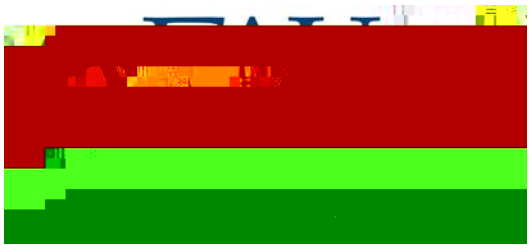

**Technical Safeguards and Authentication Policy**
June 7, 2016

**SCOPE**
This policy applies to Florida Atlantic University's Covered Components and those working on behalf of the Covered Components (collectively "FAU") for purps ' (c S c e D ɔ
olations in accordance with this policy.

**POLICY**
nnical safeguards to comply with the HIPAA Security Rule.

**-** Refer to Glossary and Terms

l Access Controls.

Unique User Identification.

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.

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

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

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.

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

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 de