PRIVACY & EQUITY IN THE NEW SCHOOL YEAR

Steps for In-Person, Remote, or Hybrid Learning

JULY 2020

CENTER FOR DEMOCRACY & TECHNOLOGY

A SERIES OF PAPERS ON STUDENT PRIVACY

Privacy and Equity in the New School Year:
Steps for In-Person, Remote, or Hybrid Learning

Executive Summary **2**

Introduction **3**

Overview of Planned Approaches to Schools Reopening and Role of Tech, Data, and Privacy **5**

Emerging In-Person Privacy Practices **7**

I. Risks in Data Collection and Sharing 8

II. Mitigating Risks 9

Community Engagement and Transparency 9

Complying with FERPA 10

Collection Obligations *11*

Sharing Restrictions *11*

Data Governance Best Practices 14

Emerging Technology-Based Privacy Practices **16**

I. Risks Imposed by Remote Learning Technology 16

II. Mitigating Risks by Remediating New Technology 17

Conclusion **19**

Additional Resources **20**

Appendix: Additional Exceptions to Parental Consent **22**

Endnotes **24**

This report was authored by:

Hannah Quay-de la Vallee, *Senior Technologist*
Cody Venzke, *Policy Counsel, Student Privacy*

Cover and layout designed by Tim Hoagland

Executive Summary

As local and state governments, businesses, and institutions across the country implement the first phases of reopening after weeks of lockdown, schools are beginning to plan for learning this fall. Many of those plans are still in development, but schools are considering options on a spectrum that may be divided into three groups: returning entirely to in-person learning, remaining entirely online through remote learning, or some mixture of the two, known as "hybrid learning." Hybrid learning models may involve assigning students to in-person or remote learning based on individual or familial risk factors, rotating students through remote learning, or staggering arrival and dismissal times.

Each of those models is likely to involve collecting and sharing student health information and remediating privacy gaps in remote educational technology (edtech). This guidance offers options for schools to protect student privacy as they implement those models. Student privacy is rooted in the principle that students and families should control their own information, and that principle is even more important during disruptions such as a global pandemic. Massive shifts to new learning tools entail massive shifts in transmitting and storing student information, increasing the risk that information about a student's academics, health, or family may be disclosed to the wrong individuals. The options below will help preserve students' and families' right to control their information.

First, schools conducting in-person learning, including hybrid learning, will likely have to collect and share student health information to prevent and monitor outbreaks, facilitate contact tracing, and to provide new services such as counseling or meal services. In collecting and sharing student health information, schools should take three steps to protect student privacy:

- **Engage the community.** Prior to collecting or sharing student health information, schools should ensure that students, families, and the community are informed about the goals of the data collection, the type of data being collected, the uses of the data, and how the information is being protected.
- **Comply with the Family Educational Rights and Privacy Act (FERPA).**
  - Health information collected and maintained by schools is likely covered by FERPA, not the Health Insurance Portability and Accountability Act (HIPAA). Consequently, schools should honor parent requests under FERPA to inspect records with student health information and consider requests to amend that information.
  - In sharing information with health agencies or other entities, schools will likely have to comply with FERPA's health and safety emergency exception. That exception may

    permit information sharing if school officials determine, based on an outbreak of COVID-19 within the school district, a health emergency or threat is “imminent.” Alternatively, schools may avoid FERPA’s restrictions on sharing information by permitting health agencies or other partner entities such as an independent, on-site health clinic to collect and maintain the information directly.
    - Schools and districts should also consider other state and federal laws that may impact their data collection and sharing, but this brief will focus on FERPA.
- **Implement data governance best practices.** Schools should ensure they have written policies and practices regarding the collection of student health data. Those policies should specify who has decision-making authority, the goals for the collection, limitations on access and use, plans for retaining and deleting the information, and the requirements for data sharing agreements with other entities.

Second, schools that adopted new technology to continue learning during the pandemic should “remediate” their technological landscape. By “remediate,” we mean ensuring that edtech adopted during the rapid transition to remote learning complies with legal requirements and best practices for student privacy. That remediation will require three steps:

- **Inventory remote learning edtech.** In order to understand the edtech used by teachers and the student information it holds, schools should first survey teachers to inventory that technology. That inventorying process should be open and not punitive to ensure complete disclosure by teachers of the technology they used during remote learning.
- **Incorporate new edtech into the school’s existing systems.** Edtech that the school or school district wishes to retain should be incorporated into the learning environment by ensuring compliance with federal and state student privacy laws and interoperability with existing edtech, including systems for storing and evaluating student work.
- **Decommission other edtech.** Edtech the school or school district does not wish to maintain should be decommissioned by extracting information such as grades, attendance records, or student work from the technology and loading it into existing systems. Schools should then ensure that the data is deleted from decommissioned edtech systems, which may involve more than simply deleting user accounts.

Introduction

Privacy is the idea that individuals have the right to control their own information and that the entities collecting and using that information must do so in ways that respect individual autonomy. In the case of education, that right belongs to students and their families. Elementary and secondary schools have legal and ethical obligations to protect students’ privacy. Those obligations help protect students' and families' autonomy, safety, and well-being, especially for groups that have not received equitable access to social resources, including technology and education. For example, privacy requirements help protect students' and families' immigration status[1] or sensitive information about the learning needs of students with disabilities.[2] Privacy requirements also limit the ability of education technology companies to collect information about the students they serve.[3]

Those obligations have become even more important in light of the ongoing pandemic. The positive aspects of technology have enabled schools, families, and students to remain connected. To help ensure that learning continued even as schools closed, teachers turned to streaming media, social media, text messages, telephone conferences, and broadcast television.[4] School districts have in turn used edtech to collect data on student attendance, and have deployed dedicated teams to contact families of students who have not engaged with distance learning.[5] Some commentators have proposed using artificial intelligence to help track student progress and to coordinate scheduling and student placement when schools reopen.[6]

The pandemic has also exacerbated the challenge of maintaining student privacy posed by using technology in education. Some educators expressed concern about keeping student information private on online video platforms,[7] while some teachers and students experienced intrusions into their online classrooms by strangers displaying racist tattoos or child sexual abuse material, a practice that became known as "zoombombing."[8] Many of those challenges, especially to student privacy, have fallen on historically marginalized groups, sometimes due to reasons as mundane as the coding of fields in electronic records. Students in North Carolina, for example, petitioned the state superintendent to protect students from having their transgender status revealed to classmates because their online learning platform automatically populated fields with the students' legal names—ones the students no longer identified with.[9] Remote learning similarly raised concerns about the privacy of information regarding students with disabilities, as school counselors and psychologists worked to maintain confidentiality in remote learning environments.[10]

Consequently, schools now in the process of reopening face a number of challenges in using technology in the classroom, in remote learning, and in protecting students' health information. This paper walks elementary and secondary school leaders through key considerations in confronting two new challenges created by schools reopening: (1) maintaining student privacy while collecting and sharing student health information during in-person learning and (2) properly evaluating or "remediating" edtech for either continued remote learning or a transition to in-person or hybrid learning models.

Overview of Planned Approaches to Schools Reopening and Role of Tech, Data, and Privacy

School reopening plans are still coming into focus, but there are a few approaches that are emerging.

The avenues available to schools are in-person learning with social distancing measures, staying fully virtual for the new school year, or some hybrid of in-person and distance learning. Each of these approaches has advantages and drawbacks, and all of them will require substantial planning and adjustment on the part of schools, districts, teachers, and families.

Socially distanced in-person learning: In-person learning in the COVID context will look quite different from what schools were doing before the pandemic. The variety of activities that take place during the school day means that numerous interventions would be required to make in-person schooling sufficiently safe, and a number of factors will have to be considered before schools reopen, such as state and local guidance and whether schools are able to provide necessary safety resources like hand sanitizer and soap.[11] Class sizes will have to be reduced dramatically, recess games will have to be restricted to those that allow for social distancing, and mealtimes will have to be reimagined to minimize group gathering and sharing of spaces.[12] However, despite all these measures, in-person learning will still carry some risk of students and teachers contracting and spreading COVID-19. Consequently, schools are likely going to have to consider how to manage health testing, contact tracing, and responsible information sharing in the event that cases emerge among their students, staff, and faculty. Schools using in-person learning will also need to consider how to care for medically vulnerable students such as those who are immunosuppressed, or who live with vulnerable family members.

Distance learning: Continued distance learning is another approach to limit the spread of the coronavirus. While distance learning has benefits as far as slowing virus transmission, it presents substantial pedagogical challenges, as the country has seen as schools have scrambled to continue providing services to students. While there are non-technical approaches such as providing paper worksheets at pick-up points for students, many distance learning approaches rely on access to technology such as laptops or tablets and reliable internet access. Tech-based approaches may allow for a higher level of engagement between teachers and students such as phone calls, texts, or video lessons.

However, tech-based approaches also present substantial equity and privacy concerns. Schools must provide hardware like tablets, so students without devices are not left behind.

Additionally, many Americans still lack reliable internet access. Although schools are trying innovative solutions such as mobile hotspots and "wifi buses," these solutions are not always feasible. Additionally, school-owned devices and school-provided internet access must be carefully managed to avoid risks to students' privacy. Tech-based approaches may also be inaccessible for some students if they are not available in alternative languages needed by English learners, or if they do not have the accessibility features needed for students with disabilities. For guidance on maintaining student privacy and equity during remote learning, see CDT's training module, "COVID-19 and Student Privacy."[13]

Hybrid learning: As the reopening process begins, some schools and districts are also considering a hybrid of in-person and remote learning. This could mean students coming to school in "shifts" (such as morning/afternoon or alternating days) and keeping up with distance learning during their remote days, or live streaming classes so they are available to students both in-person and remotely.[14] The hybrid process has the advantage of providing in-person learning, but in a way that may make it easier to socially distance by limiting the number of students in schools at any one time. It could also reduce network access concerns by allowing students to download pedagogical materials like worksheets and video lessons while they are in school to use at home later, even if they do not have reliable internet at home. Of course, these advantages are also accompanied by risks and challenges. Schools must still handle many of the challenges of distance learning, such as equitable device access, as well as in-person challenges such as contact tracing and caring for medically vulnerable populations.

COVID-19 and Student Privacy Training

New educational technologies, tools, and workflows fill an essential role in allowing schools to continue to serve their student populations amidst COVID-19. However, they also raise a novel set of privacy issues that warrant careful attention from state and local practitioners. CDT created an online interactive training module[15] designed to equip state and local education practitioners to better incorporate student privacy protections into their COVID-19 response.

Within this training, CDT recommends six perennial steps that education policymakers and practitioners should take to protect privacy during this global pandemic:

1. Utilize existing data and technology governance structures and staff.
2. Provide educators with privacy training and communications.
3. Ensure appropriate agreements are in place before using new tools and products.

4. Secure video conferencing tools.
5. Create a legal and technical data deletion plan.
6. Consider equity throughout the use of data, technology, and privacy.

In addition to these steps, the training module “COVID-19 and Student Privacy” covers legal requirements surrounding student privacy and data protection, and provides further resources on addressing student privacy issues in the context of COVID-19. It can be completed in about 20 minutes and includes narrated slides, a comprehension quiz, and downloadable resources.

Emerging In-Person Privacy Practices

In order to prevent and mitigate the spread of COVID-19, school reopening plans are turning to approaches like collecting information to assist health agencies in contact tracing and widespread testing.[16] Others are thinking about how to make schools stronger and more equitable in the aftermath of COVID-19 by better understanding the inequities faced by students that were exacerbated by the COVID-19 crisis,[17] and how to ensure both the physical and emotional health of their students upon reopening.[18] While these are important goals, they often entail collection of sensitive data, so it is important to consider the privacy and equity concerns they raise. For instance, contact tracers interview patients who have been diagnosed with COVID-19 to build a list of everyone they had been in significant contact with during the time in which they would have been contagious.[19] Tracers then use that information to reach out to those contacts, inform them that they may have been exposed to the virus, and provide them with the tools and information they need to help limit the further spread of the disease.

Collecting data related to the well-being of students is a common duty of educational institutions,[20] and the contact tracing and testing that schools adapt in the coronavirus era may fall into this same category. Indeed, some information collected by schools would potentially be useful to contact tracers in the event that a case arises in the school. For instance, attendance data would tell contact tracers which students were in prolonged contact with the person who contracted the disease, and eventually, vaccination records may inform tracers which students are still at risk for the virus and which are immune.

In addition to collecting health information, schools may also plan to share that information with health agencies or other entities to help conduct contact tracing, treatment, and planning. For example, California’s “Stronger Together” plan for reopening schools calls on schools to “[a]ddress the school’s role in documenting, reporting, tracking, and tracing infections in coordination with public health officials."[21] The Centers for Disease Control and Prevention similarly recommends that "school administrators should notify local health officials, staff, and families immediately" of any cases of COVID-19.[22]

I. *Risks in Data Collection and Sharing*

While contact tracing, health testing, and collecting and sharing health data can help maintain the safety and well-being of the school community, the information involved is also quite sensitive, and collection of that data can present several risks to students and families:

Overcollection: While it may feel like the best thing to do is collect as much information about students' health and movements as possible in case it becomes useful later, this approach is dangerous from a privacy perspective. The more data that is collected on students, the more risk there is for that data to be accidentally exposed or misused in a way that is harmful to the student. Additionally, the risks of overcollection are not borne equitably across the student population. Transgender students[23] and students with diabilities and preexisting conditions are more at risk if their health information is disclosed or misused, as exposure of this information can lead to bullying, feelings of alienation, and discrimination. Students and families without legal residency are at greater risk if their information is shared across agencies,[24] as they risk legal action up to deportation if their information is shared with law enforcement (whether directly shared by the school, or by way of another agency).

Breaches and redisclosure: Any time data is collected, there is a risk that it could be breached or redisclosed. As noted above, the impacts of breaches can be disproportionately devastating to certain student and family populations, which could exacerbate the already inequitable impact of COVID-19.

Inadvertently revealing private information: When collecting and handling sensitive data, there is often a risk that that data will be leaked or exposed in some way. Sometimes this occurs through a data breach, but it can also happen through less obvious side channels. For instance, if all students in a class receive notification through a contact tracer that they may have been exposed to the coronavirus, and the next day one member of a class is absent or has been switched to a distance learning program, the class may assume (rightly or wrongly) that the now-absent student exposed them to coronavirus, which is an exposure of that student's health information. Or, if a school prioritizes bringing students from abusive family situations back to school sooner, or keeps students with at-risk family members out of school longer, classmates may deduce something about those students' lives that they would not have chosen to share.

Stigmatization: Connected to the concern about inadvertently revealing information is the concern that students may be stigmatized for their health status. If a student is revealed to have contracted COVID, their classmates or other parents may hold that student responsible or ostracize the student out of a sense of fear, even if they are no longer contagious. Additionally, this stigmatization may intersect with other biases such as racism or classism.[25]

Legal risk: Schools opting to collect and share data with local health agencies face some legal risk, as federal and state privacy law can be confusing and may not necessarily permit data sharing.

II. Mitigating Risks

Community Engagement and Transparency

The first step in addressing the risks posed by collecting and sharing health information is to engage the community. That engagement should involve students, families, and teachers, and should span planning, implementing, and eventually ending data collection and sharing programs.[26] It is important that community engagement be transparent, alerting families and other stakeholders to both the benefits and risks associated with the program. Although stakeholders may lack the expertise to evaluate more technical aspects of data collection programs, stakeholders should be apprised of the goals of the program, the data being collected, the uses of the data, and the community's rights under the program to opt out of the collection or review, amend, or delete collected information. Schools should also communicate who is collecting health information, how the information is being used and shared, and what security and confidentiality measures are being taken to protect children's information. Likewise, the Protection of Pupil Rights Amendment requires that parents be provided notice and an opportunity to opt out of any "nonemergency, invasive physical examination or screening" that is "required as a condition of attendance."[27] Accordingly, schools should be attentive to community buy-in, and adjust or even eliminate components of a data collection that raise concerns in the community.

It is equally important that efforts to engage stakeholders meet families where they are. The pandemic highlighted disparities in resources for families and students. Thus, schools should be attentive to providing effective engagement with parents and guardians who may work multiple jobs or evening and night shifts, speak a language other than English, have a disability, or lack access to transportation or broadband internet. For example, the Technical Assistance Center of the U.S. Department of Education (the Department or the Department of Education) recommends that schools document key aspects of programs for collecting and sharing student data and publish that documentation online.[28] School districts should publish the documents in languages used by families throughout the district. Denver Public Schools, for instance, produced a video for families in multiple languages explaining how students will be tested and what will occur if a student or staff member tests positive.[29]

Offline contact may be necessary as well. During the pandemic, several schools reached out by phone or personal visits to families of students who had not logged onto remote learning platforms.[30] Schools may have to make similar efforts to contact parents directly about the schools' data collection and sharing if the schools are aware that the parents do not have broadband access at home. Schools may also consider establishing hotlines or sending informational fliers home with students. Surveys, especially of historically disadvantaged groups, may be a useful way to solicit feedback from parents.

Health and biometric data are particularly sensitive, and failure to engage the community can provoke backlash and erode trust in schools' handling of student information.[31] Working with community members will help ensure a more equitable data collection program and avoid issues later.

Complying with FERPA

Along with community engagement, one of the first steps for a school or educational institution to reduce the risk in collecting and sharing health information is to comply with the Family Educational Rights and Privacy Act (FERPA). Schools should not assume that student health information is covered by the federal Health Insurance Portability and Accountability Act (HIPAA). Instead, FERPA applies broadly to any "education record" directly "related to a student" that is maintained by an educational institution that receives federal funding.[32] In turn, HIPAA, which was passed more than two decades after FERPA, expressly excludes education records from its coverage.[33] The Department of Education has consequently advised schools that FERPA applies to both health records maintained by schools, such as vaccination records, and their release to local, state, and federal health agencies.[34] Thus, health information maintained by an educational institution is likely covered by FERPA.

Two exceptions apply to this general conclusion. First, private primary and secondary schools that do not receive funds from the Department of Education are not subject to FERPA.[35] Second, independent health clinics based on school grounds but not funded or controlled by the school are not "educational institutions" subject to FERPA.[36] Importantly, because independent health clinics are not subject to FERPA, schools may wish to consider partnerships where independent clinics or even public health agencies collect and maintain student health data directly. Those partnerships are discussed in more detail below.

Collection Obligations

FERPA does not limit the information schools may collect, but it grants parents and students the right to review and amend their information. Schools are still required to find a way to comply with that right, even if schools are closed during the pandemic.[37]

Certain medical examinations, however, are limited by the federal Protection of Pupil Rights Amendment (PPRA).[38] The PPRA requires schools to "develop and adopt policies, in consultation with parents" regarding the "administration of physical examinations or screenings that the school or agency may administer to a student."[39] A school must provide notice of its policies annually and provide updates "after any substantive change" to its policies.[40] Those notices must provide parents an opportunity to opt out for any "nonemergency, invasive physical examination or screening" that is "required as a condition of attendance."[41]

Whether parents must be allowed to opt out of screenings for COVID-19 such as temperature checks or nose and throat swabs is not yet clear. The Department has offered comparatively little guidance on the PPRA and has promulgated no regulations on scope of "invasive physical examination[s]."[42] Although the scope of that provision is ultimately up to the Department, educational institutions should consult with counsel in creating their data collection and sharing programs to ensure that their policies, annual notices, and opportunities for parental opt-out are compliant with the PPRA.

Sharing Restrictions

Schools may also wish to share student health information with health agencies or other public entities. A school maintaining student health records may share those records only as permitted by FERPA.[43] FERPA's primary rule prohibits the disclosure of personally identifiable information (PII) from educational records without parental consent. PII is "information that can be used to distinguish or trace an individual's identity either directly or indirectly through linkages with other information,"[44] and includes the student's name, identification numbers, race, sex, and familial relationships. Consistent with FERPA, information regarding students may be disclosed if: (1) it has been de-identified, (2) the school obtains parental consent, (3) FERPA's health and safety emergency exception applies, or (4) the data is collected and maintained directly by an independent health entity.

De-identified information: A school may share student information with a health agency or other entity if it de-identifies that information, which may be useful for monitoring outbreaks across the community and tailoring responses accordingly. De-identified information has had "enough personally identifiable information removed or obscured so that the remaining information does not identify an individual and there is no reasonable basis to believe that the information can be used to identify an individual."[45] Techniques to de-identify information include presenting it in aggregate form or redacting personal information. De-identification, however, must avoid students being re-identifiable, including because small groups appear in aggregate data[46] or in light of "other reasonably available information."[47] The Department of Education has provided resources to guide educational agencies in assessing their de-identification strategies to help ensure that de-identified information does not inadvertently allow students to be re-identified.[48]

Obtaining parental consent: A school may also release student health records to a health agency if it obtains parental consent. Obtaining parental consent, however, may pose difficult administrative obstacles. Contact tracing and monitoring outbreaks will almost certainly require health agencies to obtain data across a student population, and obtaining parental consent from each student's parents may be administratively infeasible. Further, given the rapid spread of the novel coronavirus, efforts to monitor outbreaks may suffer serious shortcomings if even a few parents choose not to provide consent. Consequently, obtaining parental consent may prove neither feasible nor effective.

Health and safety emergency exception to consent: A school may disclose PII from student records if an exception to the consent requirement applies.[49] In particular, FERPA's "health and safety emergency" exception permits schools to share information with "appropriate parties" without parental consent if the school "determines that there is an articulable and significant threat to the health or safety of a student or other individuals."[50] That determination must be based on the "totality of the circumstances" and the "Department will not substitute its judgment for that of the educational agency or institution" if, "based on the information available at the time of the determination, there is a rational basis for the determination" that a health or safety emergency existed.[51] This is a "flexible" standard and the Department has expressly identified “public health officials” as “appropriate parties” to receive PII under the exception.[52]

Although the standard is flexible, the determination of an emergency must be based on the facts in the school or district. An “emergency” does not include “the threat of a possible or eventual emergency for which the likelihood of occurrence is unknown, such as would be addressed in general emergency preparedness activities.”[53] Instead, the exception “is temporally limited to the period of the emergency and generally does not allow for a blanket release of personally identifiable information.”[54] Thus, the emergency, “such as an outbreak of a pandemic,” must be “*actual*, *impending*, or *imminent*.”[55] In light of the H1N1 outbreak in 2009, the Department stated that a declaration of a public health emergency would constitute an emergency, “so long as there is a *current outbreak* of H1N1 in the particular school or school district.”[56] The obligation to assess facts within the school or district is not relieved by interagency agreements[57] or even state and local law.[58]

Finally, each disclosure of PII under the exception requires the school to record, with the students’ education records, the “articulable and significant threat to the health or safety” and the parties to whom the PII was disclosed.[59] If information sharing with a health agency is designed to span large groups of students or an entire student body, schools should be prepared to document each disclosure in the students’ education records.[60]

Data collected by independent health entity: FERPA’s requirements apply only to records “maintained” by “an educational agency or institution” which has received funds from the Department of Education or by an entity acting “on behalf of” an educational institution.[61] Consequently, FERPA’s requirements do not apply to independent healthcare providers such as an independent clinic on school grounds.[62] Records maintained by an independent health clinic would not constitute "education records" subject to FERPA. Thus, a school may avoid FERPA altogether by not collecting and maintaining student health information but permitting a health agency or other entity to do so directly.

A key consideration in determining whether a health agency is maintaining information “on behalf of” a school is whether the health agency is a “contractor” for the school.[63] The Department has advised in related contexts that a party’s status as a “contractor” depends, largely, on the school’s control of the information.[64] To qualify as a “contractor,” a school “must maintain direct control over its contractor’s access to and use of personally identifiable information.”[65] Thus, if a health agency collects student health information, but the school maintains direct control of the health agency's use of the information, the collection may be considered to be "on behalf of" the school and subject to FERPA.

Before permitting health agencies to collect and maintain student health data directly, schools should consider the effects of state law. State law may control when schools may permit health agencies to access school property or to examine students, or may affect when schools may collect biometric or medical information.

Data Governance Best Practices

In addition to engaging the community and ensuring that data collection practices meet legal requirements, schools should also develop robust data governance practices and policies. Governance policies, along with the training that accompanies them, give faculty and staff the tools to manage student data in a consistent and appropriate way. There are a number of elements that should be incorporated into governance for COVID-related data.

Data governance structures: Establishing a formal data governance structure for making decisions about COVID-related data provides a mechanism to make sure that all the necessary voices are heard for each decision, and to help resolve any confusion or conflicts about those decisions. This structure should be a continuation of the community engagement process discussed above. Several organizations, such as the Privacy Technical Assistance Center, offer further guidance on establishing a data governance framework.[66]

Goals for data collection: Having explicit goals for COVID-related data collection is important, as it defines a scope and prevents overcollection. These goals should be used to evaluate the efficacy of the program[67] and determine if the program needs to be adjusted and when it should be discontinued. These goals and metrics should also be communicated with the community.

Access, use, and redisclosure limitations: Data collected for contact tracing and other health purposes may be particularly sensitive and may ultimately be shared with health agencies, meaning that schools will have to cede much of the control over how it is used, potentially exposing students to risk that the data will be used in a way that harms them. One approach to mitigate this risk is to ensure that there are use limitations attached to the data, such as restrictions on publication, resharing, or reuse of the shared data.[68] These limitations should be codified in data sharing agreements with other agencies to ensure the data is used as expected. As described above, access, use, and redisclosure limitations will be key legal considerations in developing data sharing partnerships. For more information about data sharing agreements, see CDT's prior guidance.[69]

Retention and deletion plans: In addition to use limitations, organizations should determine when and how data will be deleted. This may be an explicit timeline (tracing data will be deleted two weeks after the end of the school year, for instance) or conditions that must be met (tracing data will be deleted once a vaccine is developed and the school has vaccination records for some percentage of students). How data will be deleted will depend on how it is stored, but schools and health agencies should use a strong deletion method to prevent accidental disclosure of the data. For a more in-depth discussion of this issue, see CDT's prior work on data deletion in education.[70]

Storage and transfer: As with all student data, but particularly sensitive data such as health-related information (like COVID-positive status or preexisting conditions), secure data storage and management is critical. Where and when possible, data should be encrypted, and all data should only be accessible to those who need that access to do their jobs.[71] In addition to secure storage, schools should consider best practices for transferring data, as some methods are substantially more secure than others. Methods like secure file transfers, feeds, and data-sharing services can provide a high level of security, though vendors should be vetted carefully. Physical transfer approaches like thumb drives or even paper records can be secure from a technical standpoint, but they present operational security concerns, such as how the drives will be erased. Insecure methods, like email or fax, are susceptible to interception, and so do not provide enough protection for sensitive student information.[72]

Security and breach responses: As schools collect data for COVID-related purposes, it is important to ensure that their data breach plans account for this new data. As with all data breach protocols, there should be clear roles for the school and any other agency who may have access to the data. They should also have plans to communicate with families so they know if they were affected and where to go for further assistance. Having these plans in place can make for a more efficient and effective response to any incidents, rather than having to spend time after an incident trying to determine what to do.

Data sharing agreements: However a school decides to collect and maintain student health information, it should consider entering into a written data sharing agreement with its health agency partners. In drafting those agreements, the school and health agency should consider the following:

- type of information being collected;

- method of collection;
- purposes of the collection and the permitted uses of the information;
- retention and destruction of the information collected, including a timeline for doing so;
- limitations on access to the information;
- limitations on redisclosure of the information;
- administrative and technical measures to ensure security and prevent unauthorized access or uses;
- the school's right to conduct audits;
- procedures for handling and responding to a data breach, including notification and mitigations responsibilities;
- parents' rights to review, delete, and opt out of the collection; and,
- whether the health agency is acting as a contractor on behalf of the school.

The Privacy Technical Assistance Center of the Department of Education has provided resources to help schools and school districts draft written agreements.[73]

Emerging Technology-Based Privacy Practices

Regardless of what reopening model they use, many school districts either will have to or already have had to use new technology in the face of the pandemic. As with any time schools use new technology, it is important to do so in a way that respects the privacy, safety, and well-being of students and their families. In the rush to continue learning during the pandemic, many schools may have adopted technology without the due diligence that would have prevailed in calmer times.[74] As schools go forward, it's important to remediate their technical landscape to minimize or avoid the harm from unmanaged technology.

I. Risks Imposed by Remote Learning Technology

There are a couple of risk factors that apply to technology that was adopted during the pandemic. First, because schools were and are operating in new ways, the technology they have adopted may not have been designed for an educational context, and consequently may not be adapted for the issues and legal framework that schools present (although even software designed for education may also struggle with that framework[75]). Take Zoom as an example. Many of the issues that plagued Zoom in the early days of the pandemic stemmed from "incorrectly" configured settings, like meetings that allowed any participant to share their screen. Much of this stems from the fact that Zoom was designed as a business platform, where the assumption was that most meeting participants were not going to try to prank their colleagues, so the default setting to allow for screen sharing made sense. In the classroom context, a default of "no screensharing unless explicitly allowed" is more practical.

The second risk is that edtech adopted for distance learning may not have gone through schools' and districts' normal governance procedures. This may mean that apps or edtech that would not normally have been approved, perhaps because of privacy or equity concerns, have been adopted by teachers. There are a number of concerns with unvetted edtech. It could expose information in unexpected ways, such as students' full names being inadvertently captured on a recording of a class session.[76] The technology may also introduce access and equity concerns if it does not include necessary accessibility features, or is incompatible with adaptive technology used by students or teachers.

II. Mitigating Risks by Remediating New Technology

Inventory edtech: The first step towards bringing schools' technical landscape up to par is building an accurate picture of all the technology currently in use in the school. Engage with teachers to inventory what, if any, technology they have adopted during distance learning. This engagement should be an open process, not a punitive one, to ensure that teachers feel comfortable being forthcoming and open about what technology they have been using. Additionally, schools should take an expansive view of technology. For instance, teachers streaming lessons on Facebook may not feel as though they have adopted new technology but, depending on how students interacted with the live stream, there may still be legal or governance considerations, so schools should ensure that teachers understand what constitutes "new technology." The inventory should not be a one-time process, but rather a continual one that accounts for new technology as it is added to adapt to schools' changing needs. For more information on inventorying systems, including a sample kick-off letter to send to staff, see CDT's prior guidance.[77]

After inventorying systems, there are two approaches to managing the new technology: incorporating the technology, or responsibly decommissioning it.

Incorporating new technology: If the new technology was adopted without legal review, that technology, and any agreements that were entered into by teachers (including accepting platforms' terms of service and privacy policies) should be reviewed by the legal department to ensure that they meet legal requirements. If the agreements cannot be brought into line with laws, the technology will likely need to be decommissioned, as described below.

Beyond legal compliance, newly adopted technology should also be reviewed to ensure that it is capable of adhering to internal governance policies. This process should consider issues such as: Does the new technology require obtaining parental consent for student use? If so, has that consent been obtained? If the new technology collects any student data, is the technology capable of adhering to schools' requirements about how that data is used by third parties? If so, are there any configurations that need to be set to ensure the technology performs appropriately, and the data is handled as expected? Once these questions are evaluated, the technology should be incorporated into the schools' existing governance procedures, such as updating data incident plans to account for any new data that is collected.

In addition to ensuring the new technology is legally acceptable and adheres to schools' and districts' governance requirements, it may also need to interoperate with other technology used by the school. Ideally, the tools will have the capability built in to engage with the school's existing systems. If they do not, and the tool is valuable enough to expend resources on, school technical staff may be able to build a "transform" to connect the systems (a transform converts data from one format to another to enable incompatible systems to interact). CDT's guidance around data portability expands on interoperability between systems.[78]

Decommissioning new technology: If the school does not wish to keep using the new edtech, it must responsibly decommission it. Teachers should pull any information they will need in the future from the service. This may mean copies of student assignments, grades, or attendance lists from remote classes. For some systems, there may be a way to download this information programmatically. This can be helpful, but teachers should check with technical staff at their school to ensure that the downloaded information is in a format the school can use. Some systems may offer a variety of formats, and technical staff will be able to tell teachers which would be preferable. For some systems, students may also wish to extract copies of their work or other information stored in the service. They should be notified ahead of time that the school plans to discontinue use of the tool so they can retrieve what they need.

In addition to extracting needed information from systems, schools should also take steps to ensure that their information and that of their students is deleted from the system. Unfortunately, this may not be as simple as the teacher deleting the account, as some tools will still retain the data, in case the account is reactivated or to use for other purposes like marketing or product improvement. The tool's terms of service may provide more information about how to truly delete user data. If not, schools may also need to consult with their legal departments to explore next steps. For more information about effective data deletion, see CDT's guidance.[79]

Conclusion

The novel coronavirus pandemic placed unprecedented demands on schools and educators, who were asked to transition their entire communities online overnight. In reopening this fall, schools have the opportunity to plan ahead to protect student and family privacy. Those plans may involve in-person learning, remote learning, or a hybrid of both. In-person learning will likely require schools to collect and share students' and families' health information, and schools should prioritize engaging the community, complying with FERPA, and establishing best data governance practices. Information sharing will require schools to comply with FERPA's health and safety emergency exception or to partner with health agencies or independent health clinics to collect the health information directly. Finally, schools should inventory their edtech, integrate systems they wish to retain into existing systems, and effectively decommission the rest.

Additional Resources

Legal Compliance

U.S. Department of Health and Human Services & U.S. Department of Education, Joint Guidance on the Application of the Family Educational Rights and Privacy Act (FERPA) and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) to Student Health Records (Dec. 2019), available at https://studentprivacy.ed.gov/resources/joint-guidance-application-ferpa-and-hipaa-student-health-records.

Centers for Disease Control and Prevention, Health Information & Privacy (Sept. 14, 2018), https://www.cdc.gov/phlp/publications/topic/healthinformationprivacy.html.

Letter from Michael B. Hawes, Director, Student Privacy Policy, Department of Education, to Monica D. Batanero, Associate General Counsel, School & College Legal Servicesof California (Apr. 12, 2018), available at https://studentprivacy.ed.gov/resources/letter-school-college-legal-services-california.

Student Privacy Policy Office, FERPA & Coronavirus Disease 2019 (COVID-19) (Mar. 2019), available at https://studentprivacy.ed.gov/resources/ferpa-and-coronavirus-disease-2019-covid-19.

Privacy Technical Assistance Center, FERPA Exceptions Summary (Apr. 2014), available at https://studentprivacy.ed.gov/resources/ferpa-exceptions-summary-apr-2014-2-page-standard-size.

Best Practices

Elizabeth Laird & Hannah Quay-de la Vallee, Center for Democracy & Technology, Protecting Privacy While Supporting Students Who Change Schools (June 20, 2019), available at https://cdt.org/wp-content/uploads/2019/07/2019-06-20-Portability-and-Privacy-Issue-Brief.pdf.

Elizabeth Laird & Hannah Quay-de la Vallee, Center for Democracy & Technology, Balancing the Scale of Student Data Deletion and Retention in Education (Mar. 2019), available at https://cdt.org/files/2019/03/Student-Privacy-Deletion-Report.pdf.

Privacy Technical Assistance Center, Guidance for Reasonable Methods and Written Agreements (Aug. 2015), available at https://studentprivacy.ed.gov/resources/guidance-reasonable-methods-and-written-agreements.

Privacy Technical Assistance Center, Written Agreement Checklist (July 2015), available at https://studentprivacy.ed.gov/resources/written-agreement-checklist.

Privacy Technical Assistance Center, Data De-identification: An Overview of Basic Terms at 4 (May 2013), available at https://studentprivacy.ed.gov/sites/default/files/resource_document/file/data_deidentification_terms_0.pdf.

Privacy Technical Assistance Center, Data Governance Checklist, U.S. Department of Education (Dec. 2011), available at https://nces.ed.gov/Forum/pdf/data_governance_checklist.pdf

Marilyn Seastrom, National Center for Education Statistics, Basic Concepts and Definitions for Privacy and Confidentiality in Student Education Records at 5-6 (Nov. 23, 2010), available at https://nces.ed.gov/pubsearch/pubsinfo.asp?pubid=2011601.

Remote Learning

Center for Democracy & Technology, COVID-19 and Student Privacy, Thinkific.com (June 2020), available at https://cdt.thinkific.com/courses/covid-19-student-privacy.

Consortium for School Networking, Privacy Considerations Checklist, EdTech Guidance, https://covid19edtechguidance.com/privacy-considerations-checklist/ (last visited June 17, 2020).
Consortium for School Networking, Video Conferencing Tools in the Age of Remote Learning: Privacy Considerations for New Technologies, EdTech Guidance, https://covid19edtechguidance.com/video-conferencing-tools-in-the-age-of-remote-learning-privacy-considerations-for-new-technologies/ (last visited June 17, 2020).

Reopening Schools

Consortium for School Networking, Rubrics, EdTech Guidance, https://covid19edtechguidance.com/evaluate-your-back-to-school-readiness/ (last visited June 17, 2020).
Centers for Disease Control and Prevention, Schools Decision Tool: Public Health Considerations for Reopening Schools During the COVID-19 Pandemic (last visited June 15, 2020), https://www.cdc.gov/coronavirus/2019-ncov/community/schools-childcare/schools-decision-tool.html.
California Department of Education, Stronger Together: Health & Safety (June 8, 2020), https://www.cde.ca.gov/ls/he/hn/strongertogethehealth.asp.
Kristina Ishmael, Rebecca Heiser, Jennifer Payne, Pandemic Planning for Distance Learning: Scenarios and Considerations for PreK–12 Education Leaders, New America (May 27, 2020), https://www.newamerica.org/education-policy/reports/pandemic-planning-for-distance-learning-scenarios-and-considerations-for-prek12-education-leaders/.
Los Angeles County Office of Education, A Planning Framework for the 2020-21 School Year (May 27, 2020), available at https://www.lacoe.edu/Home/School-Reopening.
Centers for Disease Control and Prevention, Considerations for Schools (May 19, 2020), https://www.cdc.gov/coronavirus/2019-ncov/community/schools-childcare/schools.html.
John P. Bailey & Frederick M. Hess, American Enterprise Institute, A Blueprint for Back to School (May 4, 2020), available at https://www.aei.org/research-products/report/a-blueprint-for-back-to-school/.

Appendix: Additional Exceptions to Parental Consent

As described in this brief, the health and safety emergency exception to FERPA's parental consent requirement may permit schools to share data with health agencies, although its application may be limited and it may pose administrative challenges for schools. Three other common exceptions, however, are unlikely to permit that sharing.

School official exception: The schools official exception permits disclosure of PII without consent to "school officials" with "legitimate educational interests" in the information or to any "contractor, consultant, volunteer, or other party."[80] To qualify, contractors, consultants, and volunteers must perform a function "for which the agency or institution would otherwise use employees," be under the "direct control of the agency or institution," and comply with certain requirements prohibiting redisclosure of PII.[81] A school using the school official exception must provide parents with a "specification of criteria for determining who constitutes a school official and what constitutes a legitimate educational interest" in its annual notice of FERPA rights.[82] Although a written information sharing agreement is not required under the school official exception, it is a best practice for schools to establish one.[83]

Those requirements are likely to pose obstacles for schools wishing to share health information with health agencies, for three reasons. First, whether or not a school would otherwise "use employees" to perform certain health functions may depend on the activity. Although some functions such as taking temperatures might be handled by employees such as nurses, other activities such as contact tracing or testing for coronavirus seem unlikely to be functions for which the school would otherwise use employees. Consequently, in determining whether a healthy agency may receive student health information, the school should be attentive to the function it intends the agency to perform. Second, the Department has interpreted "direct control" to require "restricting the provider from using the PII for unauthorized purposes," limiting access and use, and mandating protective measures.[84] It is not clear how a health entity would implement contact tracing or other programs subject to "direct control" by the school. Third, a school's annual notice may not encompass health agencies within its definition of school officials. For example, the Department's model notice lists "attorney, auditor, medical consultant, or therapist" as possible contractors under the exception,[85] and notices with similar language may not encompass entire health agencies.

Directory information: FERPA permits certain PII to be shared without consent on the basis that it "would not generally be considered harmful or an invasion of privacy if disclosed."[86] Directory information includes a student's name, address, email address, photograph, date of birth, and grade level, among other things.[87] Directory information must be designated in a notice provided to parents, providing them an opportunity to opt out.[88] Common uses of directory information include yearbooks, playbills for student productions, honor rolls, and sports programming.[89] However, directory information cannot be released with other PII,[90] including health status or absence information.[91] Thus, a school may share the directory information of its students whose parents have not opted out, but it may not share only the information of absent or sick students, as that would reveal protected PII.

Audit and study exceptions: Finally, two closely related exceptions to FERPA's consent requirement—the audit and study exceptions—are unlikely to apply. The audit exception permits disclosure of PII to certain federal and state officials "in connection with an audit or evaluation of Federal or State supported education programs, or for the enforcement of or compliance with Federal legal requirements that relate to those programs."[92] The study exception permits disclosure to organizations to "[d]evelop, validate, or administer predictive tests," "[a]dminister student aid programs," or "[i]mprove instruction."[93] Both of those exceptions also carry similar obligations for the school to enter into written agreements with partner organizations.[94]

Those two exceptions, however, are unlikely to permit sharing with health agencies. Contact tracing and other health uses neither fall within an "audit or evaluation" of an education program, nor do they involve developing predictive tests, administering student aid, or improving instruction under the study exception. For example, the Department has described the audit exception as covering the release of college transcripts to a student's former high school "to evaluate how effectively the [high school] prepared its students for success in postsecondary education."[95] Similarly, the Department has described the study exception as covering the release of PII to "conduct a study that compares program outcomes across school districts to further assess what programs provide the best instruction."[96] Those examples bear little similarity to sharing information with a health agency.

Further, a health agency likely does not qualify as a "[s]tate or local educational authority" under the audit exception.[97] The Department, for example, advised North Dakota to discontinue its program of sharing student PII with a state agency that matched education records with wage and employment information, because the agency did not qualify as an "educational authority" and was not under the direct control of the state educational agency.[98] Consequently, a health agency likely does not qualify to receive student information under the audit exception.

Endnotes

1. Jessica Hansom, National Immigration Law Center, The Legal Authority for "Sanctuary" School Policies at 5-7 (Aug. 2018), available at https://www.nilc.org/issues/immigration-enforcement/sanctuary-school-practice-advisory/.

2. *See* 34 CFR § 300.610; *generally* U.S. Department of Education, IDEA and FERPA Confidentiality Provisions (June 2014), available at https://www2.ed.gov/policy/gen/guid/ptac/pdf/idea-ferpa.pdf.

3. Lisa Weintraub Schifferle, COPPA Guidance for Ed Tech Companies and Schools During the Coronavirus, Federal Trade Commission (Apr. 9, 2020), https://www.ftc.gov/news-events/blogs/business-blog/2020/04/coppa-guidance-ed-tech-companies-schools-during-coronavirus.

4. Patrick Wall, With Cell Phones and Laptops, Newark Teachers Stay Connected with Students During School Shutdown, Chalkbeat (Mar. 19, 2020), https://newark.chalkbeat.org/2020/3/19/21196078/with-cell-phones-and-laptops-newark-teachers-stay-connected-with-students-during-school-shutdown; Patrick O'Donnell, Cleveland Teachers Take Lessons to TV to Stem Learning Loss, Stay Connected to Students Through Coronavirus, The 74 (May 26, 2020), https://www.the74million.org/article/cleveland-teachers-take-lessons-to-tv-to-stem-learning-loss-stay-connected-to-students-through-coronavirus/.

5. Robin Lake & Bree Dusseault, Remote Classes Are in Session for More School Districts, But Attendance Plans Are Still Absent, Center on Reinventing Public Education (Apr. 26, 2020), https://www.crpe.org/thelens/remote-classes-are-session-more-school-districts-attendance-plans-are-still-absent; Naugatuck Public Schools, Distance Learning Plan at 5, 6-8, available at https://sites.google.com/naugatuck.k12.ct.us/distancelearning/home (last visited June 15, 2020).

6. Michelle Davis, What Soldiers, Doctors, and Professors Can Teach Us About Artificial Intelligence During COVID-19, Education Week (May 19, 2020), https://www.edweek.org/ew/articles/2020/05/20/what-soldiers-doctors-and-professors-can-teach.html; David Saleh Rauf, Artificial Intelligence in K-12: The Right Mix for Learning or a Bad Idea?, Education Week (May 19, 2020), https://www.edweek.org/ew/articles/2020/05/20/artificial-intelligence-in-k-12-the-right-mix.html.

7. Diane Klein, And Now, Charybdis: The Risks of Recording (Especially Synchronous) Classes, Dorf on Law (Mar. 25, 2020), http://www.dorfonlaw.org/2020/03/and-now-charybdis-risks-of-recording.html.

8. FBI National Press Office, FBI Warns of Child Sexual Abuse Material Being Displayed During Zoom Meetings (May 20, 2020), https://www.fbi.gov/news/pressrel/press-releases/fbi-warns-of-child-sexual-abuse-material-being-displayed-during-zoom-meetings; Kristen Setera, FBI Warns of Teleconferencing and Online Classroom Hijacking During COVID-19 Pandemic, FBI Boston (Mar. 30, 2020), https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-warns-of-teleconferencing-and-online-classroom-hijacking-during-covid-19-pandemic.

9. *See* T. Keung Hui, NC Transgender Students Worried About Being Outed Online During COVID-19 Pandemic, The News & Observer (Apr. 10, 2020), https://www.newsobserver.com/news/local/education/article241914151.html.

10. American School Counselor Association, The School Counselor and Virtual School Counseling, ASCA Position Statements at 94 (2017), available at https://www.schoolcounselor.org/school-counselors-members/publications/position-statements; National Association of School Psychologists, Telehealth: Virtual Service Delivery Updated Recommendations at 2 (2020), available at https://www.nasponline.org/resources-and-publications/resources-and-podcasts/covid-19-resource-center/special-education-resources/telehealth-virtual-service-delivery-updated-recommendations.

11. Howard Blume and Sonali Kohli, Schools Issue Warning: Coronavirus Testing and Tracing Are Needed Before Campuses Reopen, Los Angeles Times (May 30, 2020), https://www.latimes.com/california/story/2020-05-30/school-leaders-demand-help-on-testing-tracing-for-campuses-to-reopen; Centers for Disease Control and Prevention, Schools During the COVID-19 Pandemic (May 15, 2020),

available at https://www.cdc.gov/coronavirus/2019-ncov/community/schools-childcare/schools-decision-tool.html.

[12] Stephen Noonoo, Health Experts Say Schools Can Reopen in the Fall — But With Some Big Changes, EdSurge (May 20, 2020), https://www.edsurge.com/news/2020-05-20-health-experts-say-schools-can-reopen-in-the-fall-but-with-some-big-changes.

[13] Center for Democracy & Technology, COVID-19 and Student Privacy, Thinkific.com (June 2020), available at https://cdt.thinkific.com/courses/covid-19-student-privacy.

[14] *See* COVID-19: Going Back to School Safely Hearing Before the Senate Committee on Health, Education, Labor, & Pensions, 116th Congress (2020) (testimony of Penny Schwinn, Tennessee Commissioner of Education), available at https://www.help.senate.gov/hearings/covid-19-going-back-to-school-safely; *id.* (testimony of Susana Cordova, Superintendent, Denver Public Schools) [hereinafter Cordova Testimony].

[15] Center for Democracy & Technology, COVID-19 and Student Privacy, Thinkific.com (June 2020), available at https://cdt.thinkific.com/courses/covid-19-student-privacy.

[16] Naaz Modan, How Feasible Are School Reopening Plans for Fall?, Education Dive (May 18, 2020), https://www.educationdive.com/news/how-feasible-are-school-reopening-plans-for-fall/578112/.

[17] Khalilah M. Harris, In the Wake of the Coronavirus, We Must Design and Build the Schools We Need—Not Simply Reopen Schools As They Were, Center for American Progress (May 26, 2020), https://www.americanprogress.org/issues/education-k-12/news/2020/05/26/485446/wake-coronavirus-must-design-build-schools-need-not-simply-reopen-schools/.

[18] Trump's Call to Reopen School Buildings Is Dangerous for Students, Staff, National Education Association (Apr. 28, 2020), http://www.nea.org/home/76098.htm; John P. Bailey & Frederick M. Hess, American Enterprise Institute, A Blueprint for Back to School at 7 (May 4, 2020), available at https://www.aei.org/wp-content/uploads/2020/05/A-Blueprint-for-Back-to-School-One-Pager.pdf; Considerations for Schools, Centers for Disease Control and Prevention (May 19, 2020), https://www.cdc.gov/coronavirus/2019-ncov/community/schools-childcare/schools.html.

[19] Centers for Disease Control and Prevention, Contact Tracing - CDC’s Role and Approach (June 11, 2020), https://www.cdc.gov/coronavirus/2019-ncov/downloads/php/contact-tracing-CDC-role-and-approach.pdf.

[20] Elizabeth Laird & Hannah Quay-de la Vallee, Center for Democracy & Technology, Data Sharing & Privacy Demands in Education: How to Protect Students While Satisfying Policy & Legal Requirements (Nov. 13, 2019) [hereinafter Data Sharing Brief], available at https://cdt.org/insights/data-sharing-privacy-demands-in-education-how-to-protect-students-while-satisfying-policy-legal-requirements/.

[21] Stronger Together: Health & Safety, California Department of Education (June 8, 2020), https://www.cde.ca.gov/ls/he/hn/strongertogethehealth.asp.

[22] Considerations for Schools, Centers for Disease Control and Prevention (May 19, 2020), https://www.cdc.gov/coronavirus/2019-ncov/community/schools-childcare/schools.html.

[23] *See* T. Keung Hui, NC Transgender Students Worried About Being Outed Online, *supra* note 9.

[24] *See* Alain Jehlen, ICE Had Access to 135 BPS Student “Incident Reports,” Groups Say, Schoolyard News (Jan. 6, 2020), https://schoolyardnews.com/ice-had-access-to-135-bps-student-incident-reports-groups-say-9d4101cc9b44.

[25] Covid-19 Fueling Anti-Asian Racism and Xenophobia Worldwide, Human Rights Watch (May 12, 2020), https://www.hrw.org/news/2020/05/12/covid-19-fueling-anti-asian-racism-and-xenophobia-worldwide.

[26] Data Sharing Brief, *supra* note 20, at 6.

[27] 20 U.S.C. § 1232h(c)(2)(C).

[28] Privacy Technical Assistance Center, Guidance for Reasonable Methods and Written Agreements at 8 (Aug. 2015), https://studentprivacy.ed.gov/resources/guidance-reasonable-methods-and-written-agreements.

[29] Cordova Testimony, *supra* note 14, at 3.

[30] Jessica Bakeman, Miami-Dade Schools See Lower Virtual Attendance in Low-Income, Immigrant Communities, WLRN (Apr. 22, 2020), https://www.wlrn.org/post/miami-dade-schools-see-lower-virtual-attendance-low-income-immigrant-communities; Patrick Wall, “I Can’t Find Them”: Attendance Was Already a Challenge in Newark. The Coronavirus Create New

Barrier (Apr. 17, 2020), https://newark.chalkbeat.org/2020/4/17/21230488/i-can-t-find-them-attendance-was-already-a-challenge-in-newark-the-coronavirus-created-new-barriers.

31. *See* Kathleen McGrory, Florida Lawmakers to Consider Banning Biometrics in Schools, Tampa Bay Times (Feb. 2, 2014), https://www.tampabay.com/news/education/k12/florida-lawmakers-to-consider-banning-biometrics-in-schools/2163862/.

32. 34 CFR 99.3.

33. 45 CFR § 160.103.

34. Letter from Michael B. Hawes, Director, Student Privacy Policy, Department of Education, to Monica D. Batanero, Associate General Counsel, School & College Legal Services of California (Apr. 12, 2018), https://studentprivacy.ed.gov/resources/letter-school-college-legal-services-california; Letter from LeRoy S. Rooker, Director, Family Policy Compliance Office, U.S. Department of Education, to Martha Holloway, State School Nurse Consultant, Alabama Department of Education (Feb. 25, 2004), https://studentprivacy.ed.gov/resources/letter-alabama-department-education-re-disclosure-immunization-records; Letter from LeRoy S. Rooker, Director, Family Policy Compliance Office, U.S. Department of Education, to Heidi Atkins Lieberman, Legal Counsel, Missouri Department of Elementary and Secondary Education (Nov. 17, 1994) [hereinafter Atkins Letter], available at https://studentprivacy.ed.gov/resources/letter-missouri-department-elementary-and-secondary-education-regarding-disclosures.

35. U.S. Department of Health and Human Services & U.S. Department of Education, Joint Guidance on the Application of the Family Educational Rights and Privacy Act (FERPA) and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) to Student Health Records at 8 (Dec. 2019) [hereinafter Joint Guidance], available at https://studentprivacy.ed.gov/resources/joint-guidance-application-ferpa-and-hipaa-student-health-records.

36. *Id.* at 8-9.

37. Kala Shah Surprenant, Acting Director, Student Privacy Policy Office, FERPA & Virtual Learning During COVID-19 (Mar. 30, 2020), available at https://studentprivacy.ed.gov/resources/ferpa-and-virtual-learning; 34 CFR §§ 99.10(d)(2), .20-.21.

38. 20 U.S.C. § 1232h.

39. *Id.* § 1232h(c)(1)(D)

40. *Id.* § 1232h(c)(2)(A).

41. *Id.* §§ 1232h(c)(2)(C),1232h(c)(6)(B).

42. Student Privacy Policy Office, PPRA, Protecting Student Privacy, https://studentprivacy.ed.gov/content/ppra (last visited June 22, 2020) ("The regulations do not reflect these most recent amendments to PPRA, and certain provisions in the current regulations are superseded by these statutory amendments.").

43. 34 CFR § 99.30.

44. Student Privacy Policy Office, Glossary, Protecting Student Privacy, https://studentprivacy.ed.gov/glossary (last visited June 11, 2020).

45. Student Privacy Policy Office, Glossary, Protecting Student Privacy, https://studentprivacy.ed.gov/glossary (last visited June 11, 2020).

46. Privacy Technical Assistance Center, Data De-identification: An Overview of Basic Terms at 4 (May 2013), available at https://studentprivacy.ed.gov/sites/default/files/resource_document/file/data_deidentification_terms_0.pdf.

47. 34 CFR § 99.31(b)(1).

48. See Marilyn Seastrom, National Center for Education Statistics, Basic Concepts and Definitions for Privacy and Confidentiality in Student Education Records at 5-6 (Nov. 23, 2010), available at https://nces.ed.gov/pubsearch/pubsinfo.asp?pubid=2011601.

49. Three other common exceptions are less likely to be helpful, and we provide an analysis of those exceptions in the Appendix.

50. 34 CFR § 99.36(a), (c).

51. *Id.* § 99.36(c).

52. U.S. Department of Education, FERPA & Coronavirus Disease 2019 (COVID-19) (Mar. 2019) [hereinafter FERPA & Coronavirus], available at https://studentprivacy.ed.gov/resources/ferpa-and-coronavirus-disease-2019-covid-19.

53. Family Policy Compliance Office, Family Educational Rights and Privacy Act (FERPA) and H1N1 at 3 (Oct. 2009) [hereinafter FERPA & H1N1], available at https://studentprivacy.ed.gov/resources/ferpa-and-h1n1-virus.

54. *Id.* at 2.

55. Hawes, *supra* note 34, at 4.

56. FERPA & H1N1, *supra* note 53, at 3 (emphasis in original).

57. *Id.* at 6.

58. Hawes, *supra* note 34, at 4.

59. 34 CFR § 99.32(a)(5).

60. *Id.* § 99.31(a)(1).

61. 34 CFR §§ 99.3, .1.

62. Atkins Letter, *supra* note 34; Joint Guidance, supra note 35, at 9.

63. Joint Guidance, *supra* note 35, at 9.

64. See Letter from LeRoy S. Rooker, Director, Family Policy Compliance Office, Department of Education, to Lea Ann Schneider, Assistant Attorney General, State of North Dakota at 3 (June 23, 2005), https://studentprivacy.ed.gov/resources/letter-north-dakota-assistant-attorney-general-regarding-matching-education-and-employment; Letter from Letter from LeRoy S. Rooker, Director, Family Policy Compliance Office, to Lucille E. Davy, Commissioner, New Jersey Department of Education (Jan. 11, 2008) [hereinafter New Jersey Letter], available at https://studentprivacy.ed.gov/resources/letter-new-jersey-department-education-regarding-student-database-january-2008.

65. New Jersey Letter, *supra* note 64, at 2.

66. Privacy Technical Assistance Center, Data Governance Checklist, U.S. Department of Education, December 2011, https://nces.ed.gov/Forum/pdf/data_governance_checklist.pdf; Corey Chatis, Missy Cochenour & Stephanie Irvine, Early Childhood Data Governance in Action! Initial Steps to Establish Data Governance, Institute of Education Sciences (IES) Statewide Longitudinal Data Systems (SLDS) Grant Program, U.S. Department of Education, https://nces.ed.gov/programs/slds/pdf/EC_DataGovernance_Initial.pdf; Institute of Education Sciences (IES) Statewide Longitudinal Data Systems (SLDS) Grant Program, Data Governance Toolkit, U.S. Department of Education, https://slds.grads360.org/#program/data-governance; Center for Democracy & Technology, COVID-19 and Student Privacy, Thinkific.com (June 2020), available at https://cdt.thinkific.com/courses/covid-19-student-privacy.

67. *See* Center for Democracy & Technology et al., Principles for Protecting Civil Rights and Privacy During the COVID-19 Crisis at 2-3 (June 12, 2020) [hereinafter Civil Rights Letter], at 2, available at https://cdt.org/insights/cdt-joins-principles-for-protecting-civil-rights-and-privacy-during-the-covid-19-crisis/.

68. *Id.*

69. Center for Democracy & Technology, COVID-19 and Student Privacy, Thinkific.com (June 2020), available at https://cdt.thinkific.com/courses/covid-19-student-privacy.

70. Elizabeth Laird & Hannah Quay-de la Vallee, Center for Democracy & Technology, Balancing the Scale of Student Data Deletion and Retention in Education (Mar. 2019) [hereafter Deletion Brief], available at https://cdt.org/files/2019/03/Student-Privacy-Deletion-Report.pdf.

71. Civil Rights Letter, *supra* note 67, at 3.

72. Elizabeth Laird & Hannah Quay-de la Vallee, Center for Democracy & Technology, Protecting Privacy While Supporting Students Who Change Schools (June 20, 2019) [hereinafter Portability Brief], https://cdt.org/wp-content/uploads/2019/07/2019-06-20-Portability-and-Privacy-Issue-Brief.pdf; Data Sharing Brief, supra note 20.

73. *See* Privacy Technical Assistance Center, Guidance for Reasonable Methods and Written Agreements (Aug. 2015), available at https://studentprivacy.ed.gov/resources/guidance-reasonable-methods-and-written-agreements; Privacy Technical Assistance Center, Written Agreement Checklist (July 2015), available at https://studentprivacy.ed.gov/resources/written-agreement-checklist.

74. *See* Patrick Wall, With Cell Phones and Laptops, Newark Teachers Stay Connected with Students During School Shutdown, *supra* note 4.

75. Nick Stat, Google Sued by New Mexico Attorney General for Collecting Student Data Through Chromebooks, The Verge (Feb. 20, 2020) https://www.theverge.com/2020/2/20/21145698/google-student-privacy-lawsuit-education-schools-chromebooks-new-mexico-balderas.

76. Hannah Natanson, Failed tech, missed warnings: How Fairfax schools' online learning debut went sideways, The Washington Post (April 18, 2020) https://www.washingtonpost.com/local/education/fairfax-schools-online-learning-blackboard/2020/04/18/3db6b19c-80b5-11ea-9040-68981f488eed_story.html.

77. Deletion Brief, *supra* note 70, at 8-9; *see also* Data Inventory Guide, GovEx Labs (Mar. 8, 2019), https://labs.centerforgov.org/data-governance/data-inventory/.

78. Portability Brief, *supra* note 72.

79. Deletion Brief, *supra* note 70.

80. 34 CFR § 99.31(a)(1)(i).

81. *Id.* § 99.31(a)(1)(i)(B).

82. *Id.* § 99.7(a)(3)(iii).

83. Student Privacy Policy Office, Must a School Have a Written Agreement or Contract With a Community-Based Organization to Which it Non-Consensually Discloses Education Records to Outsource an Institutional Service Under the School Official Exception?, Protecting Student Privacy, https://studentprivacy.ed.gov/faq/must-school-have-written-agreement-or-contract-community-based-organization-which-it-non (last visited June 14, 2020).

84. Student Privacy Policy Office, Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices at 4 (Feb. 2014), available at https://studentprivacy.ed.gov/resources/protecting-student-privacy-while-using-online-educational-services-requirements-and-best.

85. Student Privacy Policy Office, FERPA Model Notification of Rights for Elementary & Secondary Schools (Apr. 2020), available at https://studentprivacy.ed.gov/node/490.

86. 34 CFR § 99.3.

87. *Id.*

88. *Id.* § 99.37.

89. Student Privacy Policy Office, Model Notice for Directory Information at 1 (Mar. 2011), available at https://studentprivacy.ed.gov/resources/model-notice-directory-information.

90. 34 CFR § 99.37(e).

91. FERPA & Coronavirus, *supra* note 52, at 5.

92. 34 CFR § 99.35(a)(1); *accord id.* § 99.31(a)(3).

93. 34 CFR § 99.31(a)(6)(i).

94. 34 CFR §§ 99.31(a)(6)(iii)(C), .35(a)(3).

95. Student Privacy Policy Office, Guidance for Reasonable Methods and Written Agreements at 2 (Aug. 2015), available at https://studentprivacy.ed.gov/resources/guidance-reasonable-methods-and-written-agreements.

96. *Id.* at 1.

97. *See* Letter from LeRoy S. Rooker, Director, Family Policy Compliance Office, Department of Education, to Lea Ann Schneider, Assistant Attorney General, State of North Dakota at 3 (June 23, 2005), https://studentprivacy.ed.gov/resources/letter-north-dakota-assistant-attorney-general-regarding-matching-education-and-employment.

98. *Id.*