



SCHOOL NURSING Fact Sheet

Data Sharing Guidance for School Nurses

School nurses collect and maintain a vast amount of personal information related to students and their health. The ability to share these data with (and obtain information from) other health care providers and agencies is important for a number of reasons, including:


- enhancing continuity of care,
- improving students' health management at school,
- preventing duplication of efforts across organizations,
- conducting important health and surveillance research,
- enriching collaboration among providers and partner organizations, and
- determining best practices in student care.

As education clearly emerges as a social determinant of health, enhanced integration of schools and child health care will be important to improving academic and health outcomes. Nonetheless, challenges to data sharing exist in the K-12 setting, some real and some perceived. This guidance document sets forth requirements imposed by federal law regarding use and disclosure of student education record data and will share strategies for devising agreements that allow legal and efficient data sharing in compliance with federal law. It also presents examples to illustrate specific data sharing situations that school nurses may encounter and how these agreements can facilitate communication and collaboration among providers and other entities in compliance with state and federal law.

Note that this guidance document is not intended to substitute for legal counsel. Parties should consult an attorney in developing, or at least reviewing, any data sharing agreement to ensure compliance with state and federal law. Also, most education and health care agencies have designated privacy officers who are knowledgeable about privacy laws and regulations, as well as relevant organizational policy and operations. These individuals should be engaged early and throughout the process of developing data sharing strategies and agreements.

FERPA

The Family Educational Rights Privacy Act (FERPA) is a federal law that governs confidentiality and sharing of information contained in student education records by schools. The Health Insurance Portability and Accountability



Act (HIPAA) controls data privacy and sharing by health care professionals; however, registered nurses practicing in a school setting will almost always be subject to FERPA instead. This is because HIPAA expressly excludes education records that are covered by FERPA.¹

Under FERPA, an “education record” is one that directly relates to a student and is maintained by the school or an entity acting on a school’s behalf. Education records include student health information, such as nurses’ exam notes in the student’s file, immunization and physical exam records, health screening results, and records related to special education or student health plans. FERPA generally forbids schools from disclosing personally identifiable information (PII)² contained in students’ education records without written consent from a parent or guardian. However, the law does provide some exceptions that allow school personnel to share certain PII without parental consent.^{3,4}

PII vs. Non-PII

FERPA does *not* require parental consent for the release of non-personally identifiable information (non-PII), so schools can share aggregate or de-identified student health information without consent for research, program evaluation, and other purposes.⁵ De-identified data removes identifiers, such as names, social security numbers, student identification numbers, thereby greatly reducing the risk of disclosure. While consent is not required to share de-identified aggregate student data, schools may still want to inform parents of the intention to share such data, with whom, and for what purpose in order to promote transparency and built trust.

Schools should also double check de-identified or aggregate data to ensure that unique identifiers are not inadvertently disclosed—a common problem for data on small populations. For example, if an aggregated data set reports that 100% of Asian/Pacific Islander students in Grade 10 at Southeast High School were seen by the school nurse for a sexually transmitted infection, and there are only two students that match that description, that otherwise “de-identified” data set contains unique identifiers.⁶ In its data sharing guidance, the U.S. Department of Education recommends three strategies for avoiding accidental disclosure due to unique identifiers: suppression (removing any data with unique identifying characteristics); blurring (reducing the precision of the reported data to “mask” the unique identifiers, such as reporting a range rather than specific figures); and perturbation (introducing “noise” or manipulating small amounts of data to prevent users from identifying individual students).⁷


FERPA also allows schools to share “directory information” without parental consent, although schools must publicly define what it considers to be “directory information” and give parents an opportunity to opt out of its disclosure.⁸ “Directory information” can include information such as name, address, telephone number, date and place of birth, participation in officially recognized activities and sports, and dates of attendance.⁹ While directory information may be disclosed without parental permission (unless parents have opted out), it may not be linked with other identifying data. For example, a school may disclose a list of students in 8th grade, but it may not disclose a list of 8th graders who received the HPV vaccine or who were absent on a certain date.

State Law

It is important to note that state law may place more stringent requirements on data privacy, use, and sharing. Generally, where a school cannot comply with both FERPA and state law, the federal law prevails. [Contact](#) the Network for Public Health Law with questions about perceived conflicts or for questions on specific state laws.

Sharing PII *with* Parental Consent

FERPA allows schools to disclose PII with written parental consent. Parental consent forms authorizing the school to release student data should:

- 
- be specific;
 - contain the *type* of information that may be shared (e.g., disciplinary records, academic records, health records, all information pertaining to a child's Section 504 plan or individualized education program (IEP)¹⁰, etc.);
 - list *with whom* the information may be shared (e.g., any licensed health care provider, a specific provider, any health care entity providing care to the child, research organizations); and
 - describe any limitations on when, how, or to whom the data may be shared. Such limitations should include a timeframe describing how long the data will be shared.

Because students' sensitive personal health information is at stake, data sharing practices—even with parental consent—should adhere to principles of ethics and good stewardship.¹¹ Data sharing agreements or memoranda of understanding can help to ensure that all parties with access to the data adhere to the same principles of ethics and professionalism.

Sharing PII *without* Parental Consent

While obtaining consent is usually the best way to ensure compliance with state and federal law, it may sometimes prove impracticable. In these situations, certain narrow FERPA exemptions allow schools to disclose student information without consent. For example, students' educational records (including health information) may be shared with any of the following persons or in any of the following situations:


1. with school officials with a "legitimate educational interest,"
2. with other schools to which the student is transferring,
3. to comply with a judicial order or valid subpoena,
4. to appropriate officials in health and safety emergencies,
5. for educational studies or federal or state audits, and
6. with parties to whom the school has *outsourced institutional services or functions*.¹²

Under this "outsourced institutional services" exemption, parties who carry out these services or functions on behalf of the school are deemed to be school officials with a legitimate educational interest in the private educational record of the students. This exemption is perhaps the most useful for enabling public health data sharing by schools, because it allows legal data sharing arrangements with outside health care providers and other entities for certain purposes without parental consent.¹³

Specifically, schools may share PII from education records with:

Contractors, consultants, volunteers, or other parties to whom an agency or institution has outsourced institutional services or functions. These outside persons or organizations are considered "school officials" under FERPA provided that:

- (1) They perform an institutional service or function for which the agency or institution would otherwise use employees;
- (2) Are under the direct control of the agency or institution with respect to the use and maintenance of education records; and
- (3) Are subject to the requirements of FERPA regarding the use and redisclosure of PII from education records.¹⁴ That is, third parties may not redisclose the PII to anyone else without written parental



consent. Employees or agents of the third party may use the data, but only for the purpose for which the original disclosure was made.

One approach to operationalize and safeguard use of this exemption is to require organizations to apply for a special institutional services status. For example, Seattle Public Schools has implemented a process by which community-based organizations can apply for an “institutional service exemption” if they meet certain criteria, sign a data sharing agreement, and complete data stewardship training.¹⁵ Data sharing agreements are important for ensuring that all parties with access to the data are bound by the requirements of FERPA and other applicable laws, as well as principles of ethics and professionalism. Data sharing arrangements and resulting agreements must comply with the requirements of the outsourced services exception under FERPA.¹⁶

Transparency

Transparency remains an important guiding principle for any data sharing arrangement. Most people are willing to share personal health information if they feel that they are fully informed and can appreciate the benefit it will have to themselves, their children, or the community at large.¹⁷ As a best practice in maintaining parent and community trust, schools and their partners should post data sharing agreements on their public websites, including the data elements that are shared, how the data are used, and the purpose for the data sharing.¹⁸ The use of PII from education records should be limited to those purposes that are specified in the data sharing agreement.

Sharing Data with Health Care Providers

While public school nurses are generally subject to FERPA, the health care providers with whom they want to share data must adhere to the HIPAA privacy rule. HIPAA allows health care providers to disclose protected health information (PHI) without parental consent or authorization for treatment purposes. Likewise, a school nurse may (under FERPA) communicate with a student’s outside health care provider to clarify that provider’s treatment orders.¹⁹ To facilitate ongoing communication with a student’s outside medical care providers, school nurses should consider obtaining a parental release that allows free exchange of information relating to the student’s care plan and progress.

Data Sharing Arrangements

Important Questions to Ask

The Network has developed a tool to assist public health practitioners and advocates in thinking through and collecting the information needed to enter into data sharing arrangements, entitled the “Checklist for Information Needed to Address Proposed Data Collection, Access, and Sharing to Improve the Health of Communities.”²⁰ Adapted from this tool, the questions below are intended to guide school nurses and other school personnel through the important issues to consider when considering a data sharing arrangement.

1. What is the purpose for data sharing?

Before entering into any data sharing arrangement, the parties need to come to an understanding about the purpose of the data sharing. What is the desired student health outcome? Data sharing arrangements should support this goal. Articulating the purpose of the data sharing at the outset is important for a number of reasons. First, the legal requirements governing data disclosure and use can vary depending on the purpose for disclosing data. For example, specific purposes may fall within certain FERPA exceptions for sharing without consent. Also, in the event that consent is required by law for data sharing, the purpose must be fully articulated in the consent form.



2. Who are the parties involved?

Which parties will have access to the student data? Are there existing relationships among those parties? Who are the champions for data sharing—those who will guide the process with vigilance? Are there multiple sectors involved (health and non-health, public and private)? Identifying existing relationships and building open and trusting relationships among those using the data is critical to ensuring compliance with legal and ethical requirements and continued use for public health and student care purposes.

3. What specific types of data are involved?

Which data elements need to be shared, and where will they be obtained? The type of data to be shared also matters. For example, law generally does not restrict the use or disclosure of de-identified data, because information that allows personal identification of an individual student has been removed. For this reason, one should first consider whether de-identified data will satisfy data sharing needs. Finally, standardized data formats facilitate and streamline data exchange.

4. Which laws apply?

Every point at which student data “changes hands” is a potential decision point with regard to the law. Generally, FERPA will apply to the sharing of student health information by schools. (In the rare circumstance where a school receives no funding from the U.S. Department of Education *and also* qualifies as a covered entity under HIPAA, then HIPAA would apply.) Health care providers with whom school nurses are sharing data must comply with the HIPAA privacy rule. Most states have passed student privacy laws that may be more restrictive than federal law. Because they set prerequisites, conditions, and limitations on data sharing, applicable laws should guide whether and how the data are disclosed, stored, used, and reused or destroyed. These issues form the backbone of any Data Sharing Agreement (DSA) or data-sharing Memorandum of Understanding (MOU).


5. What kind of agreement(s) do you need? ²¹

The parties should put agreements in place that guide data disclosure, use, and maintenance by everyone that will have access to the student data. Such agreements ensure that the parties adhere to applicable laws, as well as standards of professionalism and ethics. Agreements among the parties should be specific, compliant with applicable federal and state laws, and should support the purpose of the data sharing arrangement; they set out the applicable legal authority, spell out the terms for sharing, and provide for monitoring and accountability for compliance with these terms. Determining why you are sharing data with these specific partners can help determine which type of agreement is most appropriate. Depending on the circumstances, a Data Sharing Agreement (DSA) or MOU may be appropriate; these common types of agreements are described below.

Data Sharing Agreements (DSA)

A DSA is a legally enforceable agreement that operationalizes the sharing of data among parties, including organizations and individuals, while protecting existing data rights, such as privacy and confidentiality. Because a DSA is a binding legal document, like a contract, it suggests that the parties intend to enter into a legal commitment with one another.

Data sharing agreements may cover one specific project or data exchange, or they can reflect a larger, ongoing initiative between partners with appendices developed for specific projects. DSAs can be developed between



two parties or multiple parties and may be inter-jurisdictional (e.g., between a school district and a health department or provider's office).

Memoranda of Understanding (MOU)

Unlike a DSA, an MOU is a non-binding agreement between two or more parties that outlines the terms and scope of the data sharing arrangement, as well as the roles and responsibilities of those involved. Used to express a convergence of will and outline an understanding among the parties, an MOU is most often used where parties do not intend to establish a legal commitment to each other. Rather, the document is intended to guide the relationship and document an agreement of principle and process. Where an MOU would suffice, parties often prefer them because MOUs avoid lengthy contract review processes and are therefore easier to execute.

Looking for Innovative Solutions

School districts can develop innovative, creative ways to enable data sharing while remaining compliant with the requirements of the law. In many situations, such as when data needs to be shared between schools and outside health care providers, obtaining parental consent is usually preferred, if not required. Nonetheless, schools and providers can obtain parental consent in a way that facilitates ongoing communication and avoids unnecessary delays. For example, Detroit Public Schools are piloting a "Consent to Release Health Information Form," which parents complete upon initial matriculation to Detroit public schools.²² The consent is designed to improve care coordination through free sharing of information among health partners ("need to know individuals"), such as the child's health care providers, the child's health insurance plan, state and local health departments, and school-based health service providers. This form can be used, for example, to allow school nurses to share information about a student's progress with her primary care physician and traumatic brain injury care specialists. (See Example #3, below.)


Oftentimes, schools can develop ways of improving processes and student care by utilizing data that are not considered PII or working within FERPA exceptions. For example, can the school's purposes be accomplished using de-identified or directory data, both of which can be shared more easily under FERPA? Can the party receiving the data be deemed a school official with a legitimate educational interest under the outsourced institutional services exception? Contact the Network for Public Health Law for assistance in thinking through innovative solutions to data sharing challenges.

Examples of Sharing Education Record Data

The following examples are designed to bring to life the information presented in this guide by applying it to real-life situations in a school setting. For each example, we will explore the answers to the questions to be asked when creating a data sharing arrangement.

I. Sharing data with immunization registries to combat the measles outbreak

Health care providers have watched with concern as the incidence of measles in the United States increased to the highest number of reported cases in more than 25 years.²³ Many states maintain immunization registries that can prove invaluable to combat an epidemic. Open communication among health departments, health care providers, and schools is important to surveillance and prevention of infectious disease outbreaks. While public health law researchers emphasize the importance of coordination between immunization information systems and school immunization records policies,²⁴ the complex web of federal, state, and local-level policy regarding such information sharing is prohibitive. For example, even in states where state law allows schools to disclose PII to state immunization registries, FERPA does not (without parent permission).²⁵ Also, while HIPAA—which governs



information sharing by health care providers and other covered entities—allows certain data sharing for public health purposes, FERPA does not.

What is the purpose for the data sharing? As places where large groups of vulnerable children gather every day, schools have an interest in sharing vaccination data with health departments, health care providers, and state immunization registries to monitor and prevent outbreaks of communicable diseases.

Who are the parties involved? Schools, health care providers, state immunization registries, and state/local health departments

What specific types of data are involved? Student immunization records

Which laws apply? Student health records (including immunization records) that are maintained by the school are subject to FERPA.²⁶ FERPA does not contain a general public health exemption, and the FERPA exemption that allows disclosure of PII to protect the “health or safety of the student or other persons” applies to emergency situations and is “strictly construed.”²⁷ Parental consent is therefore required to share immunization data in nonemergent situations. Minnesota and Michigan have taken innovative approaches to this problem with different levels of success. Minnesota encourages its school districts to obtain parental consent during enrollment open houses.²⁸ Michigan had developed an “opt out” process, whereby parental consent is presumed unless the parent unchecks a “FERPA No Consent” box.²⁹ However, the U.S. Department of Education issued a guidance letter in March 2019 that opined that a “‘FERPA No Consent’ checkbox as a means of obtaining consent to disclose PII from a student’s education record to a third party does not comply with FERPA’s consent requirement.”³⁰

What kind of agreement do you need? Because each of the parties involved is subject to federal law, a DSA or MOU is not necessary. A DSA may be required if a school district decides to contract with a third party to collect and transmit the immunization data to the state registry or health department. In this case, a DSA would be appropriate, and the FERPA “outsourced institutional services” exemption would likely apply.

II. Improving care by coordinating services with health departments and Medicaid


In 2014, the District of Columbia Public Schools entered into an innovative data sharing arrangement with the D.C. Department of Health and the D.C. Department of Health Care Finance (the District’s Medicaid agency). This arrangement is instructive of a compelling public health purpose for sharing educational data, and how schools can enter into such arrangements for the benefit of their students while remaining in compliance with FERPA.

What is the purpose for the data sharing? The purpose of this data sharing arrangement is to integrate education data (e.g., chronic absenteeism, health services delivered in school) with existing public health accountability systems in order to improve delivery of services to children and adolescents attending D.C. Public Schools, eliminate duplication of efforts, and harness the power of surveillance to identify the “schools with the greatest gaps in service utilization and highest Medicaid enrollment.”³¹

Who are the parties involved? D.C. Public Schools (DCPS), the D.C. Department of Health (DOH), and the D.C. Department of Health Care Finance (DHCF)

What specific types of data are involved? Student enrollment list, health services data (including date of last well-child visit and dental visit), attendance records, student immunization records, Medicaid enrollment status

Which laws apply? The components of the municipal departments that handle health care information would be HIPAA-covered entities, and HIPAA does allow data sharing for public health purposes.³² Student records are subject to FERPA,³³ which does not contain a general public health exemption.³⁴ Because the DOH and the DHCF are performing a service or function on behalf of DCPS and are under the “direct control” of the school district regarding the use and maintenance of education records (by mutual agreement), these departments qualify as “school officials” with a legitimate educational interest in the data.



What kind of agreement do you need? The District executed a Memorandum of Agreement (MOA), another name for an MOU, which outlines the purpose of the data sharing arrangement; the type(s) of data to be shared; responsibilities of the parties; terms of data use, maintenance, and disclosure; and a time limit for the arrangement (5 years).³⁵

III. Monitoring a student returning to school after Traumatic Brain Injury (TBI)

Open communication among school personnel, the student's IEP or Section 504 plan team, families, concussion management team, and outside health care providers is essential to ensuring that post-concussion adjustments and clinical care instructions are understood and followed by school personnel, and that outside providers are aware of issues at school that might require adjustments to the care plan. Healthcare providers are subject to the HIPAA Privacy Rule, which allows disclosures for "treatment purposes," for example, to school nurses. FERPA, which governs the sharing of student health information collected and maintained at school, does not contain a treatment exemption. School nurses can exchange information to "clarify" physician treatment orders. Beyond that, parental permission is needed to authorize ongoing communication. How can schools ensure that a child's concussion care team members, both inside and outside the school, are able to communicate to ensure the highest quality of care for students returning to school after a TBI?

What is the purpose for the data sharing? To ensure communication among a student's concussion care team at school, including her teachers, and her health care providers outside of school. Continuity of care will result in quicker and safer recovery and school reentry, resulting in better outcomes physically, academically, and socially.

Who are the parties involved? School personnel (e.g., school nurse, certain members of the administration, concussion care team, IEP or 504 team, teachers, school psychologist, therapist, coaches/athletic trainers); parents/guardians; and the student's pediatrician and other outside providers (e.g., neurologist, psychologist, therapists).

What specific types of data are involved? Data relevant to a student's recovery from TBI in a school setting, which may include grades, physical exam results, therapy results, IEP/504 plans, accommodations, observations of the student's progress or behavior by school personnel, etc.

Which laws apply? Outside health care providers are subject to HIPAA and state medical records privacy laws. School personnel are subject to FERPA and state student privacy laws. Because privacy and disclosure provisions under these laws differ, data sharing arrangements must comply with both. In this situation, none of the FERPA exemptions apply, so parental consent must be obtained for the school to share student PII (beyond a nurse "clarifying" an outside provider's treatment instructions). Thus, the best option here would be to develop a parental consent form that is both HIPAA and FERPA compliant, which outlines the types of information to be shared among which parties. For students with ongoing medical care needs in school, such a consent form could be executed with a stipulation that it will expire upon the student's graduation, transfer to a different school, or upon termination by the parent.

What kind of agreement do you need? Usually, a DSA or MOU is a best practice to outline the roles and responsibilities of the parties with regard to the data to ensure compliance with state and federal law. While a DSA or MOU is not required in this particular situation (because each party is already bound to adhere to the requirements of either HIPAA or FERPA), such an agreement would advance the goal of transparency and confirm the intent of the parties to follow the law and exercise professionalism and good stewardship.



Conclusion

Improving communication and data exchange between schools and health care providers is important to improving academic and health outcomes for children and adolescents. Federal law does not restrict the sharing of non-PII, such as de-identified data, or directory information that is not linked to other data. FERPA regulations allow schools to share PII *with* parental consent, so obtaining consent is often the best approach for ensuring efficient and effective communication. However, where obtaining parental consent is not practicable, state and federal law does allow for sharing of PII under certain exceptions that can help to ensure continuity of care, improve collaboration and communication among health care providers, and address public health emergencies. Whether data sharing occurs with or without parental consent (under a legal exception), agreements among all parties with access to the data are important to ensure that student health information is protected in compliance with the law.

SUPPORTERS

The Network for Public Health Law is a national initiative of the Robert Wood Johnson.



Robert Wood Johnson Foundation

This document was developed by Kerri McGowan Lowrey, JD, MPH, Deputy Director and Director for Grants & Research, Network for Public Health Law—Eastern Region, and reviewed by Erin Maughan, PhD, MS, RN, PHNA-BC, FNASN, FAAN, Director of Research, National Association of School Nurses. The Public Health Law Network provides information and legal technical assistance on issues related to public health. The legal information and assistance provided in this document does not constitute legal advice or legal representation. For legal advice, please consult specific legal counsel.

Updated January 2020

¹ 45 CFR § 160.103 (2)(i) and (ii). Note that some schools are not subject to FERPA (i.e., private/religious schools that receive no funding from the U.S. Department of Education). Nurses practicing in such schools, which also qualify as HIPAA-covered entities, must comply with HIPAA. Nonetheless, the tenets for legal data sharing practices are consistent.

² “Personally identifiable information” is any information that, alone or in combination with other information, could be used to identify a specific student. PII includes but is not limited to the student’s name, the names of the student’s family members, address, personal identifiers such as the student’s social security number and birth date, and any information that is linkable to a specific student. See Family Educational Rights and Privacy Act Regulations, 34 CFR Part 99 (<https://www2.ed.gov/policy/gen/guid/fpco/pdf/ferparegs.pdf>).

³ Under FERPA, education records may be disclosed without consent to: 1) school officials with legitimate educational interests, 2) schools in which a student seeks or intends to enroll, 3) state and local officials pursuant to a state statute in connection with serving the student under the juvenile justice system, 4) comply with a judicial order or subpoena (reasonable effort to notify parent or student at last known address), 5) accrediting organization, 6) parents of dependent student, 7) authorized representatives of federal, state, and local educational authorities conducting an audit, evaluation, or enforcement of education programs, 8) organizations conducting studies for specific purposes on behalf of schools, 9) in a health or safety emergency, 10) child welfare agency or tribal organization for those children in foster care, and 11) directory information.

⁴ See, Network for Public Health Law, *Data Privacy in School Nursing: Navigating the Complex Landscape of Data Privacy Laws (Part I)*, online at: https://www.networkforphl.org/_asset/tzqw3y/Data-Privacy-in-School-Nursing-Navigating-the-Complex-Landscape-of-Data-Privacy-Laws-Part-1.pdf.

⁵ For information on legal and practical ways of using de-identified data for public health purposes, as well as the Network for Public Health Law’s De-Identification Toolkit, visit: https://www.networkforphl.org/resources/topics_resources/health_information_and_data_sharing/de-identification_of_data/.

⁶ U.S. Department of Education, Data Sharing Toolkit for Communities, March 2016, <https://www2.ed.gov/programs/promiseneighborhoods/datasharingtool.pdf>.

⁷ Id.

⁸ [34 CFR § 99.37](#)

⁹ U.S. Department of Education, FERPA Frequently Asked Questions, <https://www2.ed.gov/policy/gen/guid/fpco/faq.html#q4>.

¹⁰ The Individuals with Disabilities Education Act (IDEA), a federal special education law, requires educational entities to develop an individualized education program (IEP) for each student with a disability to ensure that the student's unique needs are met in an academic setting. Individuals with Disabilities Education Act, 20 U.S.C. § 1414d (2004). A Section 504 Plan is developed pursuant to Section 504 of the Rehabilitation Act of 1973, a federal civil rights law. Section 504 requires school district to provide a "free appropriate public education" (FAPE) to students with a disability. A Section 504 Plan ensures a FAPE for students with disabilities by providing accommodations, aids, and services that are designed to meet the student's individual educational needs. 29 U.S.C. § 794 (Section 504).

¹¹ See, e.g., National Forum on Education Statistics. (2010). Forum Guide to Data Ethics (NFES 2010–801). U.S. Department of Education. Washington, DC: National Center for Education Statistics, noting that "[w]hile laws set the legal parameters that govern data use, ethics establish fundamental principles of 'right and wrong' that are critical to the appropriate management and use of education data in the technology age."

¹² [34 CFR §99.31](#)

¹³ [34 CFR §99.31\(a\)\(1\)\(i\)\(B\)](#)

¹⁴ [34 CFR §99.33\(a\)](#)

¹⁵ Seattle Public Schools, Institutional Service Exemption to FERPA,

https://www.seattleschools.org/departments/communitypartnerships/data_access_for_cbos/institutional_service_exemption_to_ferpa.

¹⁶ Data Across Sectors for Health (DASH), *A Legal Approach to Sharing Health and Education Data*, May 2018. Online at: https://dashconnect.org/wp-content/uploads/2018/05/DASH-Bright-Spot_Chicago.pdf.

¹⁷ See, DASH, *Four Tips for Navigating Consent to Facilitate Data Sharing*, October 6, 2016, online at: <https://dashconnect.org/2016/10/06/four-tips-for-navigating-consent-to-facilitate-data-sharing/>.

¹⁸ See Privacy Technical Assistance Center (August 2015), U.S. Department of Education, *Responsibilities of Third-Party Service Providers under FERPA*, online at https://studentprivacy.ed.gov/sites/default/files/resource_document/file/Vendor%20FAQ.pdf.

¹⁹ U.S. DEPT OF HEALTH AND HUMAN SERVS. & U.S. DEPT OF EDUC., 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 RECORDS (Nov. 2008), <https://www2.ed.gov/policy/gen/guid/fpco/doc/ferpa-hipaa-guidance.pdf> at 6.

²⁰ The Checklist is available online at

https://www.networkforphl.org/resources_collection/2019/09/30/400/tool_checklist_of_information_needed_to_address_proposed_data_collection_access_and_sharing.

²¹ The U.S. Department of Education's Privacy Technical Assistance Center has issued a Written Agreement Checklist that contains helpful information on best practices and mandatory elements for drafting written agreements:

https://studentprivacy.ed.gov/sites/default/files/resource_document/file/Written_Agreement_Checklist.pdf

²² See Elliott Attisha and Kerri Lowrey, "Data Privacy and Sharing in Schools and How It Can Support a Healthy Learning Environment," Network for Public Health Law Data Summit, Plymouth, Michigan, October 3, 2019.

²³ See, e.g., USA Today, Measles outbreak: As students head back to school, US and world officials warn about risks, August 22, 2019. Online at <https://www.usatoday.com/story/news/nation/2019/08/14/measles-outbreak-could-worsen/1998544001/>.

²⁴ Hedden EM, Jessop AB, Field RI. An education in contrast: state-by-state assessment of school immunization records requirements. *Am J Public Health*. 2014;104(10):1993–2001. Online at <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4167093/>.

²⁵ States may pass laws that are more protective than FERPA or HIPAA, but laws that are less restrictive are preempted by federal law.

²⁶ 20 U.S.C. §1232g(a)(4)(a).

²⁷ 20 U.S.C. § 1232g(b)(1)(I). Regulations implementing this statute note that this section is to be "strictly construed." 34 C.F.R §§ 99.31(a)(10) and 99.36. See also, LeRoy Rooker, Director, Family Policy Compliance Office, US Department of Education, Letter to Ms. Martha Holloway, State School Nurse Consultant, Department of Education, Montgomery, Alabama, February 25, 2004.

²⁸ Minnesota Department of Health's sample school consent language for data sharing with state immunization registry can be found online at <https://www.health.state.mn.us/people/immunize/miic/privacy/ferpa.html>.

²⁹ "FERPA No Consent" Checkbox in MCIR/SIRS and FORMS, Frequently Asked Questions, Information for Schools, https://www.mcir.org/wp-content/uploads/2019/08/FAQ_for_FERPA_8-21-2019-pdf.pdf.

³⁰ Hawes, Michael B. Letter to Michigan Senator Tom Barrett (March 27, 2019). The "FERPA No Consent" checkbox method of obtaining parental consent for educational record disclosure does not satisfy consent requirements under FERPA, which requires that a consent for disclosure of education records be signed and dated and specify the records that may be disclosed, state the purpose of the disclosure, and identify the party or class of parties to whom the disclosure may be made. 34 CFR § 99.30. Available online at https://studentprivacy.ed.gov/sites/default/files/resource_document/file/Michigan%20immunization%20response_508-compliant.pdf.

³¹ Healthy Schools Campaign, Washington, D.C., <https://healthyschoolscampaign.org/policy/sharing-data-meet-student-health-needs-washington-d-c/>.

³² 45 CFR 164.512(b)(1)(i) (Covered entities may disclose PHI to public health authorities that are legally authorized to receive such reports for the purpose of preventing or controlling disease, injury, or disability.) and 45 CFR 164.512(b)(2) (Public health authorities that are also covered entities may use or disclose PHI for public health purposes.)

³³ 20 U.S.C. §1232g(a)(4)(a).

³⁴ 20 U.S.C. § 1232g(b)(1)(I). Regulations implementing this statute note that this section is to be "strictly construed." 34 C.F.R §§ 99.31(a)(10) and 99.36. See also, LeRoy Rooker, Director, Family Policy Compliance Office, US Department of Education, Letter to Ms. Martha Holloway, State School Nurse Consultant, Department of Education, Montgomery, Alabama, February 25, 2004.

³⁵ The Memorandum of Agreement can be viewed online at <https://www.ncemch.org/IAA/states/2015-IAAs/DC-IAA.pdf>. See Section VIII Confidentiality and Data Protection for the language of the "outsourced services" exception and how it was operationalized in this agreement.

Appendix A. Sample Data Sharing Agreement

The Allied School District (“School District”) and the New State Department of Juvenile and Family Services (“Juvenile Services”) enter into this Data Sharing Agreement (“Agreement”) and are referred to herein as the “Parties.” The Parties commit to each other as set forth below.

I. Purpose

The Allied School District has been awarded a grant by the United States Department of Justice (U.S. DOJ) to develop and implement a Stay in School 2020 Program (hereinafter the “Program”). The goal of the Program is to improve academic outcomes and interrupt the “school-to-prison pipeline” by aligning the educational and social needs of students. The purpose of this Agreement is to define roles and responsibilities under the Program as they relate to data use and data sharing.

II. Period of Agreement

The period of the agreement will extend from _____ until _____.

III. Justification for Disclosure and Use

The ability of the Parties to share students’ academic, disciplinary, social services, and correctional data is essential to carry out the Program. Furthermore, the ability of the School District to share such data with the U.S. DOJ is necessary in order to fulfill the reporting and evaluation requirements under the award.

IV. Roles and Responsibilities

The School District will perform the following activities:

1. Collect and maintain student-level educational data, including academic success measures, attendance records, and disciplinary records;
2. Act as custodian of all data throughout the life of the Program and ensure that data are stored in compliance with applicable state and Federal law;
3. Perform analyses of Program data using a secure data analysis platform, and share results with Parties that are relevant to improving services to justice-involved students;
4. Facilitate conversations among the Parties to improve collaboration and enhance data sharing efficiency; and
5. Compile and report data to U.S. DOJ in accordance with requirements of the award.

The New State Department of Juvenile and Family Services will perform the following activities:

1. Collect and share social services, referral, and correctional data elements described in the award scope of work.
2. Store, maintain, and transfer social services, referral, and correctional data in compliance with applicable state and federal laws.

V. Description of Data

Data covered under this Agreement includes all academic, disciplinary, social services, and correctional data collected by the Parties for purposes of the Program. *[If data will be collected using a survey or other instrument, include a description of that instrument here, as well.]*

VI. Method of Data Access or Transfer

The Parties will establish specific safeguards to assure the confidentiality and security of individually identifiable data. Such safeguards will be consistent with the rules and standards promulgated by Federal statutory requirements regarding the electronic transmission of identifiable information. Data will be transferred between the parties utilizing a secure data portal developed for purposes of the Program.

VII. Location of Matched Data and Custodial Responsibility

The Parties mutually agree that the School District will be designated as custodian of the data and will be responsible for the observance of all conditions for use and for establishment and maintenance of security agreements to prevent unauthorized use. The data will be stored [describe how data will be stored]. Data will be maintained _____ [describe how data will be maintained].

Except as authorized in writing, no data covered by this Agreement shall be disclosed, released, revealed, showed, sold, rented, leased, loaned, or otherwise have access granted to any person. Access to the data covered by this Agreement shall be limited to the minimum number of individuals necessary to achieve the purpose of the Program and to those individuals on a need to know basis only.

Summary results of data matching, which are those items that cannot be used to identify any individual, may be shared. Stripping of an individual's name or individual identification number does not preclude the identification of that individual, and therefore is not sufficient to protect the confidentiality of individual data.

VIII. Confidentiality

The Parties agree to establish appropriate administrative, technical, and physical safeguards to protect the confidentiality of the data and to prevent unauthorized use or access to it. The safeguards shall provide a level and scope of security that is not less than the level and scope of security established by the Office of Management and Budget (OMB) in OMB Circular No. A-130, Appendix III – Security of Federal Automated Information System, which sets forth guidelines for security plans for automated information systems in Federal agencies.

The Parties will also ensure that data are collected, stored, and transferred in compliance with applicable state and Federal laws, including, where appropriate, the Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99), the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. 1320d et seq.; 45 CFR parts 160 and 164), the Federal Privacy Act, the Confidentiality of Alcohol and Drug Abuse Patient Records (42 U.S.C. 290dd-2, as implanted at 42 CFR part 2); and [cite relevant state law(s)].

IX. Disposition of Data

The Parties will destroy all confidential information associated with actual records as soon as the purposes of the Program have been accomplished and notify each other to this effect in writing. When the Program is complete, these parties will:

1. Destroy all hard copies containing confidential data (e.g., shredding or burning);
2. Archive and store electronic data containing confidential information off line in a secure place, and delete all on line confidential data; and
3. All other data will be erased or maintained in a secured area.

X. Data-Sharing Program Costs

Costs associated with development of the secure data portal are provided under the award. There are no additional costs anticipated for this data sharing arrangement.

XI. Amendments

Each Party may amend this Agreement only by written amendment, signed by all Parties signatory hereto. However, any individual Party may enter into separate agreements to provide services additional to those described herein, provided that such agreement does not conflict with the terms specified in this Agreement.

XII. Signatures

In witness whereof, the Parties' authorized representatives attest to and execute this Agreement effective with this signing for the period set forth in Article II.

By: _____

Date: _____

[Name]

Superintendent

Allied School District

By: _____

Date: _____

[Name]

School Nursing Coordinator

Allied School District

By: _____

Date: _____

[Name]

Commissioner

New State Department of Juvenile and Family
Services

Appendix B. Sample Consent Form for Disclosures by School District to Health Department

The *[School District]* will seek to keep students healthy and safe this fall and through the school year. As part of this effort, we will be collaborating with the *[Local]* Health Department to help track student absences. This effort will enable us to identify unusual clusters of disease and provide important information to the school community, particularly to students at high risk, about certain illnesses. These efforts will also help the health community assess the spread of disease and allocate scarce medical resources.

Pursuant to the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g, parental consent is required before personally identifiable information from your child's education records may be disclosed to *[Health Department]*, absent a health or safety emergency or another exception to the requirement of consent. If your child is age 18 or over, he or she is an "eligible student" and has to provide consent for disclosures of information from his or her education records.

Please note that information about your child may be shared with the Health Department without your consent if school officials determine that there is a significant and articulable threat to the health or safety of your child or other individuals and that the Health Department needs to know the information to protect the health or safety of your child or other individuals.

I, _____, hereby agree to allow *[School District]* to disclose *[Specify Data or Records]* related to *[Student's Name]* to *[name of Health Department]* for the purpose of *[state purpose of disclosure]*. This consent form is valid for as long as student is matriculated in *[School District]* schools.

You may withdraw your consent to share this information at any time. This request should be submitted in writing and signed.

Signature of Parent, Guardian, or Eligible Student

Date