



# THE LEGAL ISSUE

Summer 2007

Volume 1, Number 4

## Beyond Privacy: FERPA Exceptions And Communication Within The University Regarding Student Conduct

By Manuel R. Rupe, Senior Assistant University Counsel, UCDHSC

Recent events at higher education institutions throughout the country, including the tragic events at Virginia Tech, have raised many questions regarding how information is shared within higher education institutions regarding students, and how common misperceptions regarding legal limitations on the disclosure of information can create harmful institutional inertia. Appropriately, many higher education institutions place considerable emphasis on respecting student's privacy and protecting their personal information. The federal Family Educational Rights and Privacy Act ("FERPA") provides significant legal protections for students, and generally requires a student's consent to disclose information within a student's educational record. However, FERPA includes some important, and often times overlooked, exceptions that provide higher educational institutions with opportunities to share and disclose information within the institution that may assist the institution in protecting its students and employees.

Importantly, FERPA does not prohibit a higher education institution from disclosing information to persons within the institution related to disciplinary action taken against a student for conduct that posed a significant risk to the safety or well-being of that student, other students, or other members of the school community. However, such persons must have a legitimate educational interest in the behavior of the student. 34 C.F.R. § 99.36(b)(1) and (2). This exception to FERPA covers not only risks of harm to other students (e.g., student who live in the same residence hall) and faculty (e.g., faculty who have the student in their class), but also the risk that a student may harm themselves. The focus of the exception is on the student's conduct or behavior, however, which presents challenges when institutions are, for example, addressing a student's comments, i.e., suicidal ideation.

At many higher education institutions, students experience significant difficulties with alcohol or substance abuse or other self-destructive behaviors. This often includes students (whether or not of the legal drinking age) who engage in excessive or binge drinking. In addition to diversion or other substance abuse treatment programs, institutions often struggle with whether or not they may contact a student's parents, who may be able to provide additional support or assistance to students dealing with a substance abuse issue. Under FERPA, a higher education institution may disclose information from an educational record if the disclosure "is to a parent of a student . . . regarding the student's violation

*Continued on Page 2.*

The material contained in this newsletter has been prepared by the Office of University Counsel for informational purposes only. This newsletter does not provide legal advice. By providing this information, an attorney/client or other relationship is neither intended nor established. The Office's client is the University and not any particular employee. We urge you to consult with your advising counsel regarding your individual situation.

- ◆ UCB: (303) 492-7481
- ◆ UCCS: (719) 262-3820
- ◆ UCDHSC – 9<sup>th</sup> Ave. and Anschutz Campuses: (303) 315-6617
- ◆ UCDHSC – Downtown Denver Campus: (303) 556-6511

*Edited by Mary Stone, UCDHSC Office*

## **Beyond Privacy** *(Continued from page 1)*

of any Federal, State, or local law, or of any rule or policy of the institution, governing the use or possession of alcohol or a controlled substance if (A) the institution determines that the student has committed a disciplinary violation with respect to that use or possession; and (B) the student is under the age of 21 at the time of the disclosure to the parent.” 34 C.F.R. § 99.31(a)(15)(i). Thus, FERPA allows institutions to communicate with parents regarding a student’s disciplinary violation and their difficulties with alcohol or substance abuse. Additionally, FERPA permits such disclosure if the violation is of an institutional rule or policy, such as a policy related to the use, possession, or consumption of alcohol in residence halls, even if the student did not violate a state or federal law.

Moreover, in emergency situations, higher education institutions are generally able to disclose information to first responders, such as law enforcement, to assist persons in determining how to effectively respond to an incident. Specifically, under FERPA a higher education institution “may disclose personally identifiable information from an education record to appropriate parties in connection with an emergency if knowledge of the information is necessary to protect the health or safety of the student or other individuals.” 34 C.F.R. § 99.36(a). This exception is not limited to the health or safety of students, but includes all persons.

While FERPA provides important protections for student privacy and information, it also allows for disclosures that meaningfully impact the campus community. The exceptions to FERPA provide higher education institutions with the opportunity to disclose information within the institution, as well as with parents, so that such institutions may be more responsive to, and aware of, students who are experiencing problems or challenges and may need help. Importantly, higher education institution employees should consult with legal counsel if they believe they have information regarding students that may impact employee or student health or safety, but are concerned as to whether such disclosure may violate FERPA.

## **Student Privacy: Electronic Information & FERPA**

By Jessica Chavez Salazar, Legal Staff Associate/Researcher, UCB

Technology constantly creates new ways to manage student information. When I was in college and needed a transcript, I walked over to the Records Office, filled out a paper request form (using an actual pen), paid the fee, and waited for the transcript to arrive in the mail. Today, students are often able to request transcripts using the Internet. There’s even a school in Japan that uses an infrared device to read and recognize the unique vein pattern found in each student’s hand. This pattern is then recorded on the student’s ID card, which may be used to access transcripts and student records at campus kiosks simply by scanning the card and placing his or her hand over a reader.<sup>1</sup> While we are not at that extreme, and regardless of the method used, it is always important to be vigilant in maintaining the security of electronic information. Grades, schedules, and tuition records are all records maintained on computers. These documents, even in digital format, still fall under FERPA’s definition of “education records.”<sup>2</sup> This article briefly points out three specific privacy concerns related to FERPA and electronic student records.

FERPA addresses student education records maintained by a school or its agent. Student information maintained on a university computer system may meet the definition of “education records.”<sup>3</sup> Under FERPA, schools are prohibited from disclosing student education records, outside of directory information, without prior written consent from the student or unless an exception applies. An “education record” may include a student e-mail message if the message is “maintained” by the university. One court found that e-mail messages generated by a student, directed to a faculty advisor, were

***Continued on Page 3.***

<sup>1</sup> Vincent Kiernan, *Show Your Hand, Not Your ID*, THE CHRON. HIGHER EDUC., Dec. 2, 2005, at A28. Available at <http://chronicle.com/weekly/v52/i15/15a02801.htm>.

<sup>2</sup> “Education records” means, except as otherwise provided for in the statute, “those records, files, documents, and other materials which (i) contain information directly related to a student; and (ii) are maintained by an educational agency or institution or by a person acting for such agency or institution.” 20 U.S.C. §1232(g).

<sup>3</sup> The definition of “record” was amended in 1996 to add “computer media.” See 34 C.F.R. § 99.3.

## Student Privacy: Electronic Information

(Continued from page 2)

education records because they directly related to the student and were sent for the purpose of seeking the advice of a person acting on behalf of the college.<sup>4</sup> However, another court found that an e-mail message being drafted on a student's computer was not being maintained by the institution and, therefore, was not an education record.<sup>5</sup> Determining which e-mails are properly considered to be student education records heavily relies on the specific facts involved. As such, questions regarding this area should be directed to the Office of University Counsel.

While FERPA prohibits obvious actions, such as releasing a student's transcripts to a third-party without consent, it may also address security measures used by the university to prevent unauthorized access to electronic student education records. A university with inadequate security measures resulting in unauthorized access to student education records through "hacking" may arguably be engaging in a FERPA violation.<sup>6</sup> Unauthorized access to records is not unique to our university system. According to the Privacy Rights Clearinghouse, there have been over 70 data breaches at institutions of higher education since January 2005.<sup>7</sup> As computer systems become more complex, combined with the seemingly limitless motivation of hackers to break into these systems, even more privacy issues will be revealed. While there is no private right of action in enforcing FERPA,<sup>8</sup> a university found to have a "policy or practice" in violation of FERPA may be subject to sanctions enforced by the Department of Education Family Policy Compliance Office ("FPCO"). A "policy or practice" may possibly include the use of inadequate computer security measures, or using systems known to be easily "hacked" into by others.<sup>9</sup>

This same responsibility to protect electronic student records extends to unauthorized access by university officials. In an opinion letter to Tazewell County, Virginia School Board, the FPCO discussed the software used by many higher education institutions to manage student and employee information.<sup>10</sup> In that letter, FPCO Director Leroy S. Rooker, stated that the FPCO "would consider a record management system that allows unauthorized individuals to have access to education records to constitute a policy or practice of violating FERPA."<sup>11</sup> He pointed out that a teacher would not be allowed to leave a stack of report cards in a location that students could freely look through. In the same manner, a university should not have an electronic system in place that allows unauthorized access, even by university officials.<sup>12</sup> Additionally, universities that have computerized systems such as PeopleSoft or Banner may need to keep track of which school officials are accessing a student record, depending on the system's parameters. For example, if a university system allows broad access to student records, that system must be able to track exactly who accesses a particular student's education record in order to address and remedy any inappropriate access to that student's record. Otherwise, allowing university officials to operate on an "honor system" may result in a policy or practice of permitting access to student education records without the university previously determining if the official has a legitimate educational interest.<sup>13</sup>

With the current wide-spread usage of computers, universities must be willing to frequently revisit FERPA and its application to electronic student education records. Appropriately determining which electronic records receive FERPA protection, maintaining adequate campus technology security measures in order to prevent a breach of the campus computing system, and properly managing access to electronic student education records by school officials are all areas that raise possible FERPA concerns. I recognize and appreciate all of the conveniences associated with computers, but after reading an article about yet another major data breach,<sup>14</sup> there are definitely times when I miss the good-old days of my typewriter.

<sup>4</sup> See *President of Bates College v. Congregation Beth Abraham*, 2001 WL 1671588, (Me.Super., Feb. 13, 2001).

<sup>5</sup> See *Owasso Indep. Sch. Dist. v. Falvo*, 534 U.S. 426 (2002).

<sup>6</sup> Beth Cate, Shakespeare on Cyberliability, NACUA Annual Conference, June 27, 2005. Available at [http://counsel.cua.edu/FERPA/03G\\_Cate.pdf](http://counsel.cua.edu/FERPA/03G_Cate.pdf).

<sup>7</sup> <http://www.privacyrights.org/ar/ChronDataBreaches.htm> (current as of July 10, 2007). See also Tom Zeller Jr., "Some Colleges Falling Short in Data Security," *The New York Times*, April 4, 2005.

<sup>8</sup> *Gonzaga Univ. et al. v. Doe*, 536 U.S. 273 (2002).

<sup>9</sup> Cate, *supra* note 2.

<sup>10</sup> <http://www.ed.gov/policy/gen/guid/fpc/ferpa/library/tazewellva-mcgraw.html>.

<sup>11</sup> *Id.*

<sup>12</sup> Only school officials with a "legitimate educational interest" may have access to student educational records without written consent from the student, i.e. officials who need access to student records in order to perform their legitimate institutional functions. See 34 C.F.R. §99.31.

<sup>13</sup> Interview available at <http://counselonline.cua.edu/archives/interviews/rooker.cfm>.

<sup>14</sup> Data Breach Occurs at Northwestern, June 1, 2007. Available at <http://www.northwestern.edu/newscenter/stories/2007/06/data.html>.

# FERPA: Not the Only “Privacy” Statute to Which CU Needs to Pay Attention

By Prentice R. Ehret, Senior Legal Staff Associate/Researcher, UCB

Above in this issue, as well as in the last edition of *The Legal Issue* (available at <http://www.uchsc.edu/ouc/legalissue.php>), we have addressed the Family Educational Rights and Privacy Act (“FERPA”), the primary statutory scheme applicable to privacy issues in higher education. FERPA, however, is not the only federal law concerning such privacy issues. This article will address two other federal statutory schemes which may apply to the functions of various departments on the campuses of the University of Colorado, and will also briefly discuss the manner in which they both “interface” with FERPA. While this article will limit itself to those two statutes, it is not meant to imply that these are the only two other than FERPA to concern themselves with privacy issues.

The federal laws in question are the Gramm-Leach-Bliley Act (“GLBA”), also known as the Financial Services Modernization Act of 1999, and the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”). While the applicability of these statutes may differ on the various campuses and within the departments of those campuses, it behooves all campuses to assess the functions of their departments and components in light of the requirements of these two statutory and regulatory schemes.

The following is a summary of an informational booklet written by Christine R. Williams, former Associate General Counsel at the University of Akron, and published by the National Association of College and University Attorneys in March, 2007. The booklet is entitled *FERPA, GLBA & HIPAA: The Alphabet Soup of Privacy*.

## **The Gramm-Leach-Bliley Act (GLBA)**

The Gramm-Leach-Bliley Act (“GLBA”) applies to “financial institutions,” a term which is defined broadly within the statute as any institution engaging in the financial activities enumerated under the Bank Holding Company Act of 1956, including “making, acquiring, brokering, or servicing loans” as well as “collection agency services.” Because institutions of higher education participate in financial activities, such as making Federal Perkins Loans, they are considered under the regulations of the Federal Trade Commission (“FTC”) to be “financial institutions” for purposes of GLBA. While these functions would certainly place financial aid departments under the coverage of the act, GLBA may also apply to bursar’s offices if they perform services such as cashing checks. However, merely accepting credit cards for such purposes as the purchase of books or making tuition payments does *not* bring an institutional department under GLBA.

GLBA has both “privacy” provisions and “security” provisions; however the privacy provisions do not apply to institutions of higher education as long as they are in compliance with the privacy provisions of FERPA. This is because the FTC reasoned that higher education institutions should not be burdened with having to comply with two different regulatory schemes regarding the privacy of student records. As is noted further down in this article, the Department of Health and Human Services (“HHS”) applied similar reasoning in exempting student medical records from HIPAA coverage. Thus institutions of higher education need only comply with the security provisions of GLBA, which require a minimum level of security for “confidential consumer information,” which is defined as nonpublic personal information which the institution obtains from customers seeking a financial product or service, e.g., students or parents of students applying for financial aid. This includes any such information regardless of format (paper or electronic).

In order to be in compliance with the security provisions of GLBA, colleges and universities must develop an information security program designed to protect the security and confidentiality of customer information and to guard against unauthorized access to such information. This requires designating an individual who is responsible for coordinating the program, and conducting a risk assessment in order to identify reasonably foreseeable risks to the security of customer information. Institutions of higher education must also implement procedures for selecting and retaining service providers who will have access to protected nonpublic customer information, and must obtain a written commitment from these providers to implement and maintain appropriate safeguards to protect such information.

At present, the FTC has not issued regulations outlining the potential sanctions that will apply to higher education institutions which are not in compliance with the security requirements of GLBA. Nonetheless, it is incumbent on the financial aid and bursar’s offices of all of CU’s campuses to conduct a survey and assessment of the functions within their departments to ascertain what functions fall under the coverage of GLBA, and what is required in order to be in compliance with the act.

*Continued on Page 5.*

## More Privacy Statutes

(Continued from page 4)

### The Health Insurance Portability and Accountability Act (HIPAA)

The Health Insurance Portability and Accountability Act, commonly known as "HIPAA," was enacted by Congress to create rules to provide for the portability of health care insurance, and to simplify the administration of both health care and insurance. It also addresses the privacy and security of "protected health information" ("PHI"), which is defined as any *individually identifiable* health information. *Identifiable* refers not only to data that is explicitly linked to a particular individual, but also includes health information with data items which reasonably could be expected to allow individual identification.

As a statutory and regulatory scheme, HIPAA constitutes a "floor" rather than a "ceiling," i.e., it does not preempt state laws that may be more restrictive. Like GLBA, HIPAA has "privacy" regulations and "security" regulations. While the privacy regulations restrict access to PHI in any form, the security regulations apply only to PHI in electronic form.

In order to be subject to regulation under HIPAA, an institution must be either a "covered entity" or be a "hybrid entity" which has "covered components." In order to be a covered entity or a covered component of a hybrid entity, an institution or institutional department must not only provide health care, but must also transmit health information *in electronic form* at any stage related to the process of obtaining insurance reimbursement. Consequently, most institutions of higher education are either not covered entities, or are hybrid entities with covered components. The University of Colorado falls into the latter category.

The HIPAA privacy regulations primarily limit the manner in which PHI can be used and disclosed. Even permitted uses and disclosures are limited to the "minimum necessary," i.e., an employee of a health treatment facility or insurance provider should have access only to the information necessary for them to complete their designated tasks.

Just as in the case of GLBA, there is a "FERPA exception" to the application of HIPAA to the medical treatment records of students in postsecondary institutions. Since such records are addressed under FERPA, they are not subject to regulation under HIPAA. This leads to the rather counter-intuitive prospect that these records are not protected by *either* FERPA *or* HIPAA as long as they are not shared with anyone other than the treatment provider either inside or outside the institution. If they are shared with someone other than the treatment provider (which is almost always the case), they are subject to FERPA protection as "education records," but are not subject to protection under HIPAA.

However, while student health centers on the various campuses are not subject to HIPAA regulation as to student health records, regardless of whether or not they transmit health records electronically, they would be subject to the HIPAA privacy requirements as to the records of *non-students*, such as faculty, staff, or family members of students, if electronic transmission is involved at any stage. This is an evaluation that has to be performed on a campus-by-campus basis.

Records relating to research involving human subjects where health care or health information is implicated will be subject to HIPAA protection and regulation. On the other hand, any health records obtained or retained by the University as a result an employment relationship (e.g., pre-employment physicals, workers compensation records, etc.) are excluded from coverage under HIPAA.

Sanctions for failure to comply with any applicable privacy or security regulations under HIPAA can range from civil penalties of \$100 for each violation to a maximum of \$25,000 per year for the same violations. Much more drastic criminal penalties can be enforced where there was a knowing and deliberate violation of HIPAA regulations, and can result in as much as ten years' imprisonment where such knowing violation was for personal gain or malicious harm.

### More Information

Each campus has its own procedures regarding FERPA compliance and the release of student information. The **Boulder Campus's** Notice of Student Rights and Procedures on the Designation and Release of Directory Information is available at [http://registrar.colorado.edu/regulations/ferpa\\_confidentiality\\_records.html](http://registrar.colorado.edu/regulations/ferpa_confidentiality_records.html). The **Denver and Health Sciences Center Campuses'** Notification of Student Rights is available at <http://www.cudenver.edu/Student+Life/NSO/FERPA.htm>. The **Colorado Springs Campus's** FERPA Notice of Student Rights is available at <http://www.uccs.edu/studentsuccess/newsite/pates/currentstudents/ferpa.html>.

**All questions regarding access to student records and FERPA should be directed to your campus registrar's office.**

- Boulder Carol Mash (303) 492-6907
- Downtown Denver Campus: Thomas Hartman (303) 556-2737
- Health Sciences Center: Diana Warren (303) 315-7676
- Colorado Springs: Steve Ellis (719) 262-3375

