
NYSFAAA

Protecting Student Privacy in Virtual and Remote Work Environments

LaSonya Griggs
Associate Dean of Enrollment Management
Tompkins Cortland Community College

Agenda

- Review FERPA requirements for colleges and universities
- Provide ED responses to common questions about FERPA during COVID-19
- Provide privacy and security best practices
- Provide resources for review and use

Family Educational Rights and Privacy Act (FERPA)

- FERPA Regulations: 34 CFR Part 99
- FERPA protects the privacy of student education records
- Postsecondary institutions must have a student's permission to disclose personally identifiable information (PII) from student education records unless a FERPA exception applies

FERPA Exceptions

It is lawful for FERPA protected information to be shared with:

- School officials with legitimate educational interest
- Other schools to which a student is transferring
- Specified officials for audit or evaluation purposes
- Appropriate parties in connection with financial aid to a student
- Accrediting agencies
- To comply with a judicial order or lawfully issued subpoena
- Appropriate officials in cases of health and safety emergencies

https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html?

Remote Work Environments

Scenario #1

- I am a college professor and need information about my students on hand while I switch to virtual instruction. Can I take home with me PII from my students' education records?

Scenario #1 - Response

- Yes – FERPA does not prohibit faculty from taking PII from student's education records home with them as long as the faculty has a legitimate educational interest in the education records, as determined by their institution.
- School officials who take education records home are prohibited from further disclosing the PII from the education records, except as otherwise permitted under FERPA; and should use reasonable methods to protect the education records, and the PII in those records, from further disclosure
- These protections can include access controls that are physical, technological, and administrative controls

Scenario #1: Questions to Consider

- What education records, or PII from education records, will school officials be "taking home"?
- How will those education records or PII be brought home?
- How will the school official secure the PII in those education records while the records are at home?

Scenario #1 - Best Practices

- Look at what your institution already uses for work from home solutions
- Access student records using vpn or your institution’s cloud service
- Use computer equipment issued by your institution
- Use software vetted and authorized by your institution

Scenario #2

- I’m working from home. I would like to have a conference with an eligible student. My spouse is also at home and in the same room. Is it alright if I conduct the conference?

Scenario #2 - Response

- Yes, as long as the employee
  - Does not disclose PII from the student's education record in hearing of his or her spouse during the conversation; or
  - Moves away from his or her spouse to discuss PII from the student's education records so that the spouse does not overhear your discussion; or
  - Obtains prior consent in writing (electronic) from the eligible student for the potential disclosure of PII from the student's education records to his or her spouse.

Scenario #2
Questions to Consider

- How will this "conference" occur (phone call, video call, etc.)?
- What is the subject of the conference?
  - Some subject matter is general in nature and does not involve PII from a student's education record
- What precautions can you put in place to make sure the spouse does not overhear the conversation?

Scenario #2 – Best Practices

- Schedule/arrange time for connecting with students when family are not occupying remote work space
- Wear a headset with a microphone so the student portion of the conversation is not overhead
- Don’t repeat PII if it is given to you by a student during a conversation

Virtual Environments

Scenario #3

- Our school is planning to use video conferencing or other virtual software apps to conduct business with students virtually. Can an institution use such apps under FERPA?

Scenario #3 - Response

- It depends.
- For instructional purposes, yes, as long as the education record is used for authorized purposes and does not disclose education records or PII to unauthorized parties
- For operational purposes, no. Virtual software used to enhance work from home operations or virtual offices do not have an authorized need for education records or PII.

Scenario #3
Questions to Consider

- Does your educational agency or institution currently allow this type of software?
- What is your agency or institution's process to review requests for software?
- Refer to ED resources such as:
  - FERPA and Virtual Learning Related Resources handout
  - Protecting Student Privacy While Using Online Educational Services
  - Read the platform's Terms of Service

Scenario #3

- Does FERPA address which apps can be used?

Scenario #3 - Response

- No, FERPA is a federal privacy rule and does not include explicit information security standards
- FERPA does not address the use of specific apps
- Under FERPA, educational agencies and institutions may disclose, without consent, education records, or PII contained in those records, to the providers of online learning software apps under the “school official” exception provided they meet the conditions of that exception
- Schools should work with their information security officers to review information security requirements and terms of service

Video Conferencing 10 Privacy Tips

Identify Meeting Participants

- Password protect a meeting
- Provide unique meeting ID numbers
- Create new passwords or ID numbers for recurring meetings

Tools to Limit Access to Meetings

- Lock the meeting once expected participants have arrived to prevent others from joining
- Enable settings allowing hosts to approve participants trying to join a meeting
- Some software apps allow the ability to remove participants from the meeting should the need arise

Video and Microphone Settings

- Participants may be able to see and hear you as soon as you join a meeting
- Most services allow you to mute yourself or turn off your camera
- You may be able to store default video and microphone settings
- You may be able to adjust default settings at the beginning of each video conference

Recording a Video Conference

- Many apps allow the host to record the meeting for future reference
- Participants can usually see some type of indicator that a meeting is being recorded, a bright red circle or the word “recording”. Can be recorded without these.
- Recognize that a video recording may be shared online without a participant’s knowledge
- Safest strategy is to assume you may be recorded and avoid sharing PII information during a video conference

Sharing Your Screen

- Most services allow participants to share their screen
- When screen sharing, don’t have other documents open, browser windows or other things on your screen that should not be shared
- Services may have the option to allow the host to disable screen sharing
- Services may allow screen sharing to be limited to the host

Don’t Open Unexpected Invites

- Malicious intent exists. Users can be armed.
- Inform participants of planned video conferences
- Inform participants of date/time of video conference
- Download video conference app directly from the service’s website or the platform’s app store

Confidentiality & Conferencing

- Conferencing service cannot guarantee security of your information
- Enterprise service versus free services
- Enterprise service may provide greater security

Review Service's Privacy Policy

- What information does the service collect about you?
- Does the privacy policy limit the company from using your information for purposes other than providing their conferencing service?
- Does the conferencing service share your information with advertisers or other third parties?

Update Conferencing Software

- As security issues arise, many video conferencing companies are updating their software with patches and fixes.
- Always have the latest version of conferencing software
- Only accept software updates directly from the service’s website

Set Conferencing Preferences

- Establish preferred video conferencing settings
- Share preferred default settings with staff
- Establish company-wide video conferencing dos and don’ts
- Emphasize the need to select more secure options when hosting or joining video conferences

Privacy & Security
5 Things to Consider

Current Solution

- Look at what your institution already uses
- Review your current solutions first
- Many education platforms include features that can be leveraged to support distance learning

Identify Options

- When identifying and choosing technology tools, work with your information security specialists to vet prospective solutions against FERPA requirements using a risk-based analysis

Things to Look for

- Products that apply best practices
  - Encryption
  - Strong identity
  - Authentication
- Statement and terms of service that explain how the vendor's use of PII from student education records complies with FERPA

Communication

- Be transparent with parents, students, and the school community

Ask For Help

- Consult and ask questions
  - Information security specialists
  - Peers
  - U.S. Department of Education

Resources

- FERPA & Virtual Learning During COVID-19 webinar recording (March 30, 2020)

https://studentprivacy.ed.gov/training/ferpa-and-virtual-learning-during-covid-19-webinar-recording

- Video conferencing: 10 privacy tips for your business

https://www.ftc.gov/news-events/blogs/business-blog/2020/04/video-conferencing-10-privacy-tips-your-business

- FERPA and Virtual Learning Related Resources (handout)

https://studentprivacy.ed.gov/resources/ferpa-and-virtual-learning

- Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices

https://studentprivacy.ed.gov/resources/protecting-student-privacy-while-using-online-educational-services-requirements-and-best

- United States Department of Education

https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html?

LaSonya Griggs
lag@tompkinscortland.edu

Questions