



UNITED STATES DEPARTMENT OF EDUCATION

WASHINGTON, DC 20202

AUG 28 2015

GEN 15-18

Subject: Protecting Student Information

Summary: This letter reminds institutions of higher education and their third-party servicers of their continuing obligations to protect data used in all aspects of the administration of the Title IV Federal student financial aid programs.

Dear Colleague:

Instances of data breaches at organizations entrusted with personally identifiable information (PII) continue to proliferate and reinforce the need for focused action by the U.S. Government to combat cybersecurity threats and to strengthen the Government's cybersecurity infrastructure. Ensuring the confidentiality, security and integrity of Title IV financial aid information depends on cooperation among FSA, institutions of higher education ("institutions") and other entities including state grant agencies, lenders, contractors and third-party servicers.

Our expectation is that all FSA partners will quickly assess and implement strong security policies and controls and undertake ongoing monitoring and management for the systems, databases and processes that support all aspects of the administration of Federal student financial aid programs authorized under Title IV of the Higher Education Act of 1965, as amended (the HEA). Such systems, databases and processes include all systems that collect, process, and distribute information – including PII – in support of applications for and receipt of Title IV student assistance.

The Student Aid Internet Gateway (SAIG) Enrollment Agreement entered into by each Title IV participating institution includes a provision that the institution "[m]ust ensure that all Federal Student Aid applicant information is protected from access by or disclosure to unauthorized personnel." Institutions are reminded that under various Federal and state laws and other authorities, including the HEA; the Family Educational Rights and Privacy Act (FERPA); the Privacy Act of 1974, as amended; the Gramm-Leach-Bliley Act; state data breach and privacy laws; and potentially other laws, they may be responsible for losses, fines and penalties (including criminal penalties) caused by data breaches.

To support the expectation and the SAIG requirements described above, FSA strongly encourages institutions to follow industry standards and best practices¹ in managing information and information systems and in securing PII. Those standards and practices include:

¹Best practices include, without limitation, those found in the following NIST publications:
<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>
<http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf>;

- Assessing the risk and magnitude of harm that could result from unauthorized access, use, disclosure, disruption, modification or destruction of information or information systems;
- Determining the levels of information security appropriate to protect information and information systems;
- Implementing policies and procedures to cost-effectively reduce risks to an acceptable level; and
- Regularly testing and evaluation of information security controls and techniques to ensure effective implementation and improvement of such controls and techniques.

Such standards and practices also include collaborating with, and utilizing the resources of, US-CERT and other organizations dedicated to protection of information systems and the sensitive data they process.

The SAIG Agreement also includes a provision that in the event of an unauthorized disclosure or an actual or suspected breach of applicant information or other sensitive information (such as PII) the institution must immediately notify FSA at CPSSAIG@ed.gov. This provision is especially important as it helps FSA identify risks and breaches that impact multiple institutions and other entities.

In addition to other provisions within the SAIG Agreement, FSA requires institutions to comply with the Gramm-Leach-Bliley Act. Under Title V of the Gramm-Leach-Bliley Act, financial services organizations, including institutions of higher education, are required to ensure the security and confidentiality of customer records and information. This requirement was recently added to the Program Participation Agreement and is reflected in the Federal Student Aid Handbook.

The HEA also requires institutions to maintain appropriate institutional capability for the sound administration of the Title IV programs. Such capability would include satisfactory policies, safeguards, monitoring and management practices related to information security. Further, FERPA generally prohibits institutions from having policies or practices that permit the disclosure of education records or PII contained therein without the written consent of the student, unless an exception applies. Any data breach resulting from a failure of an institution to

http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf; NIST 800-37 Rev. 1; and

<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171.pdf>. NIST 800-171.

In addition, useful resources for institutions can be found at the following:

Cyber Resiliency Reviews: <https://www.us-cert.gov/ccubedvp/self-service-crr>

Critical Infrastructure Cyber Community Voluntary Program: <https://www.us-cert.gov/ccubedvp/>

Cybersecurity Information Sharing and Collaboration Program: https://www.us-cert.gov/sites/default/files/c3vp/CISCP_20140523.pdf;

Enhanced Cybersecurity Services: <http://www.dhs.gov/enhanced-cybersecurity-services>

Information Sharing and Analysis Organization rollout: <http://www.dhs.gov/isao>

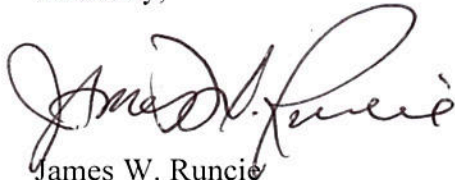
National Initiative for Cybersecurity Careers and Studies: <http://niccs.us-cert.gov>

maintain appropriate and reasonable information security policies and safeguards could also constitute a FERPA violation.

Finally, we note that institutions frequently enter into contractual arrangements with other organizations to fulfill institutional obligations with respect to the Title IV federal student financial assistance programs. If your institution has entered into such an arrangement, we remind you of 34 CFR §668.25, which includes a provision that the institution remains liable for any action by its third-party servicers.

If you have any questions about the information contained in this Dear Colleague Letter, please contact us at FSA_SchoolSecurity@ed.gov.

Sincerely,



James W. Runci
Chief Operating Officer
Federal Student Aid



Ted Mitchell
Under Secretary