FERPA SECURITY CHECKLIST

FOR EDUCATION

A ready reference for compliance with the Family Educational Rights and Privacy Act*

ENJOY SAFER TECHNOLOGY™

Under the federal FERPA law, educational institutions have the responsibility to protect the privacy of student records. The law applies to institutions that receive funds from the U.S. Department of Education under any program that the department administers. Virtually all public schools and school districts, most private and public postsecondary institutions, and professional postsecondary schools such as medical schools are required to comply. Private elementary and secondary schools are generally not required to comply because they typically do not receive federal funding.

As part of compliance with FERPA, ensure that these policies, practices, and procedures are in place at your institution.

1. Annual Notification

Annually notify eligible students, or their parents for those under the age of 18, of their rights under FERPA. The notice shall include the following, including procedures for exercising rights where applicable:

- Right to inspect and review the student's education records
- Right to seek amendment of education records
- Right to consent to disclosures of personally identifiable information
- Right to file a complaint concerning alleged failures to comply
- Criteria for defining legitimate educational interests, determining who qualifies as a school official, and notice regarding directory information if applicable (explained below)
- Notice by a means that is reasonably likely to inform parents or students, including those who are disabled and parents who are non-English speaking
- Notice of your policy to routinely forward student records to other educational institutions that a student attends or is seeking to attend, if you have such a policy

2. Right of Inspection and Review

- Comply with requests for access to records within 45 days
- Respond to reasonable requests for explanations and interpretations of student records, and understand the limitations on the right to review and inspect under CFR 99.12
- If circumstances prevent the parent or student from inspecting and reviewing the records, either provide a copy or a suitable alternative arrangement
- If records contain information on more than one student, redact the other student information before disclosing
- Do not destroy any records if there is an outstanding request to inspect and review them

3. Fees

Do not charge a fee to search for a student's education records or to retrieve them. You may charge a fee for providing a copy of the records, but not if the fee effectively prevents a parent or student from exercising his or her right to inspect and review the records.

4. Right to Amend Records

If a parent or student requests that the education record be amended, respond within a reasonable time and if the decision is to not amend the record, inform the requestor of the decision and the right to a hearing.

FERPA SECURITY CHECKLIST
FOR EDUCATION

5. Right to Hearing

- Provide an opportunity for a hearing allowing the parent or student to challenge the content of the student's record on the grounds that it is inaccurate, is misleading, or violates privacy
- Hold the hearing within a reasonable period of time, and give notice of the date, time, and place reasonably in advance
- Ensure the hearing is conducted by an individual who does not have a direct interest in the outcome
- Allow representation by individuals other than the parent or student, including an attorney retained at parent's or student's expense
- Provide a full and fair opportunity to present evidence relevant to whether the information contained in the records is inaccurate, is misleading, or violates student privacy
- Render a decision in writing within a reasonable period of time, based solely on the evidence presented at the hearing, and include a summary of the evidence and the grounds for the decision.
- If the finding is in the party's favor, amend the record as appropriate and inform the parent or student in writing of the amendment
- If not in the party's favor, inform the parent or student of his or her right to place a statement in the record commenting on the contested information, or expressing disagreement with the decision; preserve the statement for as long as the record is maintained and disclose the statement whenever the related record is disclosed

6. Prior Consent

Before disclosing personally identifiable information (PII) from student records, obtain written, signed consent that specifies the purpose of the disclosure, records involved, and parties to whom they will be disclosed. Provide a copy of the disclosed records if the parent or student requests.

Written consent is not required for directory information (described below) or disclosure to teachers and school officials within the institution for legitimate educational interests. Other situations not requiring prior consent are described in 34 CFR 99.31.

7. Recordkeeping

- Maintain a record of each request for access and disclosure of PII from parties other than: the parent, the student, or a representative of the parent or student with written authorization; a school official with legitimate educational interest; a request for directory information; or a directive by a court order
- Record the parties who requested or received the PII and their legitimate interests in requesting or obtaining it, and maintain that record for as long as the records are maintained
- If the disclosure is with the understanding that the party may in turn disclose the PII for permissible purposes, record the names of the additional parties to which the information may be disclosed and their legitimate interests in obtaining it

Regulatory Compliance for Educational Institutions

*The following are the major regulations that apply to educational institutions, and measures that are either required or recommended as part of a compliance effort.**

FERPA—Family Educational Rights and Privacy Act

The FERPA law was enacted in 1974, before ubiquitous Internet connectivity opened the door to online intrusions and cyber-theft. However, it does include provisions for access control and authentication, specifically of school officials.

The following are recommended for any educational institution concerned with protecting student records:

- Firewall and endpoint protection on servers that store student records
- Two-factor authentication to protect against compromised passwords
- Antivirus, anti-phishing, and web filtering on computers used by school officials who have access to student records
- Encryption of any student information that is sent over the Internet, or stored on laptops or removable media

CIPA—Children's Internet Protection Act

CIPA requires that schools implement an Internet safety policy, and applies to K-12 schools and libraries that receive discounted Internet access through the federal E-rate Program.

The following are either required by CIPA or play key roles in implementing an appropriate safety policy:

- Web filtering on all computers used by students, to block obscene or other content harmful to minors
- Antivirus, antispam, and anti-phishing to protect students using email
- All of the measures for protecting student records listed under the FERPA law

FERPA SECURITY CHECKLIST
FOR EDUCATION

8. Redisclosure

- When you disclose PII to another party, disclose it on the condition that the other party will not further disclose the information without prior consent of the parent or student, unless the disclosure does not require prior consent or you have recorded the name of the third party and his or her legitimate interests
- If you receive student PII from another institution, use the information only for the purposes for which the disclosure was made
- Do not disclose information to a party that has been determined by the U.S. Department of Education to have improperly redisclosed PII

9. Disclosure to Other Educational Agencies or Institutions

- If you disclose PII to officials of another school, school system, or institution of postsecondary education that the student attends or seeks to attend, notify the parent or eligible student at his or her last known address, unless the parent or student initiated the disclosure or your annual notification includes a notice that your policy is to forward such information
- If the parent or student requests it, provide a copy of the record that was disclosed and an opportunity for a hearing to challenge its content

10. Directory Information

Directory information is information "that would not generally be considered harmful or an invasion of privacy if disclosed" and is defined in CFR 99.3. If your institution discloses such information, give public notice that includes the types of information designated as directory information, informs parents and students of their right to refuse to allow their information to be treated as directory information, and the time period during which the party must respond in writing to opt out of having that information treated as directory information.

For more information on ESET Industry Solutions for education, please visit

www.eset.com/us/business/education-security/

ENJOY SAFER TECHNOLOGY™

*This document is intended as a general guideline, and does not replace or supersede the provisions of FERPA, CIPA, HIPAA, or PCI-DSS, or guidance provided by legal or official sources.

www.eset.com

Regulatory Compliance for Educational Institutions (cont.)

HIPAA—Health Insurance Portability and Accountability Act

Schools that supply health services or handle electronic protected health information (ePHI) might be subject to HIPAA rules, which aim to ensure the confidentiality, integrity, and security of ePHI. Whether these records are covered by FERPA, HIPAA, or both is a complex question; see Joint Guidance on the Application of FERPA and HIPAA to Student Health Records.

The following are recommended as part of a HIPAA compliance initiative:

- Encryption of ePHI on portable drives, laptops, mobile devices, or transmitted via email or other Internet methods
- Firewall and endpoint protection on all servers that hold ePHI
- Strong passwords or multifactor authentication
- Antivirus, anti-phishing, and web filtering on all computers and mobile devices

PCI-DSS—The Payment Card Industry Data Security Standard

Schools that accept payment cards are subject to the PCI-DSS standards, which are designed and enforced by the card brands to guard against theft of cardholder data.

The following are part of a PCI compliance initiative:

- Firewall configured to protect cardholder data
- Encryption to protect cardholder data sent across public networks
- Antivirus software installed, enabled, and regularly updated
- Strong access control measures such as multifactor authentication