DATA SHARING & PRIVACY DEMANDS IN EDUCATION:

HOW TO PROTECT STUDENTS WHILE SATISFYING POLICY & LEGAL REQUIREMENTS

NOVEMBER 2019

CENTER FOR DEMOCRACY & TECHNOLOGY

A SERIES OF PAPERS ON STUDENT PRIVACY

ABOUT CENTER FOR DEMOCRACY & TECHNOLOGY

The Center for Democracy & Technology is a 501(c)(3) working to promote democratic values by shaping technology policy and architecture, with a focus on the rights of the individual. CDT supports laws, corporate policies, and technological tools that protect privacy and security and enable free speech online. Based in Washington, D.C., and with a presence in Brussels, CDT works inclusively across sectors to find tangible solutions to today's most pressing technology policy challenges. Our team of experts includes lawyers, technologists, academics, and analysts, bringing diverse perspectives to all of our efforts.

Learn more about our experts and the issues we cover: https://cdt.org/

ABOUT STUDENT PRIVACY

CDT's vision for the *Student Privacy Project* is to create an educated citizenry that is essential to a thriving democracy by protecting student data while supporting its responsible use to improve educational outcomes. To achieve this vision, CDT advocates for and provides solutions-oriented resources for education practitioners and the technology providers who work with them, that center the student and balance the promises and pitfalls of education data and technology with protecting the privacy rights of students and their families.

AUTHORED BY

Elizabeth Laird, Senior Fellow
Hannah Quay-de la Vallee, Senior Technologist

Cover and layout designed by Tim Hoagland

CENTER FOR DEMOCRACY & TECHNOLOGY

Data Sharing and Privacy Demands in Education: How to Protect Students While Satisfying Policy and Legal Requirements

Executive Summary

Any decision to share data, especially across agencies, requires careful deliberation and diverse stakeholder engagement to minimize unintended consequences to students and their families. Sharing data always involves risk, and potential harm to students and their families is not limited to inadvertent disclosures. It can also include violating parents'[1] and students' expectations, increasing administrative burden, and using data in biased manners that limit educational opportunities for students and potentially violate their civil rights.[2]

At the same time that practitioners and policymakers are considering if and when to share data, they are faced with legal requirements and policy demands that require sharing student information. Data is shared today across agencies to meet legal requirements, follow federal guidance, provide basic services to individuals, and support efforts to serve vulnerable students. Privacy efforts have largely been focused on ensuring data sharing is legally compliant, but protecting students requires more than legal compliance. This technical guide offers best practices to meet data sharing needs while protecting student privacy.

Education Data Sharing Policy and Legal Requirements

Data sharing is happening today as education practitioners share and receive data with other agencies to fulfill existing legal requirements and policy demands. In 2014, the Data Quality Campaign conducted a survey of states, and as Figure 1 illustrates, almost every state was sharing data across agencies. In the past five years, legal requirements and policy demands have only increased, and data sharing has expanded to keep pace.

State education agencies and school districts have discretion and may share data for a multitude of reasons. Regardless of when they may choose to share data, there are existing legal and policy demands that either require or strongly encourage practitioners to share data across agencies in order to:

- Administer funding;
- Comply with accountability laws;
- Provide basic services; and
- Serve vulnerable students.

[1] A note on terminology: This brief uses the term “parent” throughout for the sake of consistency with existing common terms like “parental consent.” This brief uses a broad definition of parent, including foster parents, legal guardians, adult students, and other responsible adults.

[2] *Civil Rights Principles for Safe, Healthy, and Inclusive School Climates*, October 2019, http://civilrightsdocs.info/pdf/education/School-Climate-Principles.pdf.

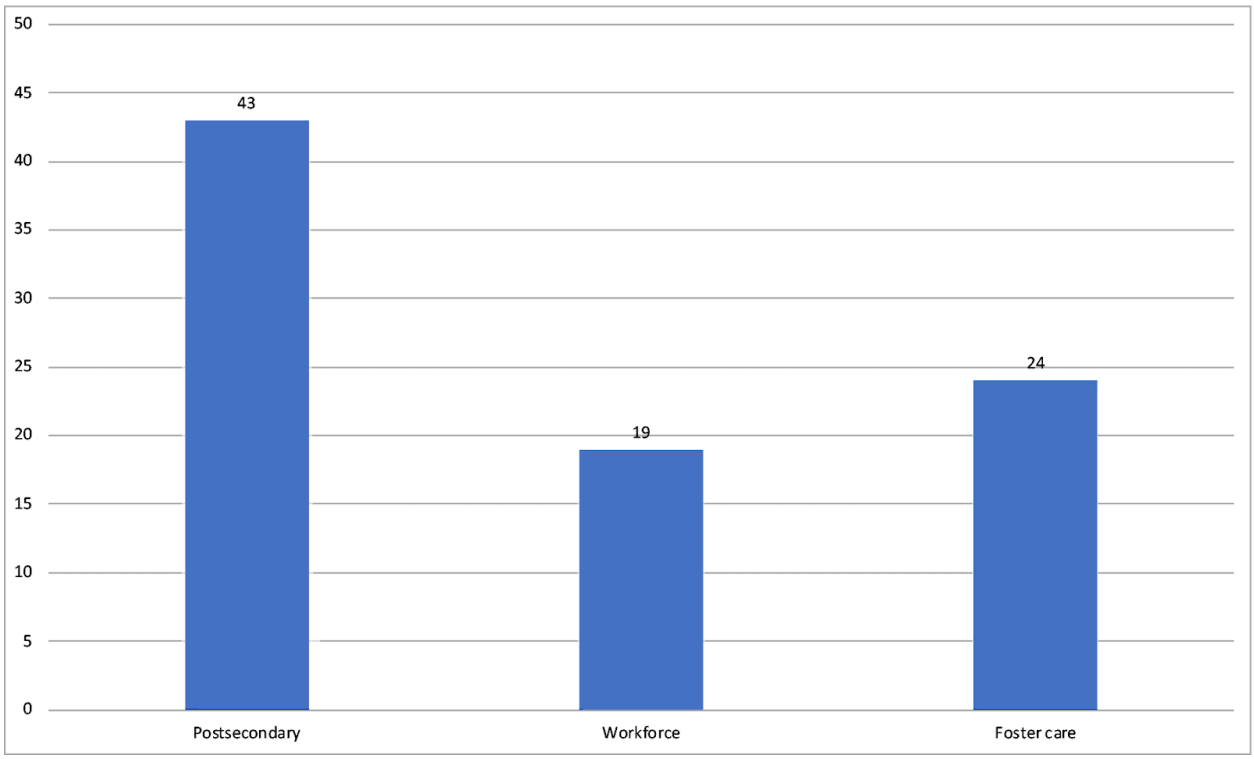

Figure 1: Number of States Sharing K-12 Data with Other Agencies[3] [4]

Administer Funding

State education agencies are required to analyze data and submit reports as a condition of receiving federal funding. Compiling some of these federal reports can require sharing data across agencies. For example, the EdFacts Initiative is led by the U.S. Department of Education, and one of its reporting requirements[5] is for states to provide information on college enrollment of their high school graduates. State education agencies do not typically collect or maintain data on college enrollment, so to provide this report, they need to get this data from other sources, which may include a separate state agency that oversees public postsecondary institutions.[6]

Additionally, the Carl D. Perkins Career and Technical Education Act of 2006 supports the "academic achievement of career and technical education students, strengthen[s] the connections between

[3] Data Quality Campaign, *Data for Action 2014: Paving the Path to Success*, November 2014, https://dataqualitycampaign.org/wp-content/uploads/2016/03/DataForAction2014_0.pdf.
[4] Data Quality Campaign & the Legal Center for Foster Care and Education, *Supporting Students in Foster Care*, May 1, 2015, https://dataqualitycampaign.org/wp-content/uploads/2016/03/DQC-Foster-Care-Mar24.pdf.
[5] U.S. Department of Education, *High School Graduates Postsecondary Enrollment File Specifications SY 2018-19*, https://www2.ed.gov/about/inits/ed/edfacts/eden/non-xml/fs160-15-3.docx.
[6] U.S. Department of Education, *Every Student Succeeds Act State and Local Report Cards Non-Regulatory Guidance*, January 2017, https://www2.ed.gov/policy/elsec/leg/essa/essastatereportcard.pdf.

secondary and postsecondary education, and improve[s] state and local accountability."[7] As a condition of receiving this funding, states are required to report annually on 13 core indicators of performance, four of which require sharing, linking, and analyzing K-12, postsecondary, and work data.[8]

Comply with Accountability Laws

The Every Student Succeeds Act (ESSA) is the primary federal school accountability law, a core component of which is ensuring "that vital information is provided to educators, families, students, and communities through annual statewide assessments that measure students' progress toward those high standards."[9] This entails public reporting on student groups, including but not limited to students in foster care, those experiencing homelessness, and those experiencing economic disadvantage.[10] State and local education agencies typically do not have sufficient information to accurately and comprehensively identify these student groups, so as a result, states are pursuing data sharing agreements with other agencies to analyze and report accurate, quality, and comprehensive data on these student groups.[11]

Provide Basic Services

The United States Department of Agriculture administers the National School Lunch Program, and has encouraged state and local education agencies to determine meal assistance eligibility through data sharing instead of via parental disclosure on eligibility forms.[12] This process, known as Direct Certification, was first used in 1986. Starting in 2004, states were required to use Supplemental Nutrition Assistance Program (SNAP) data to directly certify students to receive meal assistance. In 2010, 95% of students receiving SNAP were required to be certified through the direct certification data sharing process. Direct certification through Medicaid was also added.[13]

Serve Vulnerable Students

---

[7] U.S. Department of Education, *Carl D. Perkins Career and Technical Education Act of 2006*, March 2007, https://www2.ed.gov/policy/sectech/leg/perkins/index.html.
[8] U.S. Department of Education, *Perkins IV Accountability Requirements*, https://www2.ed.gov/about/offices/list/ovae/pi/cte/factsh/accntblty1-fs-080328qa-kc.doc.
[9] U.S. Department of Education, *Every Student Succeeds Act (ESSA),* https://www.ed.gov/essa.
[10] U.S. Department of Education, *Every Student Succeeds Act State and Local Report Cards Non-Regulatory Guidance*, January 2017, https://www2.ed.gov/policy/elsec/leg/essa/essastatereportcard.pdf.
[11] Kate Stringer, "ESSA Says State Report Cards Must Track How Many Students in Foster Care Are Passing Their Reading & Math Tests and Graduating High School. Only 16 Do," *The 74*, February 20, 2019, https://www.the74million.org/article/essa-says-state-report-cards-must-track-how-many-students-in-foster-care-are-passing-their-reading-math-tests-and-graduating-high-school-only-16-do/.
[12] U.S. Department of Agriculture Food and Nutrition Service, *Direct Certification in the National School Lunch Program: State Implementation Progress Report to Congress - School Year 2015-16 & School Year 2016-17*, October 2018, https://fns-prod.azureedge.net/sites/default/files/resource-files/NSLPDirectCertification2016.pdf.
[13] Alison Maurice, *Direct Certification Improves Low-Income Student Access to School Meals: An Updated Guide to Direct Certification*, Food Research & Action Center, November 2018, http://frac.org/wp-content/uploads/direct-cert-improves-low-income-school-meal-access.pdf.

Federal laws aimed at serving specific groups of students encourage and may require data sharing to coordinate services. For example, the Uninterrupted Scholars Act is aimed at supporting students in foster care. This law amends the primary student privacy law, the Family Educational Rights and Privacy Act (FERPA), to allow educational agencies to share student data without parental consent with a caseworker ''when such agency or organization is legally responsible."[14]

Governance and Technical Considerations for Data Sharing Across Agencies

As state and local education agencies share data, especially across agencies, there are important governance and technical considerations that can support privacy and security in the process. Each instance of data sharing will likely be unique, but to mitigate risk and respect individuals' privacy rights, any data sharing initiative should, at a minimum, incorporate best practices related to:

- Governing data sharing across agencies;
- Transferring data; and
- Matching and integrating data.

Governing Data Sharing Across Agencies

Because transporting, sharing, and integrating data can pose risks to students' well-being and privacy, organizations that want to share data should implement strong data governance policies and practices to preserve privacy and security. According to the Institute of Education Science's Statewide Longitudinal Data Systems Grant Program, data governance is "the overall management of data, including its availability, usability, integrity, quality, and security."[15] A robust data governance system can help keep students' data safe by addressing issues such as ensuring that someone at the organization is explicitly tasked with supporting students' privacy, to prevent employees from mishandling data due to lack of clear policies or training; developing and enforcing clear policies for when and how to delete data, to limit the possibility of unnecessary but potentially harmful permanent records for students; following best practices when transferring or porting data, to avoid data breaches; and conducting training and regular audits, to ensure that everyone follows the policies. Although these issues are relevant whenever an organization collects or uses data, there are also data governance concerns that are especially germane to sharing data, such as how to manage student and parent engagement, how to ensure that students and families understand how their data is used and shared, and issues that may arise with data sharing agreements.

Additionally, it is crucial to remember that data governance is never complete. Technology, community

[14] U.S. Department of Education, *Guidance on the Amendments to the Family Educational Rights and Privacy Act by the Uninterrupted Scholars Act*, May 2014, https://www2.ed.gov/policy/gen/guid/fpco/ferpa/uninterrupted-scholars-act-guidance.pdf.

[15] Institute of Education Sciences (IES) Statewide Longitudinal Data Systems (SLDS) Grant Program, *SLDS Issue Brief: Communicating the Value of Data Governance*, U.S. Department of Education, December 2017, https://nces.grads360.org/services/PDCService.svc/GetPDCDocumentFile?fileId=28771.

values, and organizational needs evolve over time, so data governance should be an active consideration throughout the life of a sharing partnership to ensure that policies and practices grow in parallel. Consequently, this section will discuss general data governance questions and those unique to the data sharing process. Many of these questions will apply both to the partner organizations that are sharing data and to any third parties or vendors involved in the process.

- ***How will stakeholders be engaged in the sharing process?***

  Data integration is not just relevant to the data stewards themselves. Students, families and teachers all have a vested interest in how data is shared and used. Engaging these stakeholders, both when discussing and designing a sharing plan and throughout the sharing program, can help ensure that their perspectives are understood and that any concerns they might raise can be addressed. In order to reap the full benefits of engagement, it is important to be transparent and evenhanded. Parents should be made aware of the potential benefits and pitfalls of the program so that they can provide relevant and helpful feedback and understand the trade-offs being made.

  Depending on the nature of the program, it may be unfeasible to get parent feedback on implementation details, as parents may not have the expertise necessary to weigh in on the operational components. This does not absolve the sharing organizations from doing robust family engagement, but rather requires them to be thoughtful about how they do that engagement. One approach in this situation is to engage with parents about the goals of the program (to ensure the program meets their needs), the overarching principles that will govern how student data will be handled and used (so that organizations do not find themselves drifting towards questionable data use even in the service of a noble goal), and the methods for measuring and communicating outcomes (so that parents can see for themselves whether the program is effective, even if they cannot be involved in the technical details).

  Developing buy-in from families is an important part of stakeholder engagement (whether that engagement is done at a principles level or a more detailed level). This may mean adjusting or even canceling the program if organizations find that families are unhappy with or concerned about the program. Parental buy-in is particularly important in situations where schools are using an exception to federal and/or state student privacy legislation that does not require parental consent, since in this context parents do not have a way to avoid sharing data, even if they disagree with the program. Even if using a parental consent model, however, it is still important to engage parents to ensure the program meets their needs, so they don't feel they are choosing between begrudgingly consenting and missing out on services, and so that if they do consent, they understand what they are consenting to and how it will serve their child.

- ***How will decisions about data sharing be made?***

  Establishing a formal data governance structure for making decisions about the program, including ensuring that someone at the organization is explicitly tasked with supporting

students' privacy,[16] 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. Establishing an explicit structure for making decisions should be a continuation of the stakeholder engagement process, as this governance structure should be built to ensure that the principles and goals developed through family engagement are kept central to all decisions made about the sharing program.

A data governance structure incorporates a number of components, such as a formal process around decision-making, standardized procedures and policies, and data access management. Several organizations, such as the Privacy Technical Assistance Center, offer further guidance on establishing a data governance framework.[17]

- ***How will the sharing organizations communicate with stakeholders?***

  In addition to engaging stakeholders early on, organizations should develop a framework for communicating throughout the process, such as a blog, newsletter, or other forum, in order to continue informing families and receiving feedback as the sharing program evolves and new families enter the program. This forum should be accessible to all parents, as things like town hall-style meetings likely will not be sufficient as not all parents will be able to attend. Communications should be made available in the range of languages spoken by parents and guardians. These steps will provide a channel of communication for feedback as long as the sharing program is in place, and will help ensure that new students and families are aware of the program and able to understand how their information will be used.

- ***What are the goals and success metrics for sharing data?***

  Having explicit goals for the data sharing program is important, as it defines a scope for the sharing and provides a framework for determining if the data sharing program is successful. These goals should be used to develop concrete success metrics that can be used to evaluate the efficacy of the program, and determine if and how the program needs to be adjusted, or even if it should be discontinued. These goals and metrics should also be communicated with stakeholders through the channels discussed above.

---

[16] Elizabeth Laird, *Chief Privacy Officers: Who They Are and Why Education Leaders Need Them*, Center for Democracy & Technology, January 2019, https://cdt.org/files/2019/01/Student-Privacy-Chief-Privacy-Officer-Issue-Brief.pdf.

[17] 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, and 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.

- ***How does the data sharing agreement prescribe use limitations for the shared data?***

  Sharing data cedes much of the control over how it is used, and exposes students to additional risk that the data will be used in a way that harms them. One approach to mitigate this risk is to incorporate use limitations, such as restrictions on publication, resharing, or reuse of the shared data, into the data sharing agreement. This way, partner organizations understand how the data may be used and who is allowed to access it, and agree to respect those limitations for the shared data.

- ***Who will be responsible for developing and adhering to a deletion and retention schedule for shared data?***

  Sharing data means that the responsibility for managing a deletion and retention schedule is now distributed across all organizations that have access to the data. Organizations have to agree about deletion timelines and methods in order for each individual organization's retention schedule to be meaningful. For instance, if a school shares data with a service provider, and that school says it deletes discipline information after two years but the service provider retains it for five years, the school's retention policy is far less meaningful for students and families because that data continues to exist and is capable of affecting the student. For a more in-depth discussion of this issue, see CDT's prior work on data deletion in education.[18]

- ***How will an organization evaluate how well its partner organization is adhering to the terms of the data sharing agreement?***

  It is important for organizations to ensure that their sharing partners are committed to and capable of meeting the terms of the sharing agreement. To this end, partner organizations may want to incorporate compliance measures into their sharing agreement. These measures can take a variety of forms, from requiring partner organizations to receive training on best practices for handling data, to mandating executive-level engagement during signing and enforcement of the agreement, to full-scale audit provisions for organizations handling particularly sensitive information such as mental health data.

  If a partner organization is found to be remiss in meeting the agreement terms, but would still be a sufficiently valuable sharing partner, it may make sense to consider a compliance plan, such as requiring monthly reports on activities (what data was received, what data has been used and how, has any data been deleted, etc.).

- ***What protocols are in place for managing a breach of the data sharing agreement?***

  Organizations should create protocols for addressing the violation of a sharing agreement or other data incident such as an unauthorized disclosure (like a hack and leak of data or an

[18] Elizabeth Laird & Hannah Quay-de la Vallee, *Balancing the Scale of Student Data Deletion and Retention in Education*, Center for Democracy & Technology, March 2019, https://cdt.org/files/2019/03/Student-Privacy-Deletion-Report.pdf.

unapproved reshare to a third party). Those protocols should include clear roles for partner organizations. 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. In addition to a response plan, partner organizations should also determine who is responsible for providing remedies in the event of a breach, and communicate that to families so they know where to go for assistance.

- ***Is a warehouse approach or a federated model a better fit for the sharing context?***

  Infrastructure and software choices will likely impact the governance and management of data sharing programs. There are two primary approaches to structuring the storage and access of shared data: a warehouse approach, where all shared data is stored in a centralized location that each organization has access to, and a federated approach, where each organization maintains its own data and provisions access to the other organizations. Each of these carries a different set of benefits, risks, and considerations. The Privacy Technical Assistance Center has written guidance to help organizations determine which approach is best suited to their program.[19]

- ***How will organizations determine which people at each organization have access to the shared data?***

  It may be that each organization has latitude to determine who in their organization has access (though there are legal limitations that may restrict who is able to access certain data), or it may be that all the organizations determine access policies together to ensure that each accessing organization has sufficient governance controls in place.

- ***Does the data adhere to a data standard? Are all organizations using compatible standards?***

  Data standards are sets of rules governing the content and format of data so that it can be recognized by any system that adheres to those rules. This enables different schools and systems to receive student information and incorporate it into their own systems without having to adapt the information each time in an ad-hoc way. Sharing records and matching can be easier and less error-prone if partner organizations use compatible standards. If organizations are not compatible, it may be necessary to develop a program to transform data from one organization's standard to another's and vice versa to simulate compatible standards. In either of these approaches (compatible standards or a data transform), however, it is still important to ensure that the systems are not matching in error.

Transferring Data

Depending on the purpose of the data sharing, the sharing organizations may provide ongoing access to each other's data, or they may choose to share once or on an ad-hoc basis. In any case, using secure

[19] Privacy Technical Assistance Center, *Integrated Data Systems and Student Privacy*, U.S. Department of Education, January 2017, https://studentprivacy.ed.gov/sites/default/files/resource_document/file/IDS-Final.pdf.

methods to transfer the data can protect students from the harms that could arise from insecure transfers, such as a data breach.

For one-time data sharing, it is likely not worth the resources to set up a dedicated infrastructure like a data warehouse or secure file transfer feeds, but rather makes more sense for the organizations to exchange individual data files. For more regular data sharing, a more formal infrastructure like a warehouse or scheduled secure transfers can be easier to manage, since once the structure is in place it can be used on an ongoing basis rather than having to manage the transfer manually every time.

Regardless of how often data is shared, sharing should be done securely to protect students from the harm of breached or inaccurate data. (Many security measures like encryption serve to both keep the data private and safe from tampering). There is a number of different mechanisms for sharing data, from email to thumb drives to secure file transfers. These approaches range in how much security they provide. Email is not a secure method, and as such should not be used to transfer sensitive information. Thumb drives can be secure, but users must have a sophisticated understanding of how to handle them carefully (they must know how to properly erase them, must ensure they are not lost, etc.). Secure file transfers can be quite safe, however vendors should be evaluated on a case-by-case basis by someone with technical security expertise, as their security practices may vary.[20]

The following questions can help organizations determine how to structure their data transfer to suit their needs.

- ***Governance*: For ad-hoc or non-regular data sharing, what data governance procedures are in place?**

  For ad-hoc sharing, it may seem reasonable to decide how to transfer the data on an ad-hoc basis. However, this approach can easily lead to inconsistently secure sharing practices that depend on the judgment of the person managing that particular sharing instance. Providing and enforcing a general sharing policy and related protocol prior to sharing data will give employees guidance on what sharing methods are appropriate for different types of data. The policy and protocol should lay out how and when given data items should be shared, which may depend on factors like the sensitivity of the data, how often it is shared, and why it is shared. More sensitive data may require higher security practices like file transfer feeds. CDT's issue brief on data portability in education provides more discussion about different policies for transferring data.[21] Data transfers that happen at regular intervals might use an automated feed, while ad-hoc data sharing requires employees to initiate transfers, and thus necessitates guidance about when and how to do so. This policy and guidance should also include information about who employees should go to if they are unsure which data sharing protocol to use. CDT's prior

[20] Elizabeth Laird & Hannah Quay-de la Vallee, *Balancing the Scale of Student Data Deletion and Retention in Education*, Center for Democracy & Technology, March 2019, https://cdt.org/files/2019/03/Student-Privacy-Deletion-Report.pdf.
[21] Elizabeth Laird & Hannah Quay-de la Vallee, *Protecting Privacy While Supporting Students Who Change Schools*, Center for Democracy & Technology, June 2019, https://cdt.org/files/2019/07/2019-06-20-Portability-and-Privacy-Issue-Brief.pdf.

work on Chief Privacy Officers in education discusses some ways of building this capacity[22]. Laying out this governance may also prove helpful for identifying areas where an organization lacks the tools it needs to share data securely. This may help administrators make the case to develop or procure the appropriate technology.

- ***How often will data be transferred?***

  If data is to be transferred often between organizations, having a secure sharing infrastructure in place to automatically handle transfers and provisions may reduce both the burden of managing the process and privacy and security risks due to human error.

- ***How many organizations will the data be shared amongst?***

  If many organizations are involved in the data sharing, it may be impractical to manage the transfers on an ad-hoc or individual basis.

- ***How sensitive is the data, and how should data sensitivity be determined?***

  More sensitive data requires better security. Email could be appropriate for very low-sensitivity data, or data that is publicly available, but should only be used for highly-sensitive data with prior consent from family and not as a regular transfer method. While "sensitivity" may be useful for determining transfer methods, data sensitivity is context- and situation-dependent, and each person may have different feelings about which of their data are sensitive.

Matching and Integrating Data

When combining two data sets that have students in common, the sharing organizations need a way to match up subjects across data sets. For instance, they must be able to tell apart the records of two Rachel Horwitzes, or ensure that Jennifer Smith in data set A is the same person as Jennifer Marie Smith in data set B.

Organizations may face a trade-off between matching accuracy and amount of data shared. Sharing more data may result in a higher matching rate, but may also pose a risk to student privacy. The following questions will help organizations determine what approach they should take for matching data.

- ***Governance: How will organizations handle potential matches (i.e., two records may match, but more data is required to be confident they are a match)?***

  Potential but low-confidence matches are the fundamental issue when it comes to matching records. When handling these potential records, one approach would be to assume that two records are not a match, and create a new record. This is not ideal because having two separate

[22] Elizabeth Laird, *Chief Privacy Officers: Who They Are and Why Education Leaders Need Them*, Center for Democracy & Technology, January 2019, https://cdt.org/files/2019/01/Student-Privacy-Chief-Privacy-Officer-Issue-Brief.pdf.

records for the same student may lead to that student not receiving the support they need, as well as noise in the data set. Another alternative would be to assume that the records *are* a match. This is also not an ideal approach because if, in fact, the records belong to different students, this may lead to handling *both* of these students' cases incorrectly (i.e., providing unneeded services to one student while failing to provide services for the other). Also, as with creating duplicate records, it reduces the overall quality of the dataset. A better approach to handling a potential match is to request more data about the student. If the sending organization has additional information about that student that they did not send initially, that extra data may be able to provide clarity about whether or not the records are actually a match. When possible, this data should not be repurposed, and should be deleted after a match is found.

- ***Governance: How will incorrect matches be handled?***

  If a record was matched in error (meaning a record was considered a match, but it was later determined it was a separate person), organizations need a framework in place to undo the match and restore the two records. This requires having robust logs about changes and updates to records so any changes made to the record while it was incorrectly matched can be reverted. It may also mean re-examining any decisions that were made on the basis of that record.

- ***How many students' data are going to be matched?***

  For one-time or limited-time data matching over relatively small groups of students, matching by full name or name and date of birth may be sufficient (although this may be population-dependent). For larger groups, or ongoing integration, name matching is likely insufficient.

- ***What is the matching accuracy rate? How is it measured?***

  Knowing the matching rate can help organizations calibrate what information they need to collect from their partner organization. Organizations should periodically evaluate whether the data they are collecting is enough to ensure a relatively high match rate or, alternatively, if they are collecting unnecessary information (i.e., collecting less information would not substantially impact their match rate).

- ***What are the data elements of the shared records? Are there any data elements in common in the records to be matched?***

  Review the list of common elements. If there are non-sensitive unique identifiers like student ID numbers, those would be ideal for matching records. However, if there is no such element, it may be that a set of non-sensitive elements (such as name plus date of birth) can be combined to match records. If matching on very sensitive information like social security numbers, extra care should be taken to protect the students' sensitive data.

Conclusion

Any time data is shared, there is the potential for inadvertent disclosures, violation of expectations, increased administrative burden, and data used in biased manners that can limit educational opportunities for students. At the same time, state and local education agencies are required to share data to fulfill legal and policy demands. As the field continues to debate if and when to share data, important questions about how to do it in a privacy-protective manner that respects an individual's rights require answers now. Each data sharing effort has unique considerations, but at a minimum, any effort to share data should incorporate best practices related to governing data sharing across agencies, transferring data, and matching and integrating data to protect students while satisfying policy and legal requirements.