Dr. David L. Soltz
President
Bloomsburg University of Pennsylvania
400 East Second Street
Bloomsburg, Pennsylvania 17815

JAN 12 2010

Dear Dr. Soltz:

This Office is responsible for administration of the Family Educational Rights and Privacy Act (FERPA), which protects the privacy interests of parents and eligible students in students' education records. See 20 U.S.C. §1232g and 34 CFR part 99. Under that authority we investigate, process, and review complaints and violations and provide technical assistance to ensure compliance with all FERPA requirements. We are responding to a letter dated November 11, 2009, from David E. Stover, Bloomsburg University Legal Counsel, in which he explained that a laptop computer owned by the University's psychology department was stolen and that the laptop's hard drive contained student rosters, class lists, student grades and social security numbers.

Under FERPA, a parent or eligible student must provide a signed and dated written consent before a postsecondary institution discloses personally identifiable information from the student's education records. 34 CFR §§99.5(a); 99.30. Exceptions to the consent requirement are set forth in § 99.31(a) of the regulations. "Disclosure" means "to permit access to or the release, transfer, or other communication of personally identifiable information contained in education records to any party, by any means, including oral, written, or electronic means." 34 CFR § 99.3.

The preamble to the December 8, 2009, FERPA regulations explains the necessity for educational agencies and institutions to ensure that adequate controls are in place so that the education records of all students are handled in accordance with FERPA's privacy protections. *See* 73 *Fed. Reg.* 74806, 74843 (Dec. 9, 2008). The "Department Recommendations for Safeguarding Education Records" (Safeguarding Recommendations) that were published in both the Notice of Proposed Rulemaking (NPRM) and the Final Regulations are intended to provide agencies and institutions additional information and resources to assist them in meeting this responsibility. (The NPRM was published at 73 *Fed. Reg.* 15574, March 24, 2008.)

The FERPA Safeguarding Recommendations recognize that no system for maintaining and transmitting education records, whether in paper or electronic form, can be guaranteed safe from every hacker and thief, technological failure, violation of administrative rules, and other causes of unauthorized access and disclosure. Although FERPA does not dictate requirements for

safeguarding education records, the Department encourages the holders of personally identifiable information to consider actions that mitigate the risk and are reasonably calculated to protect such information. Of course, an educational agency or institution may use any reasonable method, combination of methods, or technologies, taking into consideration the size, complexity, and resources available to the institution; the context of the information; the type of information to be protected (such as SSNs or directory information); and methods used by other institutions in similar circumstances. The greater the harm that would result from unauthorized access or disclosure and the greater the likelihood that unauthorized access or disclosure will be attempted, the more protections an agency or institution should consider using to ensure that its methods are reasonable.

As explained in the FERPA Safeguarding Recommendations, one resource for administrators of electronic data systems is "The National Institute of Standards and Technology (NIST) 800-100, Information Security Handbook: A Guide for Managers" (October 2006). See http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf. Another resource is NIST 800-53, Information Security, which catalogs information security controls. See http://csrc.nist.gov/publications/nistpubs/800-53-Rev1/800-53-rev1-final-clean-sz.pdf. Similarly, a May 22, 2007, memorandum to heads of Federal agencies from the Office of Management and Budget requires executive departments and agencies to ensure that proper safeguards are in place to protect personally identifiable information that they maintain, eliminate the unnecessary use of SSNs, and develop and implement a "breach notification policy." Although directed towards Federal agencies, this memorandum may also serve as a resource for educational agencies and institutions. See http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf.

The Department's FERPA Safeguarding Recommendations specify that an educational agency or institution that has experienced a theft of files or computer equipment, hacking or other intrusion, software or hardware malfunction, inadvertent release of data to Internet sites, or other unauthorized release or disclosure of education records, should consider one or more of the following steps:

- Report the incident to law enforcement authorities.
- Determine exactly what information was compromised, i.e., names, addresses, SSNs, ID numbers, credit card numbers, grades, and the like.
- Take steps immediately to retrieve data and prevent any further disclosures.
- Identify all affected records and students.
- Determine how the incident occurred, including which school officials had control of and responsibility for the information that was compromised.
- Determine whether institutional policies and procedures were breached, including organizational requirements governing access (user names, passwords, PINS, etc.); storage; transmission; and destruction of information from education records.
- Determine whether the incident occurred because of a lack of monitoring and oversight.
- Conduct a risk assessment and identify appropriate physical, technological, and administrative measures to prevent similar incidents in the future.
- Notify students that the Department's Office of Inspector General maintains a website describing steps students may take if they suspect they are a victim of identity theft at

http://www.ed.gov/about/offices/list/oig/misused/idtheft.html; and
http://www.ed.gov/about/offices/list/oig/misused/victim.html.

The Safeguarding Recommendations note also that FERPA does not require an educational agency or institution to notify students that information from their education records was stolen or otherwise subject to an unauthorized release, although it does require the agency or institution to maintain a record of each disclosure. 34 CFR §99.32(a)(1). However, student notification may be required in these circumstances for postsecondary institutions under the Federal Trade Commission's Standards for Insuring the Security, Confidentiality, Integrity and Protection of Customer Records and Information ("Safeguards Rule") in 16 CFR part 314. In any case, direct student notification may be advisable if the compromised data includes student SSNs and other identifying information that could lead to identity theft.

Under FERPA, no funds shall be made available to an educational agency or institution that has a policy or practice of permitting the release of personally identifiable information in education except as authorized by statute. 20 U.S.C. §1232g(b). Failure to take reasonable and appropriate steps to protect education records could result in the release or disclosure of personally identifiable information from education records and may also constitute a policy or practice of permitting the release or disclosure of education records in violation of FERPA requirements. Should this Office investigate a complaint or other indications of noncompliance, we would take into consideration what steps an educational agency or institution has taken in response to a data breach or other unauthorized access to, release, or other disclosure of education records.

If you have any questions, please contact this Office at (202) 260-3887.

Sincerely,

Paul Gammill
Director
Family Policy Compliance Office

cc: David E. Stover