Frequently Asked Questions about Cybersecurity Compliance

Who needs to worry about data security?

Data security affects everyone at a postsecondary institution (PSI) from the president to applicants. No one is exempt from data security, and each person has a role in ensuring data security.

Why do I need to worry about data security?

You should worry about data security for three reasons. First, the educational sector has an initial level of security maturity, as assessed by Gartner, which results in high risk and low cybersecurity maturity. Second, the educational sector is a rich trove of email addresses and credentials, financial information, research, and development. Third, PSIs that distribute Title IV funds have entered into agreements with FSA via a Program Participation Agreement (PPA) and a Student Aid Internet Gateway (SAIG) Agreement. Those agreements include stipulations about safeguarding data.

What are data security requirements?

Title IV PSIs are financial institutions per the *Gramm-Leach-Bliley Act* (GLBA, 2002). Per the Federal Student Aid (FSA) Program Participation Agreement (PPA) and the Student Aid Internet Gateway (SAIG) Agreement, PSIs must have GLBA safeguards in place. PSIs without GLBA safeguards may be found administratively incapable (unable to properly administer *Title IV* funds). GLBA safeguards require institutions to:

- develop, implement, and maintain a documented data security program;
- designate an employee or employees to coordinate the program;
- identify reasonably foreseeable internal and external risks to data security via formal, documented risk assessments of:
    - employee training and management;
    - information systems, including network and software design, as well as information processing, storage, transmission, and disposal; and
    - the ability to detect, prevent, and respond to attacks, intrusions, or other systems failures;
- control the risks identified, by designing and implement information safeguards and regularly test/monitor their effectiveness;
- oversee service providers by
    - taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the FSA, student, and school (customer) information at issue; and
    - requiring your service providers by contract to implement and maintain such safeguards; and

- evaluate and adjust your school's data security program in light of
  - the results of the required testing/monitoring,
  - any material changes to your operations or business arrangements, and
  - any other circumstances that you know may have a material impact on your information security program.

Further, *Title IV* schools are subject to the requirements of the Federal Trade Commission Identity Theft Red Flags Rule ("Red Flags Rule") (72 Fed. Reg. 63718) issued Nov. 9, 2007. The Red Flags Rule requires an institution to develop and implement a written identify theft prevention program to detect, prevent, and respond to patterns, practices, or specific activities that may indicate identity theft.

What is a breach?

Per GLBA, PSIs must protect against any unauthorized disclosure, misuse, alteration, destruction, or other compromise of information, such as unauthorized access. The Department of Education and Federal Student Aid considers each of these a breach. Each PSI must have in place administrative, technical, and physical safeguards which:

- ensure the security and confidentiality of customer information,
- protect against any anticipated threats or hazards to the security or integrity of such records, and
- protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

When do I report a breach?

The Student Aid Internet Gateway (SAIG) Agreement requires that as a condition of continued participation in the federal student aid programs, PSIs report actual data breaches, as well as suspected data breaches. *Title IV* PSIs must report **on the day** that a data breach is detected or even suspected. The U.S. Department of Education (the Department) has the authority to fine institutions—up to $54,789 per violation per 34 C.F.R. § 36.2—that do not comply with the requirement to self-report data breaches. The Department has reminded all institutions of this requirement through Dear Colleague Letters (GEN 15-18, GEN 16-12), electronic announcements, and the annual *FSA Handbook*.

How do I report a breach?

To report a breach, email cpssaig@ed.gov. Your email should include:

- date of the breach (known or suspected),
- impact of the breach (number of records, number of students, etc.),
- method of the breach (hack, accidental disclosure, etc.),
- information security program point of contact (email address and phone number are required),

- remediation status (complete, in-process, etc. with detail), and
- next steps (as needed).

If you cannot email, you should call the Department's security operations center (EDSOC) at 202-245-6550 to report the data listed above. EDSOC operates 24 hours a day, seven days per week.

We recently heard in an FSA conference session that we can no longer accept faxed or emailed copies of taxes or tax transcripts. Is this the case? Are we permitted to accept such documents via a student's school email account?

PSIs should never solicit personally identifiable information (PII)—especially sensitive personally identifiable information (SPII)—through means that are known to be insecure. PSIs should review their information requests and guidance to students and parents to ensure that instructions are clear about the explicit protection of data and how to transmit data securely transmittal.

PSIs must have secure means to receive inbound PII and SPII from students and parents. Secure means could include an appropriately safeguarded fax, a secure web portal to upload data and documents, student email accounts that encrypt communications to at least an AES-256-bit level, or separately encrypted attachments that are password protected (with the password provided in a separate email).

PSIs must remediate all data breaches. A data breach could be created if a student or parent sends PII or SPII via unsecure means, which would allow PII or SPII to be accessible by individuals who do not have a need to know.

PSIs must remediate this type of data breach immediately each time it occurs. However, at this time, this type of data breach does not need to be reported as an institutional data breach to FSA.

How can students or parents create an encrypted attachment to send to a PSI?

There are many applications that have the ability to encrypt attachments. An example is provided below for WinZip™, with the caveat that this is not the only acceptable method, and unless very carefully configured, WinZip would not fit the Federal Information Processing Standard (FIPS) which is defined by FIPS 140-2. The minimum acceptable encryption is AES 256-bit for PSIs.

WinZip instructions for file/folder encryption and password protection	
1	Open a folder to the location of the file(s)/folder(s) that you wish to encrypt.
2	Select the file(s)/folder(s) that you wish to encrypt. Note that in order to select more

	than one file/folder, you must press the “Ctrl” key on the keyboard while selecting them.
3	Right-click over one of the selected items.
4	Select WinZip. From the submenu that appears, select “Add to Zip File.”
5	In the “Add Files” dialog box, specify a ‘File name’ and ‘Destination’ (location) for the finished Zip file.
6	Select “.Zip” as the Compression Type.
7	Under Encryption, check the “Encrypt files” box.
8	Click the “Add” button.
9	A pop-up window may appear saying “You should be aware of the advantages and disadvantages of the various encryption methods before using this feature. Please press the F1 key for more information, particularly if this is the first time you are using encryption.” Select the “OK” button to continue.
10	In the “Enter Password” field, enter an appropriate password. Passwords must be at least eight characters and must contain at least one of each the following: a lowercase character (a-z), an uppercase character (A-Z), a number character (0-9), and a symbol character (!, @, #, $, %, ^, &, *, etc.).
11	In the “Re-enter Password” field, enter the same password from Step #10, and remember the password for future reference.
12	Click the “OK” button.
13	A pop-up window may appear saying “Add Complete. Your files have been added. The files will be compressed and encrypted when saved.” Click the “OK” button to continue.
14	The encrypted WinZip file should be in the location identified in Step #5 above.
15	The password must not be included in the same message and should either be included in a separate email or verbally provided to the intended user.

What if we have the documents faxed? Our fax has documents going straight to the document imaging/storage area on a server. Paper does not print. Is this an acceptable practice? Can a fax in-transmission be hacked?

Faxing, if safeguarded, is not a breach. It is assumed that a PSI has already performed a risk assessment and has secured access to the physical server. It is a further assumption that technical and logical controls are in place that would prevent individuals without a need to know (for example, system administrators) from viewing PII or SPII.

More specifically, faxes arriving securely would depend on the method of how it arrives. If the fax is printed upon arrival from a fax machine or if the fax is transmitted to a server, physical and administrative safeguards must ensure the data are only viewed or handled by authorized personnel with a need to know. Confidentiality and integrity are each key whether it is physical or digital.

The fax-hack question is substantively different. A lot would depend on if your institution is leveraging a Private Branch Exchange (PBX) or if it is a straight Signaling System 7 (SS7) connection to the standard Public Switched Telephone Network (PSTN). Physical or logical access to the PBX on your campus or cloud has the potential for breach, as well physical access to your PSTN equipment. Any of these could potentially cause a breach in the confidentiality of the data.

However, as a PSI, your team should do a risk assessment of your technology design and handling process to review where risks exist and put in the appropriate controls or compensating controls. You also should document your risks and controls in your information security program document. Examples include putting the fax machine (PTSN connection, physical print-out type that is the non-networked standard) in a controlled space that only authorized personnel can access. For the hack risk, you might inspect from the demarcation point to the device regularly to ensure no interception evidence. You may further document the security controls inherited via your ILEC/CLEC (telephone service carrier). Regular testing also should be documented to show that your PSI has given this thoughtful consideration.