CampusGuard News

10/1/2019

HIPAA vs. FERPA: High Level Guidance for Higher Ed

Colleges and universities maintain medical information related to employees, students, and community members in various ways and locations, at on-campus health centers, counseling centers, in student records, and in human resource/employment files. There is often a common misconception that all of this health information falls under and must be protected according to the Health Insurance Portability and Accountability Act Privacy and Security Rules (**note:** referred to as "HIPAA" throughout this article). While this personal information does indeed need to be protected, this guidance document takes a closer look at where HIPAA does and does not apply within higher education.

- **What is HIPAA?**
  HIPAA provides privacy and security for protected health information (PHI). The HIPAA Privacy Rule protects sensitive PHI by establishing a set of patient rights and standards that apply to healthcare providers collecting, transmitting, and/or storing patient information. The HIPAA Security Rule deals specifically with Electronic Protected Health Information (ePHI). It lays out three types of security safeguards required for compliance: administrative, physical, and technical. Failure to comply with HIPAA can result in severe consequences and fines.

- **When does HIPAA apply?**
  While HIPAA protects PHI, it does only apply to that information when it is in use by a "covered entity." As a general rule, covered entities include: (1) health plans (health plans also include employer-sponsored group health plans (e.g. self-funded, self-administered, etc.), government and church sponsored plans, and multi-employer health plans); (2) health care clearinghouses; and (3) healthcare providers who electronically transmit health information in connection to billing, payment, and/or insurance coverage (doctors, clinics, dentist, nursing homes, etc.)

- **What does this mean for Higher Education?**
  It is not uncommon for college and university administrators to assume their institution is a covered entity under HIPAA because they have a student health center on campus that provides medical treatment to students, maintains their patient records, and engages in electronic billing transactions.

  However, the HIPAA Privacy Rule contains an important exception; it does not apply to health records maintained by an educational institution if those health records meet the definition of "education records" or "treatment records" under the Family Educational Rights and Privacy Act (FERPA).

- **When does FERPA apply?**
  FERPA applies to most public and private postsecondary institutions (all schools receiving funding from the Department of Education) and protects student information, including:

- FERPA “education records”: Records that are: (1) directly related to a student and (2) maintained by an educational agency or institution, or by a party acting for the agency or institution.
- FERPA “Treatment records”: Records pertaining to a student who is eighteen years of age or older, or is attending an institution of postsecondary education, which are made or maintained by a university physician, psychiatrist, psychologist, or other recognized professional or paraprofessional in connection with the provision of treatment to an eligible student, and are not available to anyone other than persons providing such treatment, except that such records can be personally reviewed by a physician or other appropriate professional of the student’s choice.

Because student health records at a university health center generally fall within these FERPA definitions, they are therefore exempt from HIPAA.

- **When would HIPAA actually apply to a Health Center?**
  If a student health center provides medical treatment to *non-students, such as staff members, spouses of students, or the community/public,* and bills for those services, these medical records relating to such treatment are *not* within the scope of FERPA, so the HIPAA would apply to the protection of these records.

  Colleges and universities are required to comply with FERPA with respect to the health records of their student patients and with HIPAA for the health records of their non-student patients.

- **What about University hospitals?**
  Will FERPA or HIPAA apply to records for students who are patients at a university hospital? Patient records maintained by a hospital affiliated with a university that is subject to FERPA are not typically “education records” or “treatment records” under FERPA because the university hospitals generally do not provide health care services to students on behalf of the educational institution. These hospitals are providing such services without any regard to the person’s status as a student. Therefore, these records are subject to HIPAA.

  However, in a situation where a hospital does run the student health clinic on behalf of the university, the student clinic records would again meet the exception and be subject to only FERPA.

- **What about Health Insurance provided to faculty and staff?**
  HIPAA applies to employee's health information related to the employer’s group health plans such as medical, dental, employee assistance program (EAP) and health flexible spending arrangement (FSA). This is true regardless of whether the group health plan is insured (i.e. by insurance company) or self-insured by the employer. However, the employer will not generally have HIPAA responsibilities for an insured group health plan "if" it does not receive employee health information other than for the limited purpose of enrollment activities. For a fully-insured group health plan, HIPAA will generally be handled by the insurance company.

HIPAA will also not apply if the health plan has both of the following characteristics: (a) it has fewer than 50 participants and (b) it is self-administered.

Employee health information that is obtained from a source other than the employer's group health plans, such as medical information related to employment (e.g. pre-employment physicals, drug testing results, medical leave or workers' compensation) will also not fall under the HIPAA requirements.

- **Can a college or university ask an employee or student for medical information?**
  HIPAA does not regulate the ability of institutions to request medical information from their employees and students for legitimate business reasons. For example, employees may need to provide a doctor's note to a supervisor to validate a sick day, or share information with co-workers regarding a leave of absence to undergo medical treatments. Students may also need to provide medical documentation to validate absences from class or to provide the basis for a request for ADA accommodations. This type information is not subject to HIPAA.
- **What about medical information for student athletes?**
  It is not uncommon for athletic trainers or physical therapists to operate as if they have an individual obligation to comply with HIPAA whenever he or she receives or views medical information relating to a student athlete. Remember that HIPAA does not apply to medical records that fall within the scope of FERPA, therefore, HIPAA does not apply to records generated when providing treatment to student athletes. University athletic departments may also provide secondary insurance coverage to student athletes, but the PHI data should be kept and protected by the third-party insurance provider.

FERPA and HIPAA are both designed to protect sensitive personal information and prevent anyone without authorization from accessing the information. While it is always important for colleges and universities to comply with the various requirements in HIPAA for protecting sensitive information, for most institutions, HIPAA will either not apply at all or will only be applicable for a small subset of areas or services on campus.

We strongly recommend that you consult with your legal department if there are ever any questions around what information may be subject to HIPAA. Once you understand what information falls under HIPAA or FERPA, you can verify all required security controls are in place to protect this data from compromise. You may also reach out to your dedicated CampusGuard CRM/SA Team to discuss in more detail.

Additional guidance from our Security Advisor team below:

[Coudeyras]: *When it comes to protecting sensitive information, understanding which regulations and laws apply is key. Once it has been determined that your organization is a HIPAA covered entity, the next step is to take a deep look at the HIPAA Privacy and Security rules and determine whether your organization complies. Building technical, administrative, and physical controls into business as usual activities is the best long range strategy to decrease risk.*