SECTION 6: OTHER PRIVACY POLICIES AND PROCEDURES

6.6 Student Data Access – Electronic Health Records

POLICY

The University of Florida (UF) Privacy Office and Identity Access Management (IAM), along with applicable departmental and clinical leadership, shall collaborate to provision appropriate, role-based access to protected health information (PHI) and other Restricted Data.

The scope of this policy includes UF students and students from other colleges with an academic relationship with UF. This policy does not apply to EMR systems operated by the College of Dentistry, the College of Nursing, or the College of Veterinary Medicine.

GENERAL INFORMATION

1. Access roles and rights are primarily based on the course program and curriculum needs.
2. The Privacy Office responsibility includes working with UF student sponsors and UF Health IAM staff for:
    a. Following up with sponsoring colleges, departments, and programs as necessary to validate the status of students included on the applications.
    b. Providing needed information about student status after access has been approved related to suspension and/or termination of access.
    c. Auditing student access to PHI.
3. Authorized UF students may be provided with supervised access to PHI, including personal user account logins and passwords for the current UF Health electronic medical record (EMR) systems, based on the student's program and curriculum needs.
4. Any data, including de-identified data, accessed by students may only be transported specific to class assignments, with advance written approval/direction of the student's sponsor, and following Privacy Office policies for removal of patient data.
5. **Students Who Are Also Employees:** Work-related EMR access for UF students should be requested by the employing department and directed through UF Health IAM.
6. **Non-Compliance:** Immediate disciplinary action will be initiated by UF against students who misuse the UF Health Information System or the data maintained in the system. Violations may result in permanent loss of access privileges. Sanctions for misuse or misconduct will be recommended by the Privacy Office in collaboration with the student's college.

UF STUDENT ACCESS TO EPIC

Students in certain UF Health Science Center programs

1. The UF Privacy Office has vetted and approved access to the UF Health Information Systems (Epic) for the following UF and UF-sponsored students
    a. Enrolled in a UF Health Science Center (HSC) College or a health-related UF program, or
    b. Pursuing an internship or clerkship rotation under an educational or clinical affiliation agreement with UF.

2. In an ongoing effort to streamline provisioning Epic access to students in UF HSC graduate programs, program administrators may send access requests for specific programs directly to UFH Shands Identity & Access Management. For further information and a list of designated graduate programs, see 'Access to Epic' on the UF Privacy website.

Students in non-UF Health Science Center programs

1. Instructions about how UF faculty and staff (Sponsors) may request Epic access for all other educational programs may visit the UF Health Privacy website, 'Access Request Process – All other educational programs.'
2. Sponsors are encouraged to contact either UFH Shands IAM staff at (352) 265-0526 or the Privacy Office at (352) 294-8720 to discuss the request.

SPONSOR RESPONSIBILITIES (FOR ALL STUDENTS)

1. Students must be sponsored and supervised by a proctor or faculty member employed by one of UF's Health Science Centers or the student's UF health-related program.
    a. Sponsors must provide the required information for each student at least three weeks, but not more than 60 days, prior to the access start date.
    b. The sponsor will periodically review students' access rights to ensure they are only provided with the access needed to accomplish required academic tasks.
    c. The sponsor will immediately notify UF Health IAM when a student's enrollment status changes or is terminated.
2. Sponsors shall work with the Privacy Office and/or IAM staff to address any possible non-compliance issues.

UF HEALTH SHANDS REQUIREMENTS

1. Student access is generally limited to 12 continuous months at a time, with start and end-dates defined at the time of application.
2. Students must follow UF Health Information Systems requirements in addition to UF Privacy requirements regarding Epic Access.

RESEARCH

1. Students who are members of research teams, whether employed or working as volunteers, may use their currently approved EMR access for the research project as long as they are properly added to the IRB-approved protocol as an official member of the team, and the student continues in good, active, academic standing.
2. Unauthorized student activities beyond the scope of the IRB-approved protocol can result in severe consequences for the Principal Investigator and the student.
    a. Unauthorized access to patient information may result reporting to the Office for Civil Rights and appropriate disciplinary action.
    b. Students who are not actively associated with the programs listed above will not be provided personal user access accounts to the EMR for research purposes. Patient information, if permitted, may be accessed through the Shands HIM department.
    c. All access to patient information for research purposes is subject to UF IRB policies and guidelines.
    d. See 'Epic Access for Research Purposes' on the 'Access to Epic' webpage for additional information.

DEFINITIONS

1. ***Academic Relationship:*** Enrolled in a UF Health Science Center (HSC) College or a health-related program at UF, or pursuing an internship or clerkship rotation under an educational agreement with UF.
2. ***Student:*** Under FERPA, a Student is any individual (regardless of age) who is or has been attending an educational institution, and that institution maintains education records. At UF, "attendance shall commence upon formal enrollment for college-credit courses approved and scheduled by the University…" (UF4.007(2)) The term "attending" includes, but is not limited to attendance in person, by traditional correspondence / distance learning, or electronically.

PROCEDURES (See also 'Access to Epic' on UF Privacy website)

1. Sponsors
    a. Complete the Student Data Access Application form.
    b. Obtain signed UF Health Security & Confidentiality Agreement.
    c. Forms may be submitted as follows:
        - Directly to UF Health IAM for designated graduate programs (see 'Access to Epic' on the UF Privacy website for a list of programs).
        - For special academic programs, new program access requests, or other unique requests, provide the form to the Privacy Office.
2. Students
    a. Complete UF's HIPAA & Privacy General Awareness Training and the UF Confidentiality Statement.
    b. Sign the UF Health Security & Confidentiality Agreement.
    c. Complete applicable UF Health Epic online training.
    d. Other steps may also be required by the student's sponsor or UF IRBs.

PRIVACY REQUIREMENTS

1. Security standards: General Requirements. UF's health care components (i.e., HIPAA covered entities) and business associates must do the following:
    a. Ensure the confidentiality, integrity, and availability of all electronic PHI the covered entity or business associate creates, receives, maintains, or transmits.
    b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
    c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under the Privacy Rule.
    d. Ensure compliance with the above by its workforce.
2. 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 should not have access… from obtaining access to electronic PHI.
    a. 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.

b. Workforce clearance procedure. Implement procedures to determine that the access of a workforce member to electronic PHI is appropriate.

c. Termination procedures. Implement procedures for terminating access to electronic PHI when the employment of, or other arrangement with, a workforce member ends.

3. Minimum necessary uses of protected health information.

   a. 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.

   b. A covered entity must make reasonable efforts to limit the access of such persons or classes to PHI consistent with the established need.

REFERENCES

1. HIPAA: 45 CFR §164.306 Security standards: General rules, §164.308 Administrative safeguards, §164.514(d) Minimum Necessary Requirements, §164.530 Administrative Requirements, (b) Training, (c) Safeguards, and (e) Sanctions

EXHIBITS

1. See Privacy Forms *Student Data Access Request* available at, http://privacy.ufl.edu/uf-health-privacy/forms/.