Technical Safeguards and Authentication Policy
June 7, 2016

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

POLICY
FAU shall implement technical safeguards to prevent, detect, contain and correct any HIPAA Security Rule violations in accordance with this policy.

REASON FOR POLICY
To establish technical safeguards to comply with the HIPAA Security Rule.

DEFINITIONS- Refer to Glossary and Terms

PROCEDURE

1. Technical Access Controls.

    a. Unique User Identification.

        i. Workforce members authorized to access electronic protected health information ("e-PHI") are assigned a unique User ID that enables FAU's information system to identify, authenticate and track user identity and access to FAU's information systems and e-PHI.

        ii. Workplace members may not allow anyone to use their User ID to gain access to FAU's information systems under any circumstance.

        iii. Workplace members may not misrepresent themselves to FAU's information systems by using another person's User ID.

        iv. Workplace members are required to follow any password management policies and procedures to create and safeguard their User ID to prevent unauthorized access to FAU's information systems.

        v. User accounts are established consistent with administrative policies and procedures that grant access privileges.

        vi. Access control lists are maintained and updated as needed, and technical

modifications to user accounts are provided in a timely manner when access privileges are terminated or changed.

b. Emergency Access Procedure.

i. Temporary access to e-PHI or FAU's information systems may be provided in emergencies.

ii. FAU's Contingency Plan describes FAU's emergency access procedures.

2. Integrity of e-PHI. These HIPAA Policies and Procedures are designed to protect e-PHI from improper alteration or destruction.

3. Transmission Security.

a. E-PHI may only be transmitted to authorized parties.

b. When e-PHI must be transmitted in email communications, only the minimum amount of protected health information needed to achieve the purpose of the communication should be transmitted and only in an encrypted state consistent with officially-approved procedures or mechanisms defined by the FAU HIPAA Taskforce.

c. A compatible encryption method approved by the Information Security Officer must be coordinated with the recipient of email communications containing e-PHI that is transmitted over an electronic communications network.

d. When transmitting e-PHI in email communications, the following statement should be included in the email as an extra precaution:

The information contained in this transmission may contain privileged and confidential information, including patient information protected by federal and state privacy laws. It is intended only for the use of the person(s) named above. If you are not the intended recipient, you are hereby notified that any review, dissemination, distribution, or duplication of this communication is strictly prohibited. If you are not the intended recipient, please contact the sender by reply email, report the error to FAU's Chief Compliance Officer, and destroy all copies of the original message.

REFERENCES: Acceptable Use of Technology Resources (FAU Policy 12.2).