Student Privacy and Special Education: An Educator's Guide During and After COVID-19

COVID-19 has disrupted education and has forced schools to pivot quickly to a distance learning approach, which is often virtual. Using virtual learning products comes with concerns about student privacy, including for students receiving special education and related services. Federal privacy laws don't explicitly address how to handle every situation, but concerns about privacy should not be a barrier to serving students as best as educators are able. This guide is designed to provide an overview of major relevant privacy laws and to help educators think through common scenarios that might present privacy concerns, particularly for students with disabilities.

Which laws address privacy concerns in special education?

Family Educational Rights and Privacy Act (FERPA)

FERPA is a federal law that protects student education records held by an education agency, such as a school or district. It applies to any school or district that receives federal funding. FERPA limits which parties education agencies can share students' education records with without parental consent. It also provides parents with the right to review and amend their student's education record.

The law defines[1] "**education record**" as any record that is "directly related" to a student and is "maintained by an educational

The Individuals with Disabilities Education Act (IDEA) contains provisions that are aligned to FERPA's privacy requirements:

To receive federal funding under IDEA, states must have systems in place to protect the confidentiality of personally identifiable information and must maintain the right of parents to consent to the exchange of that information. IDEA also provides the right of parents to examine records relating to their student's assessment, eligibility determination, and individualized plan.[2]

1 Family Educational Rights and Privacy Act. 20 U.S.C. § 1232g. (1974). https://studentprivacy.ed.gov/node/548/

agency or institution," or any party acting on their behalf, such as an ed tech platform. A student's education record generally includes information such as grades, disciplinary records, and services provided through an Individualized Education Program (IEP) or a 504 plan, among other things. FERPA also protects students' **personally identifiable information** (PII), which is *any* information that directly or indirectly identifies a student or any information that would allow a reasonable person in the school community to identify the student with reasonable certainty. This might include, for example, their name, address, date of birth, or an identification number.

However, FERPA does allow "directory information" about a student to be shared without parental consent. Directory information may include a student's name, grade level, and phone number—the kind of information "that would not generally be considered harmful or an invasion of privacy if disclosed."[3] How a school or district defines what information they consider to be "directory information" is at their discretion, with the understanding that a Social Security number may never be designated as directory information. If a school chooses to adopt a directory information policy (and they are not required to under FERPA), parents must be given an opportunity to opt out of sharing directory information, usually through a form signed at the beginning of the school year.

How FERPA applies to distance learning: FERPA applies to education records, such as written records or video recordings. Therefore, a student's mere participation in virtual learning or sharing a student's name or image in a way that is visible on digital learning platforms generally does not implicate FERPA. Generally, the type of information about a student that is shared among classmates and educators in a virtual learning setting is not personally identifiable information.

However, where a student's image, name, or voice is recorded and stored by the school, it may become part of the education record and would then be protected by FERPA. Learn more about this in the Q&A below.

2 IDEA includes robust provisions calling for parent participation in special education, specifically allowing for the use of video and conference calls in IEP meetings. In particular, 34 CFR § 300.322(a) of IDEA calls for public agencies to "take steps to ensure that one or both of the parents of a child with a disability are present at each IEP Team meeting or are afforded the opportunity to participate." Additionally, 34 CFR § 300.328 of IDEA anticipates that parent participation may not always be possible in person and allows for parents and public agencies to "agree to use alternative means of meeting participation, such as videoconferences and conference calls."

3 20 U.S.C. 1232g(a)(5)(A)

Children's Online Privacy Protection Act (COPPA)

COPPA is a federal law that governs the information that companies can collect on children under age 13. The law applies to websites, games, and applications that are targeted to children under 13 and to situations where companies have "actual knowledge" that a user of their product is under 13. COPPA requires companies to have a privacy policy, inform parents of any data collection, and obtain parental consent to collect personally identifiable information on children.

How COPPA applies to distance learning: If schools use websites, applications, or other products with students for educational purposes, teachers or school leaders can provide consent on behalf of parents. In these situations, companies can only collect student data that is used for an "educational purpose."

Health Insurance Portability and Accountability Act (HIPAA)

HIPAA is a federal law that governs patient health privacy and sharing of electronic health records. HIPAA is not as widely applicable to education contexts as FERPA. While HIPAA typically applies to health care providers such as physicians, clinical social workers, or mental health practitioners, the governing law depends on whether the school engages in a HIPAA-covered transaction and how the records are maintained. If the health care provider practices in the school and the services provided are administered and operated through the school, the health records are considered "education records" and FERPA applies. On the other hand, HIPAA applies when the records are maintained by an outside provider and are transmitted electronically for billing purposes. However, the Department of Health and Human Services and the Department of Education clarified that if a school-employed health care provider engages in a HIPAA-covered transaction, such as billing for services through Medicaid, but the services provided are under the IDEA, the accompanying health records are located in the student's education record—subjecting the student's health information to FERPA protections, rather than HIPAA.[4]

How HIPAA applies to distance learning: HIPAA is not the prevailing law on student records in most cases where a provider is offering services based on a student's IEP and the school agency is the record holder. There may be some exceptions related to Medicaid, but FERPA is most often the law that schools and providers within schools must follow. See more about this topic in the Q&A below.

4 HIPAA excludes FERPA-protected education records. For more information, see https://studentprivacy.ed.gov/resources/joint-guidance-application-ferpa-and-hipaa-student-health-records https://www2.ed.gov/policy/gen/guid/fpco/doc/ferpa-hippa-guidance.pdf

State Laws

In addition to existing federal laws, many states have passed their own laws that further address data privacy in education and that might pose additional restrictions on schools. The Future of Privacy Forum finds that state laws often take one of three common approaches to student privacy:

1. Some laws regulate state and/or local education agencies.
2. Some regulate education technology vendors.
3. Some regulate a combination of education agencies and education technology vendors.

To be fully informed about laws that apply to your school, look into whether your state has laws on student data privacy and whether they impose additional requirements on how student data is protected or used.[5]

Professional Standards

Educators who provide therapy services, such as speech-language pathology, may have codes of conduct or best practices for teletherapy that are recommended by their professional associations or licensing authorities.

5 You can start by visiting https://studentprivacycompass.org/state-laws/

FAQs: Student Data Privacy and Virtual Learning

The COVID-19 pandemic has necessitated a rush to virtual learning, and many educators and parents are unsure about how to provide accessible virtual learning opportunities while protecting student privacy. Student privacy laws like FERPA were not written to take virtual learning into account, leaving some gray areas in how to apply the law to current circumstances. However, the federal government has previously released guidance that is helpful in answering some common questions on this topic.

Q. Is it against privacy laws to use videoconferencing with students?

A. Using digital platforms to have live virtual classes through videoconferencing does not violate student privacy laws. However, to protect the privacy of students and their families, educators should be mindful of how they use videoconferencing platforms. During virtual learning, it's important to note that a student's education record can include photos and videos of a student that are recorded and stored by the school.

Some best practices:

- Set meeting preferences so attendees do not automatically share their video when joining the call.
- Do not require students to have their video turned on during classes.
- Let parents know about live virtual classes ahead of time so they can decide whether they want their student to join by video.
- When recording a lesson that will include students' names or videos, take precautions when storing or sharing the video. Ensure that it remains protected and accessible only to those who are allowed access to students' records under FERPA.

Q. How do I know if the video platform or software my school uses is compliant with privacy laws?

A. As schools and districts made quick transitions to virtual learning, many educators and school leaders did not have the capacity to fully coordinate or vet all aspects of videoconferencing platforms. While educators should primarily focus on providing the best education possible to students, privacy concerns should also be a consideration—particularly when planning ahead for virtual learning options in the new school year.

Many videoconferencing platforms are not designed to be used by schools for virtual classes. If you're unsure about the platform your school is using, look at the language the company uses to describe the platform and its privacy policy to determine whether it is intended to be used in an educational context. Companies that designed platforms for an educational context are more likely to be aware of FERPA and COPPA requirements, and other applicable education laws. Platforms that are not intended for schools do not inherently violate privacy laws, but they may require educators to be more careful about their use and more cautious about how they share information.

Q. Can parents/family members be present during live virtual classes?

A. FERPA does not prohibit parents from observing their students' classroom, including students with disabilities. However, your **state** may have additional laws that apply here. Your school may also have a policy on classroom visitors that can be adapted to online learning. If your school allows classroom visitors, there may not be any additional restrictions on observations of virtual instruction.

Student privacy is a priority, but concerns about privacy should be carefully balanced with the need to provide education to all students in accessible and equitable ways. Requiring a student to not have family members present during live virtual learning sessions raises equity issues for students who may be sharing space with other members of their household or who may need a parent or caregiver present to help them access the content.

Q. Can live virtual classes be recorded for students to watch at a later time?

A. Educators may want to record virtual lessons for students who are not able to participate during a specified time period. While likely intended to increase equity or accessibility, this raises questions about student privacy.

Any image or video that is directly related to a student and kept by the educational agency is considered part of a student's education record and is subject to FERPA. "Directly related" generally means that a student is or becomes the focus of a video or if content of the video includes personally identifiable information (PII) in the student's education record. A single image or recording can be directly related to multiple students at once.

Consider the following questions before recording a virtual class:

- What is the purpose of recording a live lesson? Is it solely for educational purposes? Can another option be used to achieve the same goal (e.g., teachers record themselves without students present)?
- Who will the recording be shared with? Is it meant to be shared with others? Is that information shared with students who are being recorded and with students receiving the recording?
- Where will the recording be stored? How will the recording be transferred to storage? Are the transfer and storage platforms secure enough for protected student data?

Q. Can teletherapy or one-on-one services be provided on live video platforms?

A. In most cases, where health professionals are providing services on behalf of schools for students with disabilities, FERPA applies. As such, simply using a video platform to provide the service does not raise significant privacy concerns, so long as the platform used is adopted by the school contractually and the session is not recorded or shared.

However, recognizing that some providers were concerned about compliance with HIPAA requirements during the rapid transition to telehealth due to the COVID-19 pandemic, the Department of Health and Human Services (HHS) **announced** that it would allow more flexibility for providers. The department will not penalize providers for using "non-public facing" communication platforms that are not HIPAA-compliant, such as Zoom, Facebook Messenger video chat, and FaceTime. HHS also recommends that providers using communication methods that are not HIPAA-compliant warn patients of data privacy risks. Any "public facing" communications such as Facebook Live and TikTok should still be avoided.

In addition, some schools or districts have policies restricting one-on-one live video sessions between a student and an educator, not just because of privacy concerns but in an effort to ensure student safety. If your student needs one-on-one instruction or other services, make sure you're informed of your school or district's policy on this. You may want to explore the following questions:

- Is this type of interaction allowed?
- If so, are there restrictions or is parent permission needed? What record-keeping may be necessary?

Looking Ahead: School Reopening Plans and Student Privacy

Schools and districts are beginning to create plans for reopening schools in the fall while also working to mitigate health risks for students and staff. This is an extraordinarily difficult balance to strike, and some organizations and government agencies are recommending measures such as student temperature checks, symptom screening, and assigning risk levels to students based on their health and other factors. Each of these measures is intended to protect the health of students, families, and staff, but they also involve a significant amount of sensitive data collection. This raises critical questions about how schools will collect, use, and store student health data. As such, schools and districts must consider:

- For what purpose is the data being collected?
- How will the data be used?
- Where will the data be stored and for how long?
- Who will have access to the data?

In addition, students with disabilities and students with special health care needs who may be particularly vulnerable to the coronavirus may be at risk of discrimination based on their health or disability status. Data about health or disability status must never be used to track students in any way or to limit their educational access or the types of opportunities available to them. School leaders, educators, and families should be cognizant of these risks and commit to ensuring that their reopening plans protect students' data and students' educational rights in the coming year.

For more information, visit www.ncld.org or contact NCLD via email: policy@ncld.org.
P.O. Box 34056, Washington, DC 20043