered Component will identify and define the category and level of access suitable to its needs and consistent with this policy and minimum necessary use.

All workforce members handling or dealing with PHI will be assigned to the appropriate security groups within the Electronic Medical Record that delineates specific access and actions the staff member is authorized to perform when assigned to that security group. The security groups to which a staff member is assigned should be periodically reviewed and updated to reflect any changes in job duties or assignments.

Each FAU covered component must establish procedures for all workforce members to receive education and training on PHI and the rights and responsibilities regarding his/her access to PHI, at the time of hire and at least annually. The security group to which a member is assigned should be regularly reviewed and updated if necessary (e.g. re-assignments, new job duties assigned, etc.).

Each FAU covered component must establish procedures to remove access to electronic medical records any time a work force member resigns or is separated from the unit.
**MINIMUM NECESSARY DECISION TREE**

<table>
<thead>
<tr>
<th>Ask:</th>
<th>If the answer is “NO”</th>
<th>If the answer is “YES”</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is the intended use, request, or disclosure being made for or by a healthcare provider for treatment purposes?</td>
<td>Go to the next question</td>
<td>The Minimum Necessary Rule does NOT apply.</td>
</tr>
<tr>
<td>Is the use or disclosure being made to the individual, who is the subject of the PHI?</td>
<td>Go to the next question</td>
<td>The Minimum Necessary Rule does NOT apply.</td>
</tr>
<tr>
<td>Is the use or disclosure being made in response to a valid authorization?</td>
<td>Go to the next question</td>
<td>The Minimum Necessary Rule does NOT apply.</td>
</tr>
<tr>
<td>Has HHS requested disclosure for purposes of HIPAA enforcement or compliance?</td>
<td>Go to the next question</td>
<td>The Minimum Necessary Rule does NOT apply.</td>
</tr>
<tr>
<td>Is the use or disclosure required by law (i.e., reporting abuse, neglect or domestic violence, responding to a court order or subpoena, or in response to a law enforcement officer investigating a crime)?</td>
<td>The information to be used, disclosed, or requested must abide by the Minimum Necessary Rule. Verify identity and authority.</td>
<td>Certain other restrictions apply under HIPAA, but not the Minimum Necessary Rule.</td>
</tr>
</tbody>
</table>

**EXAMPLES OF ROUTINE AND NON-ROUTINE DISCLOSURES AND REQUESTS**

<table>
<thead>
<tr>
<th>Routine Disclosures</th>
<th>What to Disclose</th>
<th>Routine Requests</th>
<th>What to Request</th>
</tr>
</thead>
<tbody>
<tr>
<td>Treatment Purposes</td>
<td>Disclosures</td>
<td>Generally limit PHI to patient name, demographics, appropriate diagnosis information, and reason for referral/prescription</td>
<td>Requests for PHI from referring physicians and other health care practitioners</td>
</tr>
<tr>
<td></td>
<td>associated with routine referrals to local laboratories, pharmacies, rehab facilities, etc.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Payment Purposes</td>
<td>Disclosures</td>
<td>Limit information to records for the date of service in question</td>
<td>Requests for pre-approval and eligibility determinations</td>
</tr>
<tr>
<td></td>
<td>for billing/reimbursement purposes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Required by Law</td>
<td>Non-Routine Disclosures</td>
<td>What may be Disclosed</td>
<td>Non-Routine Requests</td>
</tr>
<tr>
<td>---------------------------------------------------------------------------------</td>
<td>-------------------------</td>
<td>---------------------------------------------------------------------------------------</td>
<td>----------------------</td>
</tr>
<tr>
<td>Disclosures for public health activities</td>
<td></td>
<td>Limit information to the specific data required by the agency. Only information related to the specific incident being reported or investigated. Additional information including patient’s history may only be disclosed by court order or subpoena.</td>
<td></td>
</tr>
<tr>
<td>Disclosures relating to victims of crime or abuse</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Non-Routine Disclosures</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Payment Purposes</td>
<td>Disclosures for billing/reimbursement activities of another health care provider</td>
<td>Disclose no information without patient’s authorization</td>
<td>Requests for billing/reimbursement activities of another health care provider</td>
</tr>
<tr>
<td>Required by law</td>
<td>Disclosures in response to court orders or subpoenas</td>
<td>Limit disclosures to the specific information contained in the order or subpoena</td>
<td></td>
</tr>
</tbody>
</table>