Barley Snyder

Higher Education Law Update March 2012

PUBLISHED ON
March 1, 2012

TABLE OF CONTENTS

A More Conservative Supreme Court To Revisit Affirmative Action In University Of Texas Case

By: Jennifer Craighead Carey

In *Gutter v. Bollinger,* 539 U.S. 306 (2003), the U.S. Supreme Court, in a 5-4 decision, upheld the University of Michigan Law School's policy of using race and ethnicity as a factor in the admissions process. In so ruling, the Supreme Court noted that race and ethnicity can be one of my factors considered by colleges when selecting students. The Court found "a compelling interest in obtaining the educational benefits that flow from a diverse student body" and credited the admissions process at the law school with using a "highly individualized, holistic review of each applicant's file". Race, according to the Court, was not used in a "mechanical way". However, the Court ruled 6-3 that the University of Michigan's undergraduate admissions program, which relied on a point system that awarded twenty additional points to African-American, Hispanic and American-Indian applicants, did not provide the "individualized consideration" necessary to survive scrutiny and therefore, had to be modified. The *Grutter* decision in essence provided a roadmap of the Constitutional parameters required for public colleges and universities to use race and ethnicity factors in their admissions process.

Now, the U.S. Supreme Court is once again poised to decide the issue of affirmative action in public university admissions, this time involving the University of Texas at Austin (the "University"). Specifically, in *Fisher v. University of Texas at Austin,* Case No. 11-345, the Supreme Court will decide whether its prior decisions interpreting the Equal Protection Clause of the Fourteenth Amendment, including *Grutter*, permit the University's use of race in undergraduate decisions.

Prior to *Grutter* the Texas legislature had approved a race neutral policy for admissions to the state's university system. Under this policy, the University automatically accepted for admission all Texas high school seniors who had ranked in the top 10% of their class. This race neutral system accounted for 83% of the admissions to the University. After *Grutter* the University continued to use this policy for admissions, but also developed a plan to increase racial diversity by providing for admission of underrepresented

African-American and Hispanic students using a comparison to the minority population in Texas. Under this plan, race was included as a specific factor in admissions calculations for those who did not qualify under the top 10% policy. This coding was also used as a factor for determining selection into academic majors and to enhance diversity in individual classes.

Ms. Fisher, who is Caucasian, applied to the University in 2008. She did not qualify under the top 10% program. She was denied admission and filed suit, claiming minorities with lower academic qualifications were accepted into the school. Both the federal district court and the Fifth Circuit Court of Appeals upheld the University's use of race as a factor in the coding system. In her Petition to the Supreme Court, Ms. Fisher argues that the Fifth Circuit misread *Grutter* and was too lenient and deferential in crediting the University's program. Significantly, in the alternative, she argues that the Court should reconsider its decision in *Grutter* "to restore the integrity of the Fourteenth Amendment's guarantee of equal protection".

The case is scheduled for oral argument in the Fall of 2012. In the *Grutter* decision, Sandra Day O'Connor cast the deciding vote in favor of the University of Michigan Law School's admissions program. She has since retired and has been replaced by Samuel Alito. It is believed that a more conservative court may in fact revisit its decision in *Grutter* as requested by the Plaintiff, Ms. Fisher, putting into jeopardy the University's program as well as similar programs across the county. We will continue to keep you apprised of developments in the case.

Back To Top

Data Security and Privacy Considerations for Colleges and Universities

By: Donald R. Geiter, CIPP/US

Every college and university in the United States routinely handles electronic data containing protected personal information. This data can include information about its students, employees or patients. In the last five years alone, hundreds of substantial data breaches, including breaches involving many colleges and universities, have resulted in the compromise of hundreds of millions of data records containing protected personal information. The cost to a college or university for a single data breach can be staggering.

A system of data privacy policies and procedures will likely reduce the occurrences of data breaches and may serve to mitigate some of the costs of a data breach. However, before a college or university can develop its policies and procedures, it must first be aware of and understand the myriad of laws relating to the protection and sharing of data containing personally identifiable information. For instance, there are Federal laws that relate to student rights, patient rights, as well personal financial information. Since most colleges and universities process credit card payments, they also need to comply with payment card industry data security standards. To complicate things further, colleges and universities must also consider that most states have their own data security and privacy laws.

This articles will give colleges and universities a very brief overview of the applicable laws and standards. A future article will provide an overview of guidelines that colleges and universities can follow to achieve compliance with these laws and standards.

The Federal law most commonly applicable to colleges and universities is the Federal Education Records Privacy Act (FERPA). FERPA governs the privacy of students' education records in the United States. More specifically, FERPA

regulates access to, amendment of, and disclosure by colleges and universities of education records and requires that the college or university obtain the written permission from the student before releasing information from a student's school record. All colleges and universities receiving funds from any U.S. Department of Education program must comply with FERPA. Lesser known than FERPA, but equally important, is the Health Insurance Portability and Accountability Act (HIPAA). HIPAA is the Federal law that provides for privacy and standardized transmission of health records and information. HIPAA applies to most college and university health centers and any institution with a medical school. HIPAA protects "individually identifiable health information", which includes demographic information collected from a student or patient or created by the college or university in their treatment. Graham-Leach-Bliley Act (GLBA) is the Federal law that governs the operations of most financial institutions. GLBA will also apply to a college or university to the extent it is engaging in lending funds (whether to students or faculty), collecting loan payments, or facilitating the process of applying for financial aid. In such case, the college or university will be considered a "financial institution" under GLBA. There are two categories of compliance requirements under GLBA: Safeguarding Rules and Privacy Rules. Fortunately, colleges and universities that are in compliance with FERPA are deemed compliant with the Privacy Rules. However, colleges and universities must still separately comply with the Safeguarding Rules, which requires them to develop and follow a comprehensive security program to safeguard protected personal information. Similarly, colleges and universities that extend credit to students may also be subject to the "Red Flag Rules" promulgated under the Fair and Accurate Credit Transaction Act. These rules require such colleges and universities to establish procedures for recognizing identity theft.

While not a Federal law, the Payment Card Industry (PCI) Data Security Standard (DSS) was created by the credit card industry nearly 10 years ago as a way to guard against attacks that involve theft and misuse of cardholder information. Under PCI DSS, colleges and universities that process credit card payments must comply with over a dozen requirements, including, maintaining and frequently testing data security systems. Depending on the number of transactions processed per year, colleges and universities may be required to perform on-site assessments of its compliance with PCI DSS.

States, including Pennsylvania, have enacted their own security and privacy laws. Most of these state laws relate to data breach notification. For instance, Pennsylvania has a data breach notification law that applies to all types of companies, including colleges and universities. The law serves to protect personal information that includes a resident's first name or first initial and last name in combination with some other data element that is not encrypted or redacted. The law requires that upon discovery of a breach, or following the reasonable belief that a breach may have occurred, the college or university must provide notice without "unreasonable delay" to the resident whose information may have been compromised. A violation of the law constitutes a violation of the Pennsylvania Unfair Trade Practices and Consumer Protection Act, which could result in treble damages and costs to the violating college or university.

Most states and the District of Columbia have enacted their own laws relating to data breach notification. While there are several common notification obligations across the various sets of state law, many states have enacted unique provisions that require a specific response if a resident of that state was affected by the breach. Consequently, if a college or university handles personal identifiable information of students, employees or patients from various states, upon a data breach, the college or university must follow the breach notification laws of each of the relevant states. In addition to requiring notice to affected persons, some states also require notice of the breach be made to certain state agencies and law enforcement authorities.

Colleges and universities are subject to significant regulation and standards with respect to how they collect, store and use protected personal information of its students, employees and patients. They also collect the information in a myriad of ways and from a large range of geographic locations, all adding to the complexities in ensuring compliance with all of the applicable data security and privacy laws and standards.

Colleges and universities are unique in that they collect protected personal information in a myriad of ways, from varying types of individuals and from a large range of geographic locations. Because of these complexities, colleges and universities should, with the assistance of their attorney, become very familiar with all of the laws and standards highlighted in this article and they should frequently audit their own systems to ensure compliance.

Back To Top

Balancing Student Privacy, Campus Security and Public Safety

By: Maria Di Stravolo Elliott

The U.S. Department of Education's Family Policy Compliance Office (FCPO) has released a new guidance on the Family Educational Rights and Privacy Act (FERPA) and the Higher Education Act of 1965 (HEA). The guidance is intended to assist school officials - who may be reassessing their campus safety policies in the wake of several high profile campus emergencies - find the proper balance between student privacy rights and campus security needs.

FERPA is a Federal law that protects the privacy interests of both parents and students in a student's "education records." FERPA generally requires parents or eligible students to provide these institutions with written consent before the school discloses personally identifiable information from a student's education records. However, in emergency situations, FERPA allows schools to make necessary disclosures without obtaining prior written consent. Part I of the guidance is designed to help school officials recognize these emergency situations where consent is not required for disclosure.

Under FERPA, personally identifiable information may be disclosed without the consent of a student or parent in the following circumstances:

1. Health or Safety Emergency

a. The central exception to FERPA's disclosure policy is a disclosure to protect the health or safety of the student or other individuals in the event of an actual, impending, or imminent emergency. School officials must believe an "articulable and significant" threat exists to make disclosures under this section.

2. Personal Knowledge or Observation

a. FERPA does not prohibit school officials from disclosing information about a student that is obtained through personal observation. However, this general rule does not apply where (1) a school official personally learns of information about a student through an official role in making a determination about the student and (2) the determination is maintained in an education record. For instance, this exception does not apply if the official was involved in formal disciplinary proceedings brought against the student.

3. Law Enforcement Unit Records

a. Records of the law enforcement unit of an educational institution are not subject to FERPA if the records are:

1. created by a law enforcement unit
2. created for a law enforcement purpose; and
3. maintained by the law enforcement unit.

4. Disciplinary Records for Violent and Non-Forcible Sex Offenses

a. FERPA permits a postsecondary institution to disclose to an alleged victim of any crime of violence or non-forcible sex offense the final results of a disciplinary proceeding conducted by the institution against the alleged perpetrator of that crime regardless of whether the institution concluded that a violation was committed ? without the alleged perpetrator's consent.

5. Judicial Order or Lawfully Issued Subpoena

a. Disclosures made pursuant to a judicial order or lawfully issued subpoena do not require parental or student consent. However, the guidance notes that the institution should generally attempt to notify the affected party prior to making the disclosure so that the parent or student can consult a legal representative and take protective action.

6. Disclosures to Parents

a. At postsecondary institutions, FERPA permits parents to have access to their children's education records, if one of the following requirements is met:

1. the student is a dependent for income tax purposes;
2. there is a health or safety emergency involving a parent's son or daughter;
3. the student, who is under age 21, has violated any law or institutional policy concerning the use or possession of alcohol or a controlled substance and the institution has determined that the student has committed a disciplinary violation with respect to that use or possession; or
4. the information is based on a school official's personal knowledge or observation of the student.

7. Treatment Records

a. Under FERPA, medical and psychological treatment records of eligible students may be disclosed to those medical professionals providing the treatment if they are made, maintained, and used only in connection with that treatment. If officials wish to disclose these treatment records for other reasons, they must use a different FERPA exception or seek the necessary party's consent.

8. Threat Assessment Teams

a. Some institutions have created "threat assessment teams" to assist in determining whether a disclosure may be made under FERPA. With a properly-implemented threat assessment program (that includes representatives from local law enforcement), schools can respond to student behavior that raises concerns about a student's mental health (and the safety of the student and others) that is chronic or escalating. By using a threat assessment team, the institutions may make other disclosures under the health or safety emergency exception, as appropriate, when an "articulable and significant threat" exists.

The HEA is a Federal law that, in Section 485(f) (also known as the Clery Act), requires all postsecondary institutions participating in the student financial aid programs under Title IV of the HEA to (1) disclose their campus security policies and (2) provide timely warnings to students, parents, and employees of crimes that represent a threat to the campus community. It further requires postsecondary institutions to collect and

disseminate crime data to the campus community. Part II of the guidance is designed to give school officials a better understanding of what information must be disclosed under the law.

What information must be disclosed, and when?

1. Timely Warnings and Emergency Notification

a. The Clery Act requires postsecondary institutions to provide timely warnings to alert the campus community of certain crimes. Under the HEA, postsecondary institutions must develop and disclose a statement of policy describing how the institution will handle emergency situations occurring on the campus that present an immediate threat to the health or safety of students or employees. The guidance notes that these provisions do not conflict with FERPA, which allows the release of personally identifiable information without consent in the case of an emergency (which is a threat to health and safety).

2. Sex Offenses under the HEA

a. Under the Clery Act, institutions must include a statement of policy regarding the institution's campus sexual assault programs that prevent sex offenses, as well as procedures to follow if a sex offense occurs, in the institution's Annual Security Reports. The guidance explains that both the accuser and the accused must be informed of the outcome (meaning the "final determination" and any sanction imposed) of the institutional disciplinary proceeding alleging a sex offense.

3. Missing Students

a. The HEA also requires postsecondary institutions that maintain on-campus student housing facilities to establish, for affected students, a missing student notification policy that includes notifying students that they can confidentially register an individual to be contacted if the student is determined to be missing. All students residing in an on-campus student housing facility must be advised that, regardless of whether they register a contact person, the local law enforcement agency will be notified in the event that the student is determined to be missing.

4. Fire Safety

a. The HEA requires postsecondary institutions that maintain on-campus student housing facilities to publish an annual fire safety report that discloses campus fire statistics, fire safety practices, and fire safety standards.

Back To Top

Higher Ed Institutions Operate in a Complex Deferred Compensation Landscape

By: Mark A. Smith

If a higher education institution that is exempt from federal income taxation wishes to provide deferred compensation to an executive or an executive-only group (generally referred to in the tax law as "nonqualified deferred compensation"), there are two separate Internal Revenue Code provisions that must be satisfied: (i) Code Section 409A, which generally governs the tax treatment of nonqualified deferred compensation no matter whether the employer is taxable or tax exempt, and (ii) Code Section 457, which imposes additional constraints on deferred compensation paid by tax exempt and governmental employers. The concept of nonqualified deferred compensation encompasses not only plans or agreements that deliver supplemental retirement benefits to an

institution's executives, but to essentially any arrangement under which the institution obligates itself currently to pay compensation in a future year. For example, these two Code Sections also have potential application to long term incentive pay plans and to severance pay commitments of higher education institutions.

The Code Section 409A restrictions on nonqualified deferred compensation fall into three general categories: (i) deferral election restrictions, which essentially require that any choices the employee is given with respect to the time and form of a future payment of deferred compensation must be exercised at the time of entering into the deferral arrangement, (ii) distribution event restrictions, which essentially require that from the outset the future distribution of the deferred compensation has to be linked to the occurrence of one of several permitted distribution events (upon separation from service, at a specified time, upon death, upon disability, upon a change in control of the employer, or upon an unforeseeable emergency), and (iii) distribution acceleration restrictions, which generally provide that distributions cannot be accelerated to an earlier date than that laid down at the time the deferred compensation arrangement is initially put in place. Deferred compensation arrangements of taxable employers that have to comply with Code Section 409A, but that are not also subject to Code Section 457, can be, and frequently are, designed to have a compensation payment date that differs from the date the compensation is no longer subject to a substantial risk of forfeiture, i.e., the "vesting" date. For example, these plans of taxable employers are typically written to say that the employee is "vested" once the employee has completed X years of service, but the deferred compensation will then get paid when the employee quits working for the employer. This sort of design, separating the distribution event from the vesting event, is possible because in the case of taxable employers the taxability to the employee and the tax deductibility by the employer are based on the distribution timing, not on the vesting timing. As a result, an employee of a taxable employer covered by a nonqualified deferred compensation plan can earn or be awarded a vested right to a payment that will occur further out in the future, and the vesting event itself does not trigger any current income tax consequences for the employee.

The additional applicability of Code Section 457 to tax-exempt employers presents them, proverbially, with both a blessing and a curse. The blessing is that Code Section 457(b) authorizes the adoption by tax-exempt employers of what is called an "eligible 457(b) plan." In brief, an eligible 457(b) plan is a retirement accumulation program that the tax-exempt employer can establish solely for the benefit of its "top hat" executive group of employees, that can be established and operated in addition to (not in place of) any Code Section 401(a) or Section 403(b) plan that may cover these same employees, and that, in effect, enables the executive group to "double up" the amount of their annual tax deferred retirement savings if they fully take advantage of the eligible 457(b) plan and also the institution's 401(a) or 403(b) plan. If the tax-exempt employer is also a governmental entity (e.g., a state owned college), the limitation on the class of eligible employees for an eligible 457(b) plan to just a top hat executive group does not apply, so in those cases all employees could be eligible for the plan. Amounts paid to an executive under an eligible 457(b) plan are taxable to the executive when paid, just like amounts paid from a 401(a) and 403(b) retirement plan.

The accompanying curse of Code Section 457, however, is that any deferred compensation commitment that a tax-exempt employer makes that does not qualify as an eligible 457(b) plan becomes subject to the tax treatment rules of Code Section 457(f). Under Code Section 457(f), nonqualified deferred compensation commitments made by tax exempt employers are taxable to the employee when the amount to be paid is no longer subject to a substantial risk of forfeiture, i.e., when it "vests," even if the promised amount is not then payable to the employee. As a result of this Section 457(f) taxability timing rule, it is most commonly the case when a tax exempt employer makes a nonqualified deferred compensation commitment to an executive that the distribution event and the vesting event

occur at the same time. Since the deferred amount is includable in the employee's federal taxable income when it vests, to not have it also then be distributable would create the hardship of the employee having to pay the income taxes on money that he cannot then draw on to cover the taxes.

As a further consequence of this 457(f) taxability timing rule, tax exempt employers have historically designed their nonqualified deferred compensation arrangements in creative and, some might say, aggressive ways in an effort to delay as long as possible the date when the deferred compensation becomes vested. One common such approach has been to make vesting subject to the employee's satisfaction of a multi-year non-competition agreement. Another has been the use of what is called a "rolling risk of forfeiture," where the vesting date is initially established as a given time, but then as that time draws near, and the executive is not ready to retire, the vesting date is automatically extended out for another fixed period. It is clear under Treasury regulations the IRS promulgated in 2007 under Code Section 409A that, for Section 409A purposes, these two sorts of purported vesting deferral mechanisms are ineffective and will be disregarded by the IRS. Further, the IRS in 2007 issued Notice 2007-62, in which it states that it intends to issue formal guidance to apply specifically to Code Section 457(f) deferred compensation arrangements defining what will constitute a substantial risk of forfeiture for 457(f) purposes. In that notice the IRS specifically cautions that the 457(f) guidance will follow the 409A regulations. As a result, tax-exempt employers are essentially on notice that many of the existing mechanisms that have been used to defer the vesting date under 457(f) arrangements will be disallowed prospectively, as soon as the promised 457(f) guidance is published.

Now is a prudent time for tax exempt higher education institutions to inventory the nonqualified deferred compensation plans, arrangements, agreements and other commitments of all sorts they may have in existence, and to assess whether any of them are in need of re-thinking or re-design, given the IRS's announced intention to extend the substantial risk of forfeiture rules in the Code Section 409A regulations and apply them to Code Section 457(f) arrangements.

Back To Top