Chapter 7

Record Keeping, Privacy, & Electronic Processes

Schools must maintain detailed records to show that FSA funds are disbursed in the correct amounts to eligible students. These records must be retained for a certain amount of time and made available to authorized parties in the course of audits, program reviews, or investigations. Personally identifiable information in these records must be safeguarded and may only be released to other parties under certain conditions specified in the regulations. You may wish to share the contents of this chapter with your school's IT office or provider.

Required Records

A school must keep comprehensive, accurate program and fiscal records related to its use of FSA program funds. Complete and accurate records are important. Program and fiscal records must demonstrate the school is capable of meeting the administrative and fiscal requirements for participating in the FSA programs. Records must demonstrate proper administration of FSA program funds and show a clear audit trail for FSA program expenditures. For example, records for each FSA recipient must clearly show that the student was eligible for the funds received and that the funds were disbursed according to program regulations. To assess your compliance with the provisions of this chapter, see Activity 2 on the fiscal management page of the FSA Assessments website.

In addition to the general institutional record keeping requirements discussed here, a school must also comply with all program-specific record keeping requirements contained in the individual FSA regulations.

Record keeping

34 CFR 668.24

Closed school or branch

If a school closes, stops providing educational programs, is terminated or suspended from the FSA programs, or undergoes a change in ownership that results in a change of control, it must provide for the retention of required records. It must also provide for access to those records for inspection and copying by the Department. A school that formerly participated in the FFEL Program must also provide access for the appropriate guaranty agency.

If a school has an additional location or branch that closes, the school should maintain its loan records beyond the end of the three-year record retention requirement to respond to the Department or to refute borrower claims of eligibility for discharge.

Records related to school eligibility

A school must establish and maintain on a current basis any application the school submitted for FSA program funds. Other program records that must be maintained include:

- Program Participation Agreement (PPA), approval letter, and Eligibility and Certification Approval Report (ECAR),
- application portion of the FISAP,
- accrediting and licensing agency reviews, approvals, and reports,
- state agency reports,
- audit and program review reports,
- self-evaluation reports, and
- other records, as specified in regulation, that pertain to financial responsibility and standards of administrative capability.

Records relating to student eligibility

A school must keep records that substantiate the eligibility of students for FSA funds, such as:

- cost of attendance information,
- documentation of a student's satisfactory academic progress (SAP),
- documentation of student's program of study and the courses in which the student was enrolled,
- data used to establish student's admission, enrollment status, and period of enrollment,
- required student certification statements and supporting documentation,
- documents used to verify applicant data and resolve conflicting information,
- documentation of all professional judgment decisions, and
- financial aid history information for transfer students.

Fiscal records

As part of meeting its fiduciary responsibilities, a school must maintain accounting and fiscal records to demonstrate its proper use of FSA funds. A school's fiscal records must provide a clear audit trail that shows that funds were received, managed, disbursed, and returned in accordance with federal requirements.

The fiscal records a school must maintain include but are not limited to the following:

- records that reflect each FSA program transaction,
- bank statements for all accounts containing FSA funds,
- records of student accounts, including each student's institutional charges, cash payments, FSA payments, cash disbursements, re- funds, returns, and overpayments required for each enrollment period,
- general ledger (control accounts) and related subsidiary ledgers that identify each FSA program transaction (FSA transactions must be separate from school's other financial transactions),
- Federal Work-Study payroll records, and
- the fiscal operations report portion of the FISAP.

A school must also maintain records that support data appearing on required reports, such as, but not limited to:

- Pell Grant statements of accounts,
- cash requests and quarterly or monthly reports from the G6 payment system (formerly G5),
- FSA program reconciliation reports,
- audit reports and school responses,
- state grant and scholarship award rosters and reports,
- accrediting and licensing agency reports, and
- records used to prepare the income grid on the FISAP.

Loan program records

There are special record keeping requirements in the Direct and FFEL loan programs. A school must maintain

- A copy of the paper or electronic loan certification or origination record, including the loan amount and the period of enrollment.
- The cost of attendance, estimated financial assistance, and expected family contribution used to calculate the loan amount (and any other information that may be required to determine the borrower's eligibility, such as the student's Federal Pell Grant eligibility or ineligibility).
- The date(s) the school disbursed the loan funds to the student (or to the parent borrower), and the amount(s) disbursed. (For loans delivered to the school by check, the date the school endorsed each loan check, if required.)
- Documentation of the confirmation process for each academic year in which the school uses the multi-year feature of the Master Promissory Note. This may be part of the borrower's file, but acceptable documentation can also include a statement of the confirmation process that was printed in a student handbook or other financial aid publication for that school year. The documentation may be kept in paper or electronic form. There is no retention limit for this

documentation; you must keep it indefinitely because it may affect the enforceability of loans.

Loan program records

34 CFR 668.24,

34 CFR 682.610, and

34 CFR 685.309(c)

A school must keep records relating to a student or parent borrower's eligibility and participation in the Direct Loan or FFEL program for three years after the end of the award year in which the student last attended the school. A school must keep all other records relating to the school's participation in the Direct Loan or FFEL program for at least three years after the end of the award year in which the records are submitted.

Campus-Based records

Schools participating in the Campus-Based Programs must keep the FISAP and any records supporting the data used to create it (e.g., the source data for the income grid) for three years from the end of the award year in which the FISAP is submitted. Consider the Fiscal Operations Report for 2022–2023 and Application to Participate for 2024–2025. It is submitted during the 2023–2024 award year by September 29, 2023. That award year ends on June 30, 2024, so schools must retain the data used to create that FISAP until at least June 30, 2027 (three years from June 30, 2024).

See *Volume 6—Campus-Based Programs, Chapter 1,* for a discussion of the record-keeping requirements for the FWS and FSEOG programs, and see *Chapter 3* of that volume about Perkins record keeping.

Record Retention Periods

Schools must retain all required records for a minimum of three years from the end of the award year. However, the starting point for the three-year period is not the same for all records. For example, FFEL/DL reports must be kept for three years after the end of the award year in which they were submitted, while borrower records must be kept for three years from the end of the award year in which the student last attended.

Different retention periods are necessary to ensure enforcement and repayment of Perkins loans, which are normally held by the school. Perkins Loan repayment records, including cancellation and deferment records, must be kept for three years from the date that the loan was assigned to the Department, cancelled, or repaid. Perkins original promissory notes and original repayment schedules must be kept until the loan is satisfied or needed to enforce the obligation.

A school may retain records longer than the minimum period required. Moreover, a school may be required to retain records involved in any loan, claim, or expenditure questioned in any FSA program review, audit, investigation, or other review, for more than three years (see *Chapter 8* for information on program reviews and audits). If the three- year retention period expires before the issue in question is resolved, the school must continue to retain all records until resolution is reached.

There are also additional record retention requirements that apply to schools granted waivers of the audit submission requirements.

Summary of Record Retention Requirements

From 34 CFR 668.24 Record retention and examinations.

Program Records

A school must establish and maintain, on a current basis, any application for FSA funds and program records that document—

- the school's eligibility to participate in the Title IV, HEA programs,
- the eligibility of the school's educational programs for Title IV, HEA program funds,
- the school's administration of the Title IV, HEA programs in accordance with all applicable requirements,
- the school's financial responsibility,
- information included in any application for Title IV, HEA program funds, and
- the school's disbursement and delivery of Title IV, HEA program funds.

Fiscal records

A school must account for the receipt and expenditure of all FSA program funds in accordance with generally accepted accounting principles.

A school must establish and maintain on a current basis—

- financial records that reflect each Title IV, HEA program transaction, and
- general ledger control accounts and related subsidiary accounts that identify each Title IV, HEA program transaction and separate those transactions from all other school financial activity.

Records for Title IV aid recipients

A school must maintain records for each Title IV recipient that include but are not limited to—

- The Student Aid Report (SAR) or Institutional Student Information Record (ISIR) used to determine a student's eligibility for FSA program funds,
- Application data submitted to the Department, lender, or guaranty agency by the school on behalf of the student or parent,
- Documentation of each student's or parent borrower's eligibility for Title IV, HEA program funds (e.g., records that demonstrate that the student has a high school diploma, GED, or the ability to benefit),
- Documentation relating to each student's or parent borrower's receipt of Title IV, HEA program funds, including but not limited to:
    - The amount of the grant, loan, or FWS award; its payment period; its loan period, if appropriate; and the calculations used to determine the amount of grant, loan, or FWS award;
    - The date and amount of each disbursement of grant or loan funds, and the date and amount of each payment of FWS wages;
    - The amount, date, and basis of the school's calculation of any refunds/returns or overpayments due to or on behalf of the student, or the treatment of Title IV, HEA program funds when a student withdraws; and
    - The payment of any overpayment or return of Title IV, HEA program funds to the to the Department.
- Documentation of and information collected at any initial or exit loan counseling required by applicable program regulations,
- Reports and forms used by the school in its participation in a Title IV, HEA program, and any records needed to verify data that appear in those reports and forms,
- Documentation supporting the school's calculation of its completion or graduation rates, and transfer-out rates under 34 CFR 668.45 (see *Chapter 6*).

Minimum Record Retention Periods

Pell and TEACH grants, Campus-Based Program records

3 years from the end of the award year for which the aid was awarded

Except:

- Fiscal Operations Report (FISAP) and supporting records—3 years from the end of the award year in which the report was submitted
- Perkins repayment records*—Until the loan is satisfied, or the documents are no longer needed to enforce the obligation
- Perkins original promissory notes—3 years from the date the loan is assigned to ED, canceled, or repaid

Direct Loans & FFEL

- Records related to borrower's eligibility and participation—3 years from the end of the award year in which the student last attended
- All other records, including any other reports or forms—3 years from the end of the award year in which the report was submitted

*includes original repayment schedule, though manner of retention remains same as promissory note

Record Maintenance

Acceptable formats

A school must maintain all required records in a systematically organized manner. Unless a specific format is required, a school may keep required records in:

- hard copy
- microform
- computer file
- optical disk
- CD-ROM
- other media formats

Record retention requirements for the Institutional Student Information Record (ISIR) are discussed here. All other record information, regardless of the format used, must be retrievable in a coherent hard copy format (for example, an easily understandable printout of a computer file) or in a media format acceptable to the Department.

Any document that contains a signature, seal, certification, or any other image or mark required to validate the authenticity of its information must be maintained in its original hard copy or in an imaged media format. This includes tax returns, verification statements, and Student Aid Reports (SARs) used to determine eligibility, and any other document when a signature, seal, etc., contained on it is necessary for the document to be used for the purposes for which it is being retained.

A school may maintain a record in an imaged media format only if the format is capable of reproducing an accurate, legible, and complete copy of the original document. When printed, the copy must be approximately the same size as the original document.

Please note that promissory notes that are signed electronically must be stored electronically and the promissory note must be retrievable in a coherent format. Because Direct Loan MPNs are stored in COD, this requirement can be satisfied through COD.

The requirement providing for other media formats acceptable to the Department allows for the use of new technology as

it is developed. The Department will notify schools of acceptable media formats; schools should not apply for approval of a media format.

Requirements for electronic promissory notes

34 CFR 668.24(d)(3)(i) through (iv)

Special requirements for SARs and ISIRs

Special maintenance and availability requirements apply for SARs and ISIRs used to determine eligibility. It is essential that these basic eligibility records be available in a consistent, comprehensive, and verifiable format for program review and audit purposes.

Hard copies of SARs that students submit to schools must be maintained and available in their original format or in an imaged media format. The ISIR, an electronic record, must be maintained and available in its original format (e.g., as it was archived using EDExpress software supplied to the school). A school that uses EDExpress has the ability to preserve the ISIR data that it has maintained during the applicable award year by archiving the data to a disk or other computer format.

Examination of Records

Location

A school must make its records readily available to the Department at a location of the school designated by the Department. These include any records of transactions between the school and the financial institution where it deposits FSA funds.

A school is not required to maintain records in any specific location. For example, it may be more appropriate for a school to maintain some records in the financial aid office while maintaining others in the business office, the admissions office, or the office of the registrar. The responsible administrator in the office maintaining the records should be aware of all applicable record retention requirements.

Cooperation with agency representatives

A school that participates in any FSA program and the school's third-party servicers, if any, must cooperate with the agencies and individuals involved in conducting any audit, program review, investigation, or other review authorized by law. See *Chapter 4* for more information on independent audits and *Chapter 8* for information on program reviews. A school must also provide this cooperation to its accrediting agency and to any guaranty agency in whose program the school participates.

Cooperation must be extended to the following individuals and their authorized representatives: an independent auditor, the Secretary of the Department of Education, the Department's Inspector General, and the Comptroller General of the United States. See the Electronic Announcement GEN-23-56 July 2023 enforcement bulletin about nondisclosure agreements improperly limiting or prohibiting employee communications with the Department.

A school must cooperate by providing

- Timely access to requested records, pertinent books, documents, papers, or computer programs for examination and copying by any of the agents listed above. The records to which timely access must be provided include but are not limited to computerized records and records reflecting transactions with any financial institution with which the school or servicer deposits or has deposited any FSA program funds.
- Reasonable access to all personnel associated with its or its servicer's administration of the FSA programs so that any of the agents listed above may obtain relevant information. A school or servicer must allow those personnel to

supply all relevant information and to be interviewed without the presence of the school's or servicer's management (or tape recording of the interviews by the school or servicer).

If requested by the Department, a school or servicer must provide promptly any information the school or servicer has regarding the last known address, full name, telephone number, enrollment information, employer, and employer address of a recipient of FSA program funds who attends or attended the school. A school must also provide this information, upon request, to a lender or guaranty agency in the case of a borrower under the FFEL Program.

Examination of records

34 CFR 668.24(f)

Privacy of Student Information Under FERPA

The Family Educational Rights and Privacy Act of 1974 (FERPA) is a federal law that protects the privacy of students' education records, which are records that are: (1) directly related to a student; and (2) maintained by an education agency or postsecondary institution or by a party acting for the agency or institution. The student records of a housing facility owned by a third party that has a contract with a school to provide housing for its students are considered under the control of the school (whether the rent is paid directly by the student or by the school on their behalf). Records maintained by the third party or the school related to students living in that housing are subject to FERPA. Note: Do not confuse FERPA with the Privacy Act of 1974 that governs the records kept by government agencies, including the application records in the federal processing system.

FERPA citations

20 USC 1232g

34 CFR 99.7 Notification of FERPA Rights

34 CFR 99.8 Law enforcement unit records

34 CFR 99.10, 11, and 12 Right of student to review records

34 CFR 99.20, 21, and 22 Right of student to request amendment to records

34 CFR 99.30 Prior consent requirement

34 CFR 99.31 When prior consent is not required to disclose information

34 CFR 99.32 Record keeping requirement

34 CFR 99.33 Limitations on redisclosure

34 CFR 99.34 Disclosure to other agencies/institutions

34 CFR 99.35 Disclosure to certain authorities for audit or evaluation of education programs

At the postsecondary level, FERPA affords eligible students with certain rights. FERPA defines an "eligible student" as a student who has reached 18 years of age or is attending an institution of postsecondary education at any age. With exceptions such as those noted in this section, FERPA affords postsecondary students the right to inspect and review their

education records, the right to seek to have their records amended and the right to have some control over the disclosure of personally identifiable information from their education records.

These rules apply to all education records a school keeps, including admissions records (only if the student was admitted), academic records, and any financial aid records pertaining to the student. Therefore, the financial aid office is not usually the office that develops a school's FERPA policy or the notification to students, although it may have some input.

You can read the FERPA model notification that the Department has posted online. The Department has issued a technical assistance document that provides information on FERPA and HEA legal requirements related to preparing for and addressing situations that threaten the health or safety of the campus community. The Department's Student Privacy Policy Office (SPPO) administers FERPA; for more information, see the Protecting Student Privacy website.

Sole possession records

Sole possession records are exempted from the definition of education record and thus are not subject to FERPA. They are kept in the sole possession of the maker of the record and are

- used as a memory or reference tool, and
- not accessible or revealed to any other person except a temporary substitute for the maker of the record.

Student's right to review education records under FERPA

A school must provide a student with an opportunity to review his or her education records within 45 days of the receipt of a request. A school is only required to provide the student with copies of education records or make other arrangements to provide the student access to the records if a failure to do so would effectively prevent the student from obtaining access to the records. A case in point would be a situation in which the student does not live within commuting distance of the school. While the school may not charge a fee for retrieving the records, it may charge a reasonable fee for providing copies of the records, provided that the fee would not prevent access to the records.

While the rights under FERPA have transferred from a student's parents to the student when the student attends a postsecondary institution, FERPA does permit a school to disclose a student's education records to his or her parents if the student is a dependent student under IRS rules.

Note that the IRS definition of a dependent is quite different from that of a dependent student for FSA purposes. For IRS purposes, students are dependent if they are listed as dependents on their parent's income tax returns. (If the student is a dependent as defined by the IRS, disclosure may be made to either parent, regardless of which parent claims the student as a dependent.)

There are other situations in which information about a student may be disclosed to her parents. A school official may

- disclose information from a student's education records to parents in the case of a health or safety emergency involving the student.
- let parents of students under the age of 21 know when the student has violated any law or policy concerning the use or possession of alcohol or a controlled substance.
- share with parents information that is based on that official's personal knowledge or observation and that is not based on information contained in an education record.

Prior written consent to disclose the student's records

Except under one of the special conditions described in this section, a student must provide written consent before an education agency or institution may disclose personally identifiable information from the student's education records.

The written consent must state the purpose of the disclosure, specify the records that may be disclosed, identify the party or class of parties to whom the disclosure may be made, and be signed and dated.

If the consent is given electronically, the consent form must identify and authenticate a particular person as the source of the electronic consent and indicate that person's approval of the information contained in the electronic consent.

The FERPA regulations include a list of exceptions where the school may disclose personally identifiable information from

the student's file without prior written consent. Several of these allowable disclosures are of particular interest to the financial aid office, since they are likely to involve the release of financial aid records.

Disclosures to school officials

Some of these disclosures may be made to officials at your school under certain conditions. Typically, these might include disclosures of admissions records, grades, or financial aid records. Disclosure may be made to other school officials, including teachers, within the school whom the school has determined to have legitimate educational interests.

Third-party servicers that your school has contracted with to perform Title IV functions are considered school officials under FERPA when they perform any of the following:

- perform a school service or function for which your school would otherwise use employees,
- are under the control of your school with respect to the use and maintenance of education records, and
- comply with FERPA requirements about the use and redisclosure of personal information from education records.

A school official may disclose personally identifiable information from student education records to a third-party servicer who meets the above criteria if the official determines that the third-party servicer has a "legitimate educational interest." Your school must include in its annual notification of rights under FERPA the criteria for determining who is a school official and what constitutes a legitimate educational interest. A school official typically has a legitimate educational interest if the official needs to review an education record in order to fulfill his or her professional responsibility. Also, for such servicers to receive disclosures without student consent as though they were school officials, they must not use that personal information to set up a bank account or maintain a credit balance for students. See DCL GEN-23-03.

Disclosures to another institution

FERPA permits an institution to disclose education records to officials of another postsecondary institution where the student seeks or intends to enroll or where the student is already enrolled so long as the disclosure is for purposes related to the student's enrollment or transfer. [34 CFR 99.31(a)(2) & 34 CFR 99.34.]

If your school routinely discloses information to other schools where students seek to enroll, it should include this information in its annual privacy notification to students, or, if not, your school must make a reasonable attempt to notify students at their last known address.

Crime and security records

There are two different FERPA provisions concerning the release of records relating to a violent crime. One concerns the release to the victim of an alleged perpetrator of a crime of violence or a non-forcible sex offense. The disclosure may only include the final results of the disciplinary proceeding conducted by the school. The school may disclose the final results of the disciplinary proceeding, regardless of whether the school concluded a violation was committed [34 CFR 99.31(a)(13)]. A separate provision permits a school to disclose to anyone the final results of any disciplinary hearing against an alleged perpetrator of a crime of violence only when that student was found in violation of the school's policy on the offense 34 CFR 99.31(a)(14)].

Records created and maintained by a school's law enforcement unit are exempt from the privacy restrictions of FERPA. A school may disclose information from these "law enforcement unit records" to anyone—including parents or federal, state, or local law enforcement authorities— without the student's consent pursuant to school policy and/or state law.

Disclosures to government agencies

Disclosures may be made for audit, evaluation, and enforcement purposes to authorized representatives of the U.S. Department of Education, which include employees of the Department—such as those of the National Center for Education Statistics and the offices of Federal Student Aid, Postsecondary Education, Inspector General and Civil Rights—as well as firms under contract to the Department to perform certain administrative functions or studies.

In addition, disclosure may be made if it is in connection with financial aid the student has received or applied for. Such disclosure may only be made if the student information is needed to determine the amount of the aid or the conditions or

student's eligibility for the aid or to enforce the terms or conditions of the aid.

Schools may, without violating FERPA, release personally identifiable information on nonimmigrant students with an F, J, or M visa to U.S. Immigration and Customs Enforcement in compliance with the Student Exchange Visitor Information System program.

Disclosures in response to subpoenas or court orders

FERPA permits schools to disclose personally identifiable information from a student's education records without the student's consent to comply with a lawfully issued subpoena or court order. In most cases the school must make a reasonable effort to notify the student who is the subject of the subpoena or court order before complying so that he may seek protective action. However, the school does not have to notify the student if the court or issuing agency has prohibited such disclosure if certain conditions are met.

A school may also disclose information from education records, without the consent or knowledge of the student, to representatives of the U.S. Department of Justice in response to an *ex parte* order issued in connection with the investigation of crimes of terrorism. "Terrorism" and "crimes of terrorism" are defined in 18 USC 2331 and 2332b(g)(5)(B).

Subpoena citations

20 USC 1232g(b)(1)(J)(i) and (ii), (b)(2)(B)

20 USC 1232g(b)(4)

34 CFR 99.31(a)(9)

34 CFR 99.32

Documenting the disclosure of information

A school does not have to record requests for access made by the eligible student, a school official who has a legitimate educational interest, some court orders or subpoenas, or a party seeking directory information or who has written consent from the eligible student.

Otherwise, a school must keep a record of each request for access and each disclosure of personally identifiable information from a student's education records to other parties. The record of the request and disclosure must identify the parties who requested the information and their legitimate interest in the information. This record must be maintained in the student's file as long as the education records themselves are kept. [34 CFR 99.32]

For instance, if Department officials request student records in the course of a program review, the school must document in each student's file that his or her records were disclosed to representatives of the Department. An easy way for the school to do this is to photocopy a statement to this effect and include it in each student's file. A statement such as the following would be appropriate for a program review conducted by a Department regional office.

These financial aid records were disclosed to representatives of the U.S. Department of Education, School Participation Division, Region, on (Month/Day/Year) to determine compliance with financial aid requirements, under 34 CFR 99.31(a)(4).

When redisclosure is anticipated, the additional parties to whom the information will be disclosed must be included in the record of the original disclosure. For instance, to continue the example for an FSA program review, the following statement might be added.

The School Participation Division may make further disclosures of this information, consistent with 34 CFR 99.33(b), to the Department's Office of Inspector General. Schools should check with program review staff to find out if any redisclosure is anticipated.

FERPA Responsibilities and Student Rights

A school is required to

- annually notify students of their rights under FERPA;
- include in that notification the procedure for exercising their rights to inspect and review education records; and
- maintain a record in a student's file listing to whom personally identifiable information was disclosed and the legitimate interests the parties had in obtaining the information (does not apply to school officials with a legitimate educational interest or to directory information).

A student has the right to

- inspect and review any education records pertaining to the student;
- request an amendment to his/her records; and
- consent to disclosure of personally identifiable information from education records, except when FERPA permits disclosure without consent.

HIPAA (Privacy of Health Records) and FERPA

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) sets standards to protect the confidentiality of health information.

However, the HIPAA Privacy Rule excludes from its coverage those records that are protected by FERPA at educational agencies and institutions that provide health or medical services to students. This is because Congress specifically addressed how education records should be protected under FERPA. For this reason, student health records are protected by FERPA, not the HIPAA Privacy Rule.

Your school's disability services office normally obtains and maintains health records for each student who applies for services or waivers, so the receipt and maintenance of health records by student services units is well established. Note: In many cases a student receiving a waiver from a school's academic progress policy would also have applied for services from your school's disability services office. Since most financial aid offices are not used to handling medical records, you may find it more practical to have the disability services office maintain the record and to refer- ence that record in your file in the financial aid office. Of course, you will have to ensure that the record maintenance requirements are complied with.

It may be helpful to review this guidance on HIPAA and FERPA. For more information on HIPAA, see HHS's HIPAA website. HIPAA regulations are published as 45 CFR Parts 160, 162, and 164.

Higher Education Act Data Use Limitations

The HEA also provides limitations on the uses of certain types of data. The provisions of the HEA apply differently to information collected on or derived from the FAFSA. This means that the HEA's provisions apply to data on the ISIR (including award and disbursement information) and to data included in NSLDS (including data on the ISIR from NSLDS).

The HEA restricts the use of the FAFSA/ISIR data to the application, award, and administration of aid awarded under the Title IV programs, state aid, or aid awarded by eligible institutions. The Department interprets "administration of aid" to include audits and program evaluations necessary for the efficient and effective administration of those student aid programs.

The HEA also prohibits nongovernmental researchers or policy analysts from accessing PII from NSLDS and prohibits the use of NSLDS data for marketing purposes. It is important to note that these prohibitions are applicable to all NSLDS data, including NSLDS data received by institutions via the ISIR.

FAFSA data restrictions

HEA Section 483(a)(3)(E)
NSLDS restrictions
HEA Section 485B(d)(2)

Sharing FAFSA Data

An institution of higher education may, with explicit written consent of an applicant who has completed a FAFSA under section 483(a), provide such information collected from the applicant's FAFSA as is necessary to a scholarship-granting organization, including a tribal organization (defined in section 4 of the Indian Self-Determination and Education Assistance Act, 25 U.S.C. 5304), or to an organization assisting the applicant in applying for and receiving federal, state, local, or tribal assistance that is designated by the applicant to assist the applicant in applying for and receiving financial assistance for any component of the applicant's cost of attendance (defined in section 472 of the HEA) at that institution.

Guidance on the Use of Financial Aid Information for Program Evaluation and Research

The Department of Education through SPPO's Privacy Technical Assistance Center (PTAC) has published *Guidance on the Use of Financial Aid Information for Program Evaluation and Research* to help schools understand using student financial aid information for program evaluation and research. That guidance is available at

studentprivacy.ed.gov

An organization that receives such information is prohibited from selling or otherwise sharing such information.

See the Department of Defense and Labor, Health and Human Services, and Education Appropriations Act, 2019 and Continuing Appropriations Act, 2019.

The E-sign Act and Information Security

The Electronic Signatures in Global and National Commerce Act (E-Sign Act) provides, in part, that a signature, contract, or other record relating to a transaction may not be denied legal effect, validity, or enforceability solely because it is in electronic form or because an electronic signature or electronic record was used in its formation. The E-Sign Act permits lenders, guaranty agencies, and schools to use electronic signatures and electronic records in place of traditional signatures and records that, under the HEA and underlying regulations, otherwise must be provided or maintained in hard-copy format.

Unless a statute or regulation specifically requires a school to provide or maintain a record or document on paper, obtain a pen and paper signature, or send a notification or authorization via U.S. mail, your school may, respectively,

- provide and maintain that record electronically,
- obtain the signature electronically as long as the electronic process complies with the E-Sign Act and all other applicable laws,
- provide notices or receive authorizations electronically. You may also use an electronic process to provide required

notices and make disclosures by directing students to a secure website that contains the required notifications and disclosures.

For additional information on electronic transactions involving student loans, see Section 2 of *Standards for Electronic Signatures in Electronic Student Loan Transactions*, in GEN-01-06.

Information security requirements

15 USC 6801(b), 6805(b)(2)

Federal Trade Commission regulations

16 CFR 313.3(n) and

16 CFR 314.1–5

Obtaining voluntary consent for electronic transactions

Before using electronic transactions to communicate with a recipient of FSA funds, the recipient must affirmatively consent to the use of an electronic record. The recipient's consent must be voluntary and based on accurate information about the transactions to be completed. This consent to participate in electronic transactions is required for all financial information provided or made available to student loan borrowers and for all notices and authorizations to FSA recipients required under 34 CFR 668.165—Notices and Authorizations. See *Volume 4* for more information on notices and authorizations for disbursements.

The consent must be obtained in a manner that reasonably demonstrates that the person can access the information to be provided in an electronic form. For example, if you are going to send financial information by email, you could send a request for consent to the recipient via email, require the recipient to respond in a like manner, and maintain a record of that response.

Safeguarding confidential information in electronic processes

Any time a school uses an electronic process to record or transmit confidential information or obtain a student's confirmation, acknowledgment, or approval, the school must adopt reasonable safeguards against possible fraud and abuse. Reasonable safeguards a school might take include password protection, password changes at set intervals, access revocation for unsuccessful logins, user identification and entry-point tracking, random audit surveys, and security tests of the code access.

If your school uses an electronic process to provide notices, make disclosures, and direct students to a secure website, it must provide notice of this each year to each student, whether via email, campus mail, or the traditional mail of the U.S. Postal Service.

The annual individual notice must

- identify the information required to be disclosed that year,
- provide the exact Web address for the information,
- state that persons are entitled to a paper copy upon request, and
- inform students how to request a paper copy.

Establishing and maintaining an information security program

The Federal Trade Commission (FTC) has ruled that most colleges are subject to the provisions of the Financial Services Act's Security Provisions (also known as the Financial Services Modernization Act). In the regulation, the commission

created a definition of financial institutions that includes most colleges on the basis of the financial relationships they have with students, donors, and others. Consequently, colleges must adopt an information security program and draft detailed policies for handling financial data covered by the law, such as parents' annual income, and take steps to protect the data from falling into the wrong hands. For specific requirements, see the discussion under *FTC Standards for Safeguarding Customer Information* later in this chapter.

While colleges have flexibility in choosing a system that provides for electronic requests for release of personally identifiable information, they must ensure that their systems provide adequate safeguards. Also, the FTC requirements apply to Title IV third-party servicers, so colleges must use servicers that are capable of maintaining such safeguards and must require servicers by contract to implement and maintain those safeguards.

Protecting student information

Under their Program Participation Agreement (PPA) and the Gramm-Leach-Bliley Act (Public Law 106-102), schools must protect student financial aid information, with particular attention to information provided to institutions by the Department or otherwise obtained in support of the administration of the federal student financial aid programs.

The GLBA requires institutions to, among other things,

- Develop, implement, and maintain a written information security program;
- Designate the employee(s) responsible for coordinating the information security program;
- Identify and assess risks to customer information;
- Design and implement an information safeguards program;
- Select appropriate service providers that are capable of maintaining appropriate safeguards; and
- Periodically evaluate and update their security program.

Presidents and chief information officers of institutions should have, at a minimum, evaluated and documented their current security posture against the requirements of GLBA and have taken immediate action to remediate any identified deficiencies.

The Department is incorporating the GLBA security controls into the Annual Audit Guide in order to assess and confirm schools' compliance with the GLBA. The Department will require the examination of evidence of GLBA compliance as part of schools' annual student aid compliance audit.

See DCL GEN-15-18 on protecting student information. It gives suggestions and resources for following industry standards and best practices on managing information systems. GEN-16-12 offers more information. On February 9, 2023, the Department posted DCL GEN-23-09, providing an overview and resources for updates to GLBA requirements under the FTC's Final Rule amending the Standards for Safeguarding Customer Information (Safeguards Rule), published December 9, 2021. The deadline for institutions to comply with these standards was June 9, 2023.

In August 2018 the Department issued a warning about a malicious phishing campaign that sought access to student accounts via student portals. That announcement identified single-factor authentication as a weakness exploited in these cyberattacks and recommended that colleges use two- or multi-factor authentication to reduce the likelihood of such security breaches. To report incidents or get answers to questions about cybersecurity, send an email to FSA_IHECyberCompliance@ed.gov.

Reporting Security Breaches to Students and the Department

The Department considers any breach in the security of student records and information to be a demonstration of a potential lack of administrative capability.

Schools' SAIG Agreements include a provision that schools must immediately notify the Department when there is breach of security of student records and information, and ED strongly encourages schools to notify their students of the breach at the same time. To notify the Department, schools should use the Cybersecurity Breach Intake form on the FSA Partners website.

In completing the form for the Department, schools should include the following:

- Date of breach (suspected or known)
- Impact of breach (# of records, etc.)
- Method of breach (hack, accidental disclosure, etc.)
- Information Security Program Point of Contact - Email and phone details
- Remediation Status (complete, in process - with detail)
- Next steps (as needed)

Federal Student Aid has consolidated its cybersecurity compliance information and resources on its FSA Cybersecurity Compliance site.

NIST Special Publication 800-171 Rev. 2

As data breaches increase, it is vital that schools protect controlled unclassified information (CUI) used in the administration of the federal student aid programs. Since 2018 many schools have adopted some or all of the recommended requirements of National Institute of Standards and Technology (NIST) Special Publication 800–171. We further encourage use of NIST 800–171 Rev. 2, *Controlled Unclassified Information in Non- federal Systems*, to help mitigate risks related to CUI.

FTC Standards for Safeguarding Customer Information

Colleges participating in the FSA programs are subject to the information security requirements established by the FTC for financial institutions.

Customer information that must be safeguarded

These requirements apply to all customer information your school has, regardless of whether it pertains to students, parents, or others your school has a customer relationship with or pertains to the customers of other financial institutions that have given such information to you.

Customer information is any record containing nonpublic personal information[1] about a customer of a financial institution, whether in paper, electronic, or other form, that is handled or maintained by or on behalf of you or your affiliates.

Establishing and maintaining an information security program

As a financial institution covered under these information security requirements, your school must develop, implement, and maintain a comprehensive information security program.[2]

The information security program must be written in one or more readily accessible parts and contain

Risk assessment. Your school must identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information and assess the sufficiency of any safeguards in place to control these risks.

At a minimum, the school's risk assessment should include consideration of risks in each relevant area of your operations, including

- employee training and management,
- information systems, including network and software design, as well as information processing, storage, transmission, and disposal, and
- detecting, preventing, and responding to attacks, intrusions, or other system failures.

Safeguards and testing/monitoring. Your school must design and implement information safeguards to control the risks you identify through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.

Evaluation and adjustment. Your school must evaluate and adjust its information security program in light of the results of the required testing and

administrative, technical, and physical safeguards that are appropriate to the size and complexity of the school, the nature and scope of its activities, and the sensitivity of any customer information at issue.

The safeguards shall be reasonably designed to achieve the following objectives:

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

Required elements of an information security program

Designated coordinators. Your school must designate an employee or employees to coordinate its information security program.

monitoring, as well as for any material changes to your operations or business arrangements or any other circumstances that it has reason to know may have a material impact on your school's information security program.

Overseeing service providers. A service provider is any person or entity that receives, maintains, processes, or otherwise is permitted access to customer information by providing services directly to your school. Your school must take reasonable steps to have service providers that are capable of maintaining appropriate safeguards for customer information, and you must require your service providers by contract to implement and maintain such safeguards.

FTC regulations: 16 CFR 313.3(n)) and 16 CFR 314).1–5 Gramm-Leach-Bliley Act: Sections 501 and 505(b)(2) U.S. Code: 15 USC 6801(b), 6805(b)(2)

[1] Personally identifiable financial information; and any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personally identifiable financial information that is not publicly available.

[2] The administrative, technical, or physical safeguards you use to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle customer information.

Preventing Copyright Violations

A school must implement written plans to effectively combat the unauthorized distribution of copyrighted material by users of the school's network without unduly interfering with educational and research use of the network.

Copyright requirements

34 CFR 668.14(b)(30)

These plans must include the use of one or more technology-based deterrents and procedures for handling unauthorized distribution of copyrighted material (including disciplinary procedures). Technology- based deterrents include bandwidth shaping, traffic monitoring, accepting and responding to Digital Millennium Copyright Act (DMCA) notices, and commercial products designed to reduce or block illegal file sharing. See GEN-10-08. No particular technology measures are favored or required for inclusion in the school's plans, and each school has the authority to determine its own plans, including those that prohibit content monitoring.

The school's plans must also include measures to educate its community about appropriate versus inappropriate use of copyrighted material, including the information described under the student consumer information rules in *Chapter 6*. These mechanisms may include any additional information and approaches that the school determines will contribute to the effectiveness of the plans. For instance, the school might include pertinent information in student handbooks, honor codes, and codes of conduct in addition to email and/or paper disclosures.

The school must have a written plan for the periodic review of the effectiveness of these measures, using relevant assessment criteria.

The school must, in consultation with its chief technology officer (or other designated officer), periodically review the legal alternatives for downloading or otherwise acquiring copyrighted material (and disseminate the results, as described in *Chapter 6*) and offer legal alternatives for downloading or otherwise acquiring copyrighted material (to the extent practicable and as determined by the school).

The Department anticipates that individual institutions, national associations, and commercial entities will develop and maintain up-to-date lists that may be referenced for compliance with this provision.