Section 1: GENERAL PRIVACY RULES

1.4 Maintaining Confidentiality of Health Information

POLICY

1. **Commitment:** The University of Florida (UF) is committed to safeguarding the confidentiality of protected health information (PHI) so that any PHI created, received, or maintained by UF is only used or disclosed in accordance with UF's policies and federal and state regulations.
2. **Scope:** Every person at UF with access to PHI in any format, including without limitation, paper, electronic, graphic, video, oral/sign language, or any other format, is responsible for safeguarding its confidentiality, and for complying with all health information privacy and security policies and procedures approved by UF.
3. **Application:** UF places significant trust in all who have access to PHI and, with that trust, comes a high level of responsibility:
4. **Uses and disclosures** of PHI for any purposes other than those authorized by the individual or permitted or required under HIPAA as described in UF Privacy Policies may constitute a privacy violation.
5. **Violations** may result in immediate disciplinary action up to and including termination of employment and/or expulsion from academic programs by UF.

DEFINITIONS

Confidentiality: The practice of controlling data or information such that it is not made available or disclosed to unauthorized persons or processes.

PRIVACY REQUIREMENTS

1. Authorization and/or supervision: Implement procedures for the authorization and/or supervision of workforce members who work with electronic PHI or in locations where it might be accessed.
2. Limited Access: Access to PHI must be limited to those persons who have a valid business or health care need for the information, or otherwise have a right to know the information.
3. Limited Uses and Disclosures: Health and financial information about patients, which becomes known to employees, volunteers, and students through authorized work- or study-related processes, must not be used for any purpose other than the completion of assigned or approved functions.
4. Mandatory Training for Workforce Members: All members of the healthcare workforce must be trained regarding the privacy and security policies and procedures as necessary and appropriate for them to carry out their functions.
5. Minimum necessary uses of protected health information: A covered entity must identify those persons or classes of persons, as appropriate, in its workforce who need access to PHI to carry out their duties; and for each such person or class of persons, the category or categories of PHI to which access is needed and any conditions appropriate to such access. A covered entity must make reasonable efforts to limit the access of such persons or classes to PHI consistent with the established need.
6. Report: any known or suspected privacy or security violations involving UF's health information to the appropriate UF Privacy Office immediately, using the Privacy Incident reporting system.
7. Safeguards: A covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of PHI.

8. Security: All PHI created, received, or maintained by UF must be secured and protected at all times from unauthorized access, damage, loss, alteration, and tampering.
9. Workforce access procedure: Implement procedures to determine that the access of a workforce member to electronic PHI is appropriate.
10. Workforce access termination procedures: Implement procedures for terminating access to electronic PHI when the employment of, or other arrangement with, a workforce member ends. See also 1.5 Privacy Safeguards.
11. Workforce Security: A covered entity or business associate must implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic PHI… and to prevent those workforce members who do not have access… from obtaining access to electronic PHI.

REFERENCES

1. Florida Statutes: 501.171(g) (Security of confidential personal information).
2. HIPAA Regulations: 45 CFR §160.103 – Definitions; § 164.308 – Administrative safeguards: (a)(3) Workforce Security, (a)(4) Information Access Management, §164.514(d) (Minimum Necessary Requirements), §164.530(b) Training and (e) Sanctions.
3. UF Information Technology Acceptable Use Policy, UF Information Security Policies

EXHIBITS

None