Yes, No, Maybe?

Legal & Ethical Considerations for Informed Consent in Data Sharing and Integration

Authors

Deja Kemp, JD, Amy Hawn Nelson, PhD, & Della Jenkins, MSSP

CONTRIBUTORS

Sharon Zanti, Jessie Rios Benitez, Emily Berkowitz, TC Burnett, Kristen Smith, Dennis Culhane

MAY 2023

AISP

Acknowledgments

Yes, No, Maybe? Legal & Ethical Considerations for Informed Consent in Data Sharing and Integration was created by Actionable Intelligence for Social Policy (AISP) with generous support from the Walton Family Foundation. We also recognize our Legal Advisory Workgroup, specifically Elliot Regenstein and Joy Royes, as well as Aaron Bean and Greg Bloom, who provided valuable review of this resource.

Suggested Citation

Kemp, D., Hawn Nelson, A., & Jenkins, D. (2023). *Yes, No, Maybe? Legal & Ethical Considerations for Informed Consent in Data Sharing and Integration*. Actionable Intelligence for Social Policy. University of Pennsylvania.

Disclaimer

This resource is not intended to constitute legal advice, nor is it a substitute for consulting with legal counsel. All information and content are for general informational purposes only. Readers should always consult with their attorney for specific legal advice.

Table of Contents

Introduction

Data sharing and integration are increasingly commonplace at every level of government, as cross-program and cross-sector data provide valuable insights to inform resource allocation, guide program implementation, and evaluate policies. Data sharing, while routine, is not without risks, and clear legal frameworks for data sharing are essential to mitigate those risks, protect privacy, and guide responsible data use. In some cases, federal privacy laws offer clear consent requirements and outline explicit exceptions where consent is not required to share data. In other cases, the law is unclear or silent regarding whether consent is needed for data sharing. Importantly, consent can present both ethical and logistical challenges, particularly when integrating cross-sector data. This brief will frame out key concepts related to consent; explore major federal laws governing the sharing of administrative data, including individually identifiable information; and examine important ethical implications of consent, particularly in cases when the law is silent or unclear. Finally, this brief will outline the foundational role of strong governance and consent frameworks in ensuring ethical data use and offer technical alternatives to consent that may be appropriate for certain data uses.

If you are new to this work, we encourage you to start with our *Introduction to Data Sharing and Integration*[1] text as a primer on the basics of sharing, integrating, and using administrative data held by government agencies and nonprofit organizations.

For more in-depth discussions of legal considerations related to data sharing and integration, including MOU templates and checklists, see our guide *Finding a Way Forward: How to Create a Strong Legal Framework for Data Integration*.[2]

What is consent? Why is this so complicated?

In the United States, there is no uniform definition of consent.[3] Instead, a patchwork of different federal and state laws each define consent differently, with varying requirements for when consent is needed. The common thread is generally that consent signifies that an individual has agreed to the use of their personal data.

The four federal statutes and regulations that most often govern the sharing and integration of individuals' data are the Privacy Act of 1974, the Health Insurance Portability and Accountability Act (HIPAA), 42 CFR Part 2, and the Federal Education Rights and Privacy Act (FERPA). In addition, states have statutes, regulations, ordinances, orders, and rules that may exceed federal protections related to data sharing. These federal and state laws apply to government-held data and protected data (e.g., health records, school records). The graphic below identifies some of the laws most likely to be relevant to the discussion.[4]

1 See **Hawn Nelson, A., et al. (2020b).**
2 See **Hawn Nelson, A., et al. (2022).**
3 Other countries have more comprehensive privacy frameworks than the US's decentralized approach. For example, the European Union (EU) passed the General Data Protection Regulation (GDPR) in 2018. The GDPR requires organizations to safeguard personal data of anyone in the EU. The GDPR also includes robust provisions on consent for to share data. See **Wolford, B. (n.d.).**
4 See **Hawn Nelson, A., et al. (2022).**

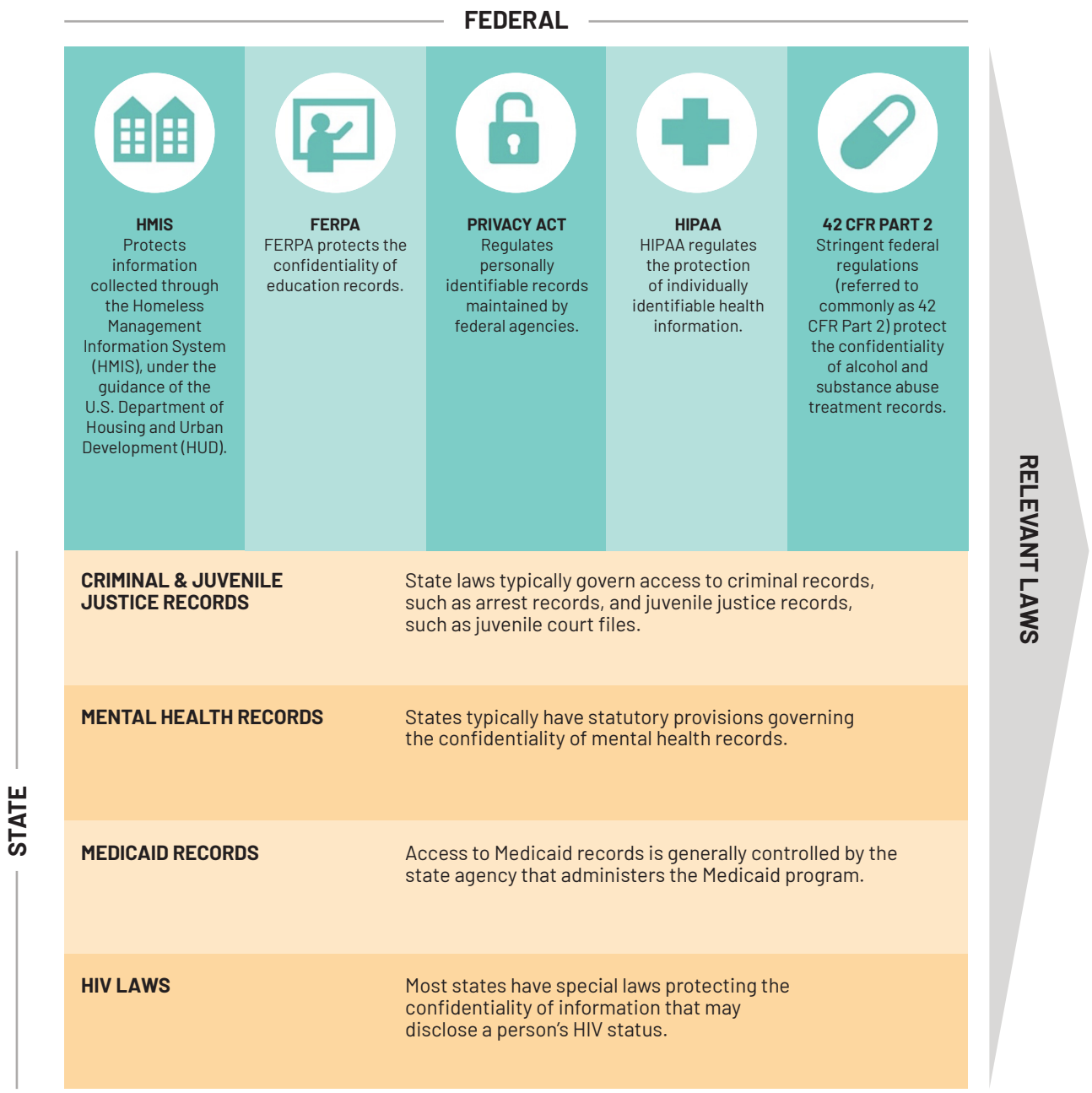


Figure 1: Federal and State Laws Relevant to Data Sharing

Under these federal statutes, as well as most state laws, whether consent is required to share data and how it must be obtained largely depend upon the type of data, who is accessing the data, and how the data will be used. The default rule is that identifiable information cannot be shared or disclosed unless consent is obtained, or an enumerated purpose or exception exists. For example, consent is expressly required to receive medical treatment or to participate in a study under the purview of an Institutional Review Board (IRB).[5]

5 The Common Rule is a 1981 rule of ethics regarding biomedical and behavioral research involving human subjects in the U.S. The Common Rule is the baseline standard of ethics by which any government-funded research in the U.S. is held, and mandates IRBs. The Common Rule, 45 CFR 46 Part A, outlines significant protections for human subjects in research governed by IRBs, which notably include informed consent. See 45 CFR 46, Part A.

Importantly, consent is not required when data are used for research, evaluation, and planning, provided the data meet criteria for exclusion or exceptions, such as when they are de-identified or anonymized prior to analysis.[6] Of course, determining whether a given data sharing use case meets the criteria for exclusion or exception under the relevant statute requires thoughtful analysis. This analysis should begin with data minimization—limiting data collection and use to what is necessary and required. If the sharing of personal information is deemed essential, then exceptions and consent frameworks must be considered.

Data minimization is the principle of limiting or minimizing the collection and disclosure of data to only what is necessary to accomplish a specific use. Data minimization is an important principle that supports privacy and ethical data use.

In the next section, we focus on HIPAA and FERPA, as these two statutes commonly govern data sharing and integration across human services. First, we summarize key exceptions under FERPA and HIPAA when consent is not required. Next, we examine requirements for consent. In subsequent sections, we discuss cases when the law is unclear or silent regarding consent, and offer tools and guiding questions to inform decision-making and support ethical data use.

Key exceptions to consent under HIPAA & FERPA

Under both HIPAA and FERPA, consent is not required where an enumerated exception exists. In these cases, we highly encourage the use of exceptions as a mechanism for ethical data use. These exceptions are there for a reason: there is minimal risk and often clear benefit to the individual whose data are being shared and to the general public.

De-identified & aggregate data

Many but not all of the exceptions have to do with the use of data that have been de-identified[7] or aggregated and therefore no longer contain personal identifiers. These data can be readily shared without consent **under both HIPAA**[8] **and FERPA**.[9]

For example, the sharing and use of even the most sensitive data, such as HIV status, is permissible if aggregated by a large geography (e.g., totaling HIV statuses across a state). As a result, we highly encourage the use of de-identified and aggregate data in lieu of consent whenever possible, as there is minimal privacy risk and may be significant benefit to data access and use. Of course, sharing and using de-identified data and aggregate data will still require a governance process and legal framework to ensure it is legal, ethical, and a "**good idea,**" and that there is clarity and transparency around decision-making.[10] Integrated data systems (IDS), also referred to as data trusts, data hubs, data collaboratives, or data intermediaries, provide this legal and governance framework.[11] IDS utilize identifiers for linkage, and can provide linked de-identified data for analysis. This allows data use to fall within enumerated exceptions.[12]

6 See, e.g., 45 CFR § 164.514 (b)(2).
7 Broadly, de-identification refers to an agreed upon process for removing identifiers from a data set prior to analysis or release.
8 HIPAA is prescriptive regarding methods of de-identification for protected health information (PHI) and allows for two methods to be used: "safe harbor" and "expert determination." See **Office for Civil Rights (2022, October 25).**
9 **Pierce West, S. (2016).** See 45 CFR 164.514; **Privacy Technical Assistance Center (2013, May).**
10 See **Hawn Nelson, A., et al. (2022).**
11 **Jenkins, D., et al. (2021).**
12 See **Privacy Technical Assistance Center (2017, January).**

The figures below outline common exceptions relevant to data sharing and integration.

HIPAA

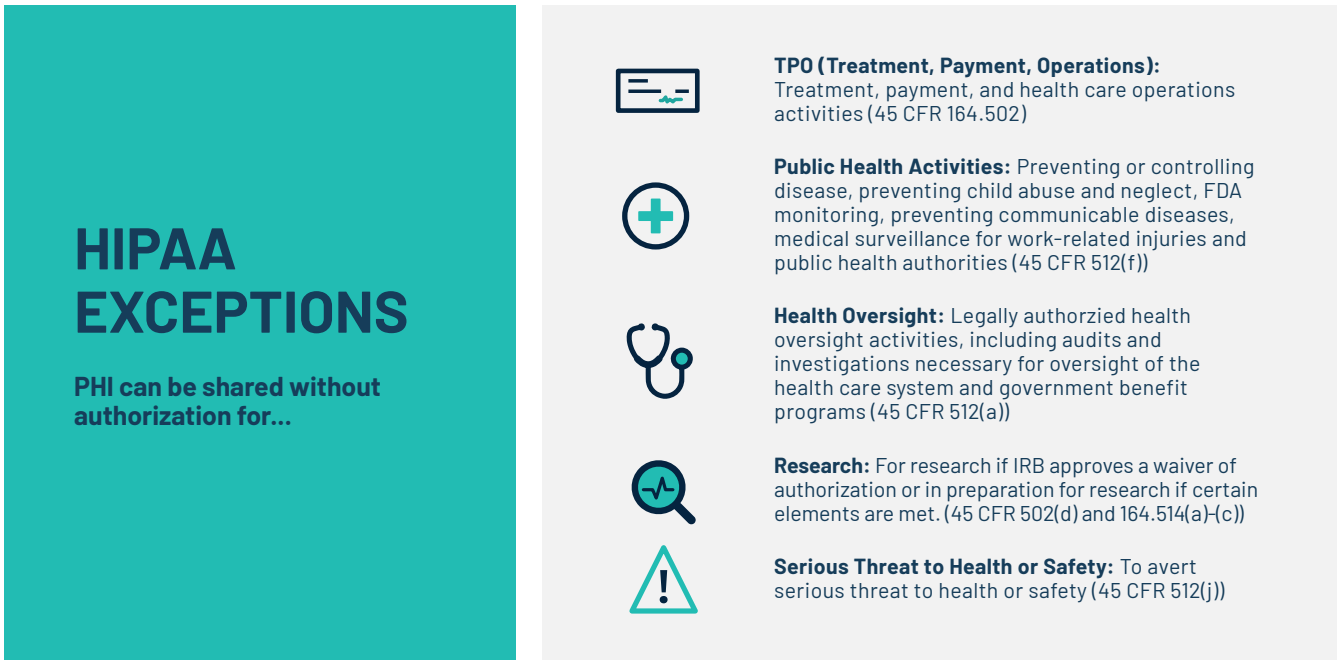


Figure 2a: HIPAA Exceptions

FERPA

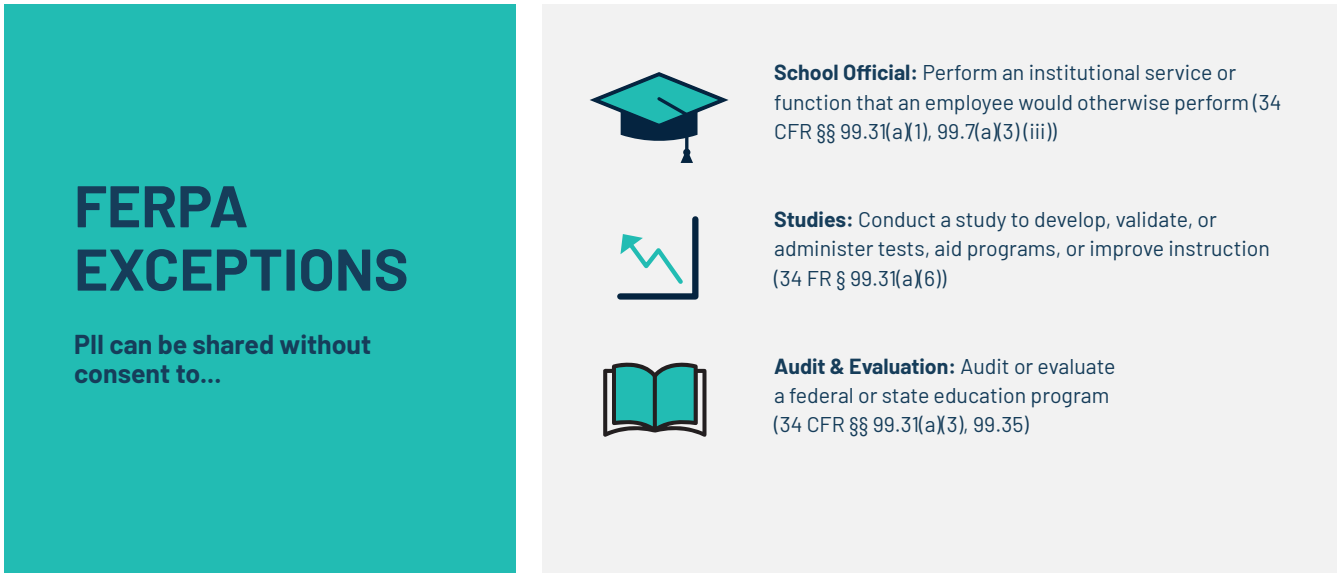


Figure 2b: FERPA Exceptions

For more information regarding these exceptions when consent is not required and simple decision tree tools for assessing whether and how they might support your data sharing use case, see **HIPAA Decision Matrix** and **FERPA Decision Matrix**, Appendix A and Appendix B.

When is consent required?

In addition to providing the exceptions above, HIPAA and FERPA both outline specific requirements for use cases when consent is expressly required and how that consent must be obtained.

HIPAA

HIPAA provides that "[a] covered entity or business associate may not use or disclose PHI, except as permitted or required by [the HIPAA Privacy Rule]."[13] The Individual Choice principle of the HIPAA Privacy Rule establishes that individuals should be given the opportunity to decide how their health information is collected, shared, and used.[14] HIPAA makes a distinction between two types of permission to allow PHI to be shared: "authorization" and "consent." Authorization is a formal detailed document that covered entities are **required** to use to share PHI for purposes not otherwise allowed under the Privacy Rule. In contrast, consent is an informal type of permission that is **optional** under HIPAA in cases where authorization is not required. An entity has the *option* (but not the obligation) to obtain consent to share PHI for **treatment, payment,** and **health care operations**.[15] Table 1 outlines the key differences between consent and authorization.

Table 1: Differences between Consent and Authorization

CONSENT	AUTHORIZATION
The Privacy Rule allows, but does not require, consent to share PHI for treatment, payment, and health care operations.[16]	The Privacy Rule **requires** authorization to disclose PHI for **purposes not otherwise allowed** by the Rule.[17]
Covered entities that elect to use consent have complete discretion to design a process that best suits their needs.[18]	An authorization has **specific elements** (requirements include description of PHI, purpose for disclosure, person authorizing disclosure, expiration date, etc.) that must be included to comply with HIPAA or there is a risk of disclosing information without proper permission.[19]

We strongly recommend that you consult your legal counsel to determine whether a written authorization or consent is required for a given use case when exceptions do not apply.

13 45 CFR § 164.502(a).
14 **Office for Civil Rights (2020, June 8).**
15 45 CFR § 164.506.
16 **Office for Civil Rights (2022, December 28).**
17 Ibid.
18 Ibid.
19 45 CFR § 164.508.

FERPA

FERPA, together with its regulations, protects the confidentiality of student records.[20] FERPA defines education records broadly as those records directly related to a student and maintained by an educational agency or institution or by a party acting for the agency or institution.[21] Generally, FERPA requires educational institutions to obtain written consent from a parent or eligible student before releasing personally identifiable information unless the disclosure is subject to an exception specified in the statute.[22] FERPA does not explicitly provide a definition of consent, and instead outlines what the written consent must contain. Figure 3 below outlines the requirements under FERPA for consent.

Figure 3: FERPA Elements for Consent

Required elements of the written consent under FERPA[23] include:

- Signature and date
- The purpose of the disclosure
- Description of the records that may be disclosed
- The name of the party or class of parties to whom the disclosure may be made

How do you get consent?

How consent is obtained is often dictated by statute or regulation. In nearly all circumstances, consent must be in writing. Consent is usually obtained in one of two ways: 1) actively, where an affirmative step is taken to give consent (sometimes referred to as "opting in"); or 2) passively, where consent is implied through inaction (sometimes referred to as "opting out").

HIPAA

As noted earlier, there are two types of permissions under HIPAA to share PHI: written authorization and consent.

AUTHORIZATION

Under HIPAA, unless a particular use is permitted or an exception exists, a formal written authorization is required.[24] Figure 4 outlines the specific elements that must be met for an authorization to be valid under HIPAA:[25]

20 See generally 34 CFR §§ 99.1-99.67; **Privacy Technical Assistance Center (n.d.).**
21 34 CFR 99.3.
22 34 CFR § 99.30(a); see also **Privacy Technical Assistance Center (2017, January).**
23 34 CFR § 99.30(b).
24 **Sullivan, J. M., & Hartsfield, S. B. (2020).**
25 See 45 CFR 164.508.

Figure 4: **HIPAA Elements for Authorization**

- Description of the PHI to be used or disclosed
- Name of the person or persons authorized to make the disclosure
- Identity of the party or class of parties to whom the disclosure may be made
- Description of the records that may be disclosed
- The purpose of the disclosure
- Expiration date or event
- Signature and date
- Statements that include: 1) a right to revoke consent; 2) assurances that treatment, payment, and enrollment eligibility are not affected; and 3) risk of redisclosure

It is important to note that these federal requirements are the floor and states may have more stringent conditions for authorizations.[26]

CONSENT

In cases where a covered entity chooses to obtain consent to share PHI for treatment, payment, and operation purposes, it has complete discretion to design a process best suited for its needs.[27] The law does not mandate what the consent instrument must contain, and a consent is not required to have the same elements as a written authorization. In these cases, some entities use "Opt-In" forms, where an individual must affirmatively elect to have their PHI shared. Some entities choose "Opt-Out" forms, where data are shared unless the individual affirmatively elects to opt out; if an individual does not sign the "Opt-Out" form, then consent is implied. Opt-In and Opt-Out forms are often used in electronic health information exchanges.[28] It is worth emphasizing that HIPAA's provisions for consent are optional. Because there is no HIPAA requirement to obtain consent for treatment, payment, or operation purposes, if an individual refuses to sign a consent form or requests restrictions, practically, under *federal law* the covered entity can simply ignore the refusal.[29] Stated plainly, this means that a covered entity could use the PHI for treatment, payment, or health care operations without the consent of the individual, unless *state law* requires the consent.[30] States can and do set more robust protections that would still limit the disclosure.

FERPA

FERPA is much more limited than HIPAA in how consent can be obtained. Under FERPA, consent must be actively and affirmatively given to share personally identifiable information. The Department of Education also specifies that oral consent is not sufficient, and that consent must be in writing.[31] As referenced in Figure 3, the consent must contain the following elements: signature; date; description of the records to be disclosed; purpose of the disclosure; and identity of the person receiving the disclosure.

26 See 45 CFR 160.203.
27 45 CFR § 164.506(b).
28 See generally **Office for Civil Rights (2013, July 26).**
29 Note, however, that some states might restrict the disclosure of data if there is a refusal. See **Clinovations, & George Washington University Milken Institute of Public Health (2016, September).**
30 **Sullivan, J. M., & Hartsfield, S. B. (2020).**
31 **Privacy Technical Assistance Center (n.d.).**

These requirements do not apply to "directory information"—information contained in an education record that would not generally be considered harmful or an invasion of privacy if disclosed.[32] Examples of directory information include name, address, telephone number, birthday, place of birth, participation in activities and sports, and dates of attendance. Schools may disclose directory information without consent.[33] However, schools must notify parents and eligible students about their intent to share directory information and allow a reasonable amount of time for them to request that the school not disclose their directory information.[34]

Practical and ethical problems with consent

Accessibility

One of the problems of consent is the inaccessibility of the legal instruments sometimes used to obtain consent. These instruments (which might include privacy notices, releases, written authorization, etc.) are often lengthy, broadly drafted, ambiguous, or filled with legalese that non-lawyers struggle to comprehend.[35] The sheer length of some of these instruments also makes them inaccessible.[36] Because of these barriers, *people do not read them*.[37] This calls into question the validity of the consent and the ethics of subsequent data use.

Validity of research

Analyzing administrative data can allow researchers to draw conclusions from a population (e.g., all public school children in grades 6–8; all Medicaid recipients in the state; all housing voucher recipients in a county), rather than relying upon a sample. This often leads to more robust findings that can inform policy and practice. However, when consent is required, consent bias may be introduced if the people who consent to research participation differ from those who decline participation in ways that impact the results.[38] While the extent of consent bias will vary from study to study, it is worth considering its potential impacts on internal validity when designing research that relies on obtaining consent.[39]

Consent management

Logistically managing consent presents administrative burdens. Entities must practically consider issues like how to manually obtain consent, where consent forms are stored and accessed, and how to manage expiring consents or revocations. Although technical solutions can assist with these challenges, they are often resource intensive, require extensive staff training, and still require human oversight.[40]

32 34 CFR § 99.37.
33 34 CFR § 99.3.
34 **US Department of Education (2021, August 25).**
35 See **Norton, T. B. (2016)** (arguing that drafters of privacy policies "employ vague or ambiguous language to either generalize very complex information practices or reserve the option to alter specific information practices in the future without creating the need to revise the policy").
36 See **Flanagan, A., King, J., and Warren, S. (2020, July).**
37 See **Solove, D. (2013)** ("Most people do not read privacy notices on a regular basis. As for other types of notices, such as end-user license agreements and contract boilerplate terms, studies show only a miniscule [*sic*] percentage of people read them. Moreover, few people opt out of the collection, use, or disclosure of their data when presented with the choice to do so").
38 **Rothstein, M. A., & Shoben, A. B. (2013).**
39 Again, it is worth restating that there is no consensus on the significance of consent bias. Instead, the argument has been made that consent bias is not justification for abandoning informed consent.
40 For a robust discussion of considerations regarding consent management systems see Stein et. al. (2021), ***Modernizing Consent to Advance Health and Equity***.

Risk of undue influence and coercion

> ***"Consent performs an enormous amount of work. Activities that would otherwise be illegitimate are made legitimate by consent."***
>
> —Daniel J. Solove[41]

A central ethical issue with consent in data sharing and integration is the risk that the way one gives and receives consent can inadvertently lead to nonconsensual activity. There are structural reasons for this—starting with why and how governments collect and use data to begin with. Typically, administrative data are collected when a community member needs to interact with an agency to receive a benefit, or when interaction is compelled (e.g., child welfare). When seeking a benefit or avoiding punitive measures, there is always a risk of *undue influence* or *coercion*. Because FERPA and HIPAA do not define undue influence or coercion, the Common Rule's guidance is instructive:

"**Coercion** occurs when an overt or implicit threat of harm is intentionally presented by one person to another in order to obtain compliance."[42]

"**Undue influence**, by contrast, often occurs through an offer of an excessive or inappropriate reward or other overture in order to obtain compliance."[43]

Sometimes individuals consent to unfavorable conditions or circumstances for a benefit. For example, people regularly consent to waive constitutional rights—such as First Amendment rights to free speech— as a condition of employment.[44] People may also consent to waive Fourth Amendment rights to be free from unreasonable search and seizures by agreeing to let a police officer conduct a vehicle search during a traffic stop if they believe it is the path of least resistance and disruption.[45] In these examples, consent (given under undue influence) lends legitimacy to activities that would be otherwise illegitimate. Similarly, individuals may feel coerced or experience undue influence to consent to sharing data in order to receive a public benefit or avoid further scrutiny. As always, context matters. What is coercive or unduly influential in one context may not be coercive or influential in another. Factors like the age of the person giving consent, medical condition, language ability, etc., can all add layers of legal complexity and nuance. These scenarios are often murky, and the risk of coercion and undue influence can be subtle.

41 **Solove, D. (2013).**
42 **Office for Human Research Protections (n.d.).**
43 Ibid.
44 **Solove, D. (2013).**

CONSENT SCENARIOS

Consider the following hypotheticals and their potential risks for coercion and undue influence:

HYPOTHETICAL #1	
A patient is informed about a research study led by their primary care physician. The physician informs the patient that they would be a good candidate and gives the patient a consent form. The physician then waits for the patient to review and sign the form in her presence. The patient has a good relationship with their doctor and trusts her judgment, and does not want her to feel insulted.	
Undue influence	In this case, the patient might feel obligated to participate in the research because the physician is the investigator and they do not want to offend her.
Coercion	In this case, there is a disparate impact in the power that the two parties hold in relation to each other. The physician arguably holds more power than the patient, in that the physician has medical knowledge that directly impacts the health and well-being of the patient. In this scenario, the physician waiting and watching to see whether the patient signs the form might intimidate the patient and potentially raise the concern that the patient might not continue to receive treatment.
HYPOTHETICAL #2	
A new initiative in State A offers transitional services to equip incarcerated persons with career readiness tools at the end of their incarceration. As part of this service, participants receive exit counseling, access to a directory of employers that hire formerly incarcerated individuals, and housing support. To receive this service, participants must sign a consent form allowing State A to share arrest data with local law enforcement agencies.	
Undue influence	In this case, the stigma and collateral consequences associated with incarceration present a significant incentive or reward for sharing this data.
Coercion	Without the use of this service, formerly incarcerated persons may face significant barriers to employment, such that a refusal to consent to sharing data could result in economic harm.

In both hypotheticals there is no clear answer, but entities charged with securing consent should take care to limit undue influence or coercion.

Racial equity & consent

> ***"As railroads and highways both developed and decimated communities, so too can data infrastructure. At this moment in our history, we can co-create data infrastructure to promote racial equity and the public good, or we can invest in data infrastructure that disregards the historical, social, and political context—reinforcing racial inequity that continues to harm communities."***
>
> —Actionable Intelligence for Social Policy[46]

Research has a fraught history of inflicting harm, particularly on vulnerable and disenfranchised populations. This history—and current surveillance and research practices—is at the root of many ethical concerns around data practices, including administrative data reuse.[47] For example, the Havasupai tribe sued the Arizona State University Board of Regents on the basis that researchers at the university used blood samples from tribal members to conduct what the tribe thought was diabetes research.[48] At the center of this dispute was how consent was obtained, and the Havasupai tribe urged that had they been adequately informed, they would not have consented to the research.[49] The members signed broad consent forms that were used to expand the research beyond the purported original scope.[50] The tribe later discovered that the researchers used the broad consent to share their members' blood with other researchers to study schizophrenia, inbreeding, and human population migration theories. The tribe sued the Board of Regents alleging cultural, dignitary, and group harm to the tribe.[51] In this way, consent (or the guise of consent) can be used to reinforce legacies of racist policies and produce inequitable outcomes.

46 **Hawn Nelson, A. et al. (2020a).**
47 **Flanagan, A., King, J., and Warren, S. (2020, July).**
48 **Drabiak-Syed, K. (2010).**
49 Drabiak-Syed, pp. 180–81.
50 Ibid.
51 Ibid.

What might ethical consent look like?

In light of the ethical risks associated with consent, reimagining ethical consent requires that we consider the context of data sharing and integration and the historical and structural oppression that shapes it. Two ways to do this are through the pursuit of social license and the use of carefully considered consent frameworks.

Social license

Routine efforts to share and use cross-sector data must develop public approval—the "social license" to operate—to ensure ethical use and drive change.

> **Social license** comes from an effort's perceived legitimacy, credibility, compliance with legal and privacy rules, and overall public trust. Earning it requires dedicating time and resources to develop relationships, source and incorporate feedback, and engage with diverse partners on an ongoing basis.[52]

Social license is a norm, and as a result there is no formal enforcement mechanism for losing social license. However, there are clear consequences for operating without social license. For example, in 2019 a data sharing agreement to share youth data for predictive analytics was terminated between St. Paul, Ramsey County, and the St. Paul Public Schools after community outcry.[53] Two dozen organizations and community leaders who had learned of the agencies' plans to share data demanded that the agreement be terminated. Not only did plans to assign risk scores to youth raise privacy concerns and essential questions about the potential for harm, but no effort had been made to establish social license. Marika Pfefferkon, a community advocate who pushed for the termination of the data sharing agreement, rightfully argued that "[d]ata is not bad, but data without any kind of oversight that includes the community does not benefit us."[54]

It is particularly important to build relationships and social license with Black, Indigenous, people of color, and other historically marginalized groups disproportionately harmed by government systems. Individuals represented "in" the data and frontline staff who support programs should be included in data governance structures and provided authentic opportunities for participation and decision-making.[55] For a detailed discussion of these issues and examples of strategies for building social license with a racial equity lens, see our **Toolkit for Centering Racial Equity Throughout Data Integration**.[56]

Consent framework recommendations

As illustrated by the example of the Havasupai tribe, how consent is obtained is just as important as the consent itself. We strongly encourage that any consent framework be collaboratively designed with the feedback and input of parties beyond general counsel and security and/or privacy officers. Consent is not just about risk mitigation or compliance, but about strong governance. In the absence of requirements dictated by federal or state law or where there is no guidance, we recommend a consent framework[57] informed by the **Common Rule.**[58] On the following page, we outline the elements to include in an ethical consent framework.

52 **Hawn Nelson, A., et al. (2022).**
53 **Melo, F. (2019, January 28).**
54 Ibid.
55 **Hawn Nelson, A., et al. (2022).**
56 **Hawn Nelson, A. et al. (2020).**
57 For another consent framework similar to the Common Rule, see **Lee, U., & Toliver, D. (2017).**
58 See 45 CFR 46.116(a)–(c).

ELEMENTS	DESCRIPTION	PRACTICAL EXAMPLES
Not Passive or Implied	Consent should be affirmatively given, allowing participants to actively ask questions and seek clarification.	✗ Opt-Out[59]
Willingly Given	The participant should have full mental capacity to provide consent, and consent should be given without undue pressure, coercion, or force. The participant should be in a position to freely decide whether to permit sharing data.	✓ Allow adequate time for prior review ✗ Participant sign "on the spot" without time for review
Understandable	The information should be given in plain language, in terms that the subject population understands. Further, the process should ensure that all risks and benefits are disclosed.	✓ Plain language ✓ Specific ✓ Brief ✗ Broad or vague language ✗ Legalese ✗ Lengthy and dense
Revocable	The instrument should clearly state that consent can be withdrawn at any time for any purpose.	✗ Language that suggests the consent exists in perpetuity ✓ Time-bound ✓ Clear instructions for how to revoke or terminate consent
Not Conditioned on a Benefit	The instrument should make clear that refusing to consent will result in no penalty or loss of benefits.	✗ Penalties or loss of benefits for refusing to give consent
No Exculpatory Language	The instrument should not contain language that purports to waive or appears to waive a participant's legal rights or appears to release the institution or its agents from liability or negligence.	✗ Release or any language that has the effect of freeing an entity from liability, negligence, fault, guilt, or blame

While Opt-Out forms reduce administrative burden, our view is that Opt-Out forms necessarily position the individual whose data will be shared in a defensive posture. In this scenario, the default is that data are shared, and the onus is on the individual to have the knowledge, time, and wherewithal to elect out.

59 For more information on the pros and cons of Opt-In vs. Opt-out, see **Heath, S. (2016, July 11).**

Four questions to get you started

When it comes to deciding whether and when to attain consent, we offer the following considerations and context to weigh as you begin to chart a path forward toward ethical use:

	CONSIDERATIONS	CONTEXT
1. Is this legal?	• What legal authority is in place to use these data? • Does the law require consent for this use? If so, does the law specify how that consent must be obtained? • Are there any exceptions under the law for this use (e.g., school official exception, public health authority)?	This might be the only question that has to be considered. If the law expressly requires consent and is explicit with how that consent must be attained, then there is no additional inquiry or decision to be made. In this case, if you want to share, the law has effectively made this decision about consent for you, and we recommend that you refer back to the checklist above to craft an ethical approach to obtaining consent.
2. Is this ethical?	• Are there risks of redisclosure or other harms, particularly for groups historically marginalized by discriminatory systems? • What is the history of data sharing and integration in this context? • Is there a benefit to the person whose data will be shared?	If there is a risk of redisclosure, risk of misuse, or history of pervasive harm, you may face an ethical imperative to obtain consent even in cases where it is not expressly required.[60] In a case where potential harms exist, those harms should be weighed against the benefits of data sharing to those "in" the data.
3. Is this a good idea?	• What is the culture (shared, learned behavior) of data sharing and integration? • What are the costs (price, staff time) of attaining consent? How will consent be managed? • Could this question be answered with de-identified, aggregate data?	If a use case is determined to be both legal and ethical, you will also need to weigh practical considerations like resources and data availability to determine the feasibility of attaining consent, as well as the feasibility of alternative methods that do not require identifiable data.
4. How do we know and who decides?	• Who is conducting the integration and analysis? Do they have sufficient understanding of the program/policy/population/history that is being studied? • Who is tasked with "getting" the consent? • Do community members, including those "in" the data, know about and support this work?	Determining the legal, ethical and practical parameters of consent is not always a simple task, and should include a variety of diverse perspectives, with clarity around decision-making authority. Care must be taken to consider differences in risks and benefits across dimensions of identity and lived experience. This means that individuals "in" the data should have decision-making power.[61]

60 For example, in the case of Henrietta Lacks, a Black tobacco farmer whose cells were taken without her knowledge and used in research and monetized by John Hopkins University for decades without consent, the university now requires consent from next of kin to use her biological data in future research. See **Butanis, B. (2022, February 18).**

61 For example, the governing body tasked with deciding who can use Lacks' biological information now includes two members of Lacks' family.

Thinking through these concepts can help you to better understand the legal parameters around consent for your data integration efforts. The following hypotheticals illustrate how to apply these questions.

HYPOTHETICAL #1	
A nonprofit organization that receives Violence Against Women Act (VAWA) funding operates a domestic violence shelter and food bank and wants to share information with a local social services agency to determine eligibility for additional services.	
Considerations:	**LEGAL:** VAWA and its accompanying regulations explicitly require consent for this purpose and lay out the elements of what that consent must contain. See 28 CFR 90.4 (b)(3)(ii). In this scenario, there is no gray area. The law expressly requires consent and is explicit with how consent must be attained.

HYPOTHETICAL #2	
A mayor's office has funding to support 2,000 new subsidized early childhood education slots at high-quality child care centers and wants to make sure the slots are filled by families who need the support most. They propose using the local IDS to share data on early childhood risk factors (lead exposure, low birth weight, parental incarceration) with social service partners and pediatricians so that families with high need can be offered opportunities to enroll in early childhood programs in the course of routine service interactions and well child visits.	
Considerations:	**LEGAL:** Consent is not required by law (data are governed by state public records law and rules regarding vital records). **ETHICAL:** Partners are split on how to weigh risk of redisclosure with benefit of services offered. **GOOD IDEA:** The cost of attaining consent from this group would be significant and defeat the purpose of quick and efficient outreach to provide services. Partners agree that the benefit of targeted outreach can be achieved without sharing individual details by simply creating a generic "flag" on the record of those families with multiple risk factors to encourage providers to offer referral to subsidized child care. **WHO DECIDES:** The IDS governance board made up of data owners from each participating public agency, as well as several parent representatives, weighs the decision.

HYPOTHETICAL #3

After recognizing low rates of early childhood immunizations, State A wants to coordinate its immunization programs with Indian Tribal Organization WIC agencies that serve Native American WIC enrollees. This initiative would require sharing WIC data with vaccine clinics.

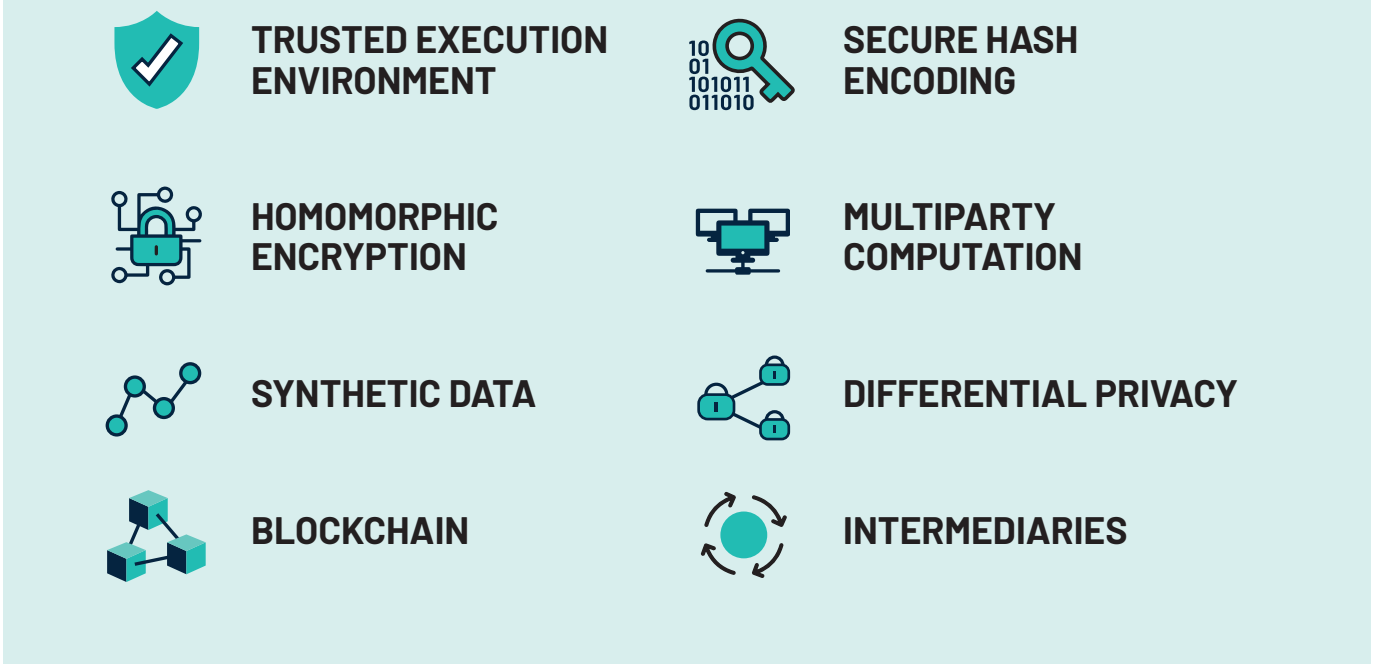
Considerations:	**LEGAL:** Under 7 CFR 246.26(h), this data could be shared without consent through a data sharing agreement. **ETHICAL:** While consent is not required, there is a history of displacement, colonization, distrust, and institutional racism, such that consent is important from an ethical standpoint given past harms and local history. The risk of sharing data without consent could deepen mistrust. **GOOD IDEA:** Consent can be reasonably managed by the vaccine clinic partner during existing touch points, and the consent instrument is clear, understandable, and drafted with the input of Tribal lawyers and members. Further, there is a significant health imperative and benefit by the Tribe to ensure that its members are vaccinated. **WHO DECIDES:** Decision put to advisory board with Tribal members, and consent drafted with input from Tribal lawyers and members.

As illustrated in hypothetical #2, IDS can play a helpful role in navigating complex questions about consent, particularly when the law is silent or unclear. IDS help institutionalize and maintain relationships among data partners by establishing strong governance, with collective decision-making processes, and clear stewardship responsibilities. For more on IDS, check out AISP's **Quality Framework.**

Technical alternatives to consent

Given the practical and ethical challenges associated with consent, governments may be interested in opportunities to leverage technical methods to enhance privacy and circumvent the need for consent in certain cases. Recently, entities charged with ensuring the privacy of personal data in both the public and private sectors have begun using privacy preserving technologies (PPTs) to do just that. PPTs (also referred to as privacy-enhancing technologies) are an umbrella of cryptographic tools used to protect and limit the exchange of personally identifiable information. The application of PPTs includes methods like homomorphic encryption and secure multiparty computation.[62] At a very high level, approaches like homomorphic encryption and multiparty computation can compute data from different sources to be used and analyzed as aggregated results while maintaining the privacy of personally identifiable information (PII).[63] The figure below lists different PPT methods.[64]

Figure 5: Privacy Preserving Technologies



The use of PPTs to share data among government agencies is relatively new and not without its own challenges and costs. That said, we have seen successful implementations of PPTs in several US jurisdictions that helped eliminate the burden of obtaining consent for certain use cases and moved ethical data sharing forward. For more on the use of PPTs, check out this **case study.**[65]

62 **Bean, A., Jaynes, J., Sexton, T. J. (2019, July 15).**
63 Ibid.
64 O'Hara, A., & Bean, A. (2022).
65 **Bean, A., Jaynes, J., Sexton, T. J. (2019, July 15).**

Conclusion

Consent and the process for obtaining consent is complex and nuanced. There is no bright-line rule to the question, "Does data sharing and integration require consent?" There will be times when the law is explicit about when and how consent is needed and attained. In other cases, there may be no clear answer. What *is* clear is that any discussion of consent must be grounded in the historical context of data sharing and integration, and the legal, practical, and ethical considerations of consent must be weighed. Social license, aided by strong consent frameworks and governance models, can support a path forward that is right in your context. Alternatives to consent—use of exceptions, de-identification, and privacy preserving technologies—are worthwhile pathways to explore as you seek to minimize the security, regulatory, and privacy risks of data sharing.

References

Bean, A., Jaynes, J., and Sexton, T. J. (2019, July 15). ***How Tulsa Is Preserving Privacy and Sharing Data for Social Good***. Data Across Sectors for Health.

Butanis, B. (2022, February 18). **Frequently Asked Questions**. The Legacy of Henrietta Lacks. Johns Hopkins Medicine.

Clinovations & George Washington University Milken Institute of Public Health. (2016, September). ***State HIE Consent Policies: Opt-In or Opt-Out***. Office of National Coordinator for Health IT.

Data Across Sectors for Health and The Network for Public Health Law. (2018). ***Data Sharing and the Law, Deep Dive on Consent***.

Drabiak-Syed, K. (2010). **Lessons from Havasupai Tribe v. Arizona State University Board of Regents: Recognizing Group, Cultural, and Dignitary Harms as Legitimate Risks Warranting Integration into Research Practice**. *Journal of Health & Biomedical Law* 6(2): 175–226.

Flanagan, A., King, J., & Warren, S. (2020, July). ***Redesigning Data Privacy: Reimagining Notice & Consent for Human-Technology Interaction***. World Economic Forum.

Hawn Nelson, A., Jenkins, D., Zanti, S., Katz, M., Berkowitz, E., et al. (2020a). ***A Toolkit for Centering Racial Equity Throughout Data Integration***. Actionable Intelligence for Social Policy. University of Pennsylvania.

Hawn Nelson, A., Jenkins, D., Zanti, S., Katz, M., Burnett, T., Culhane, D., Barghaus, K., et al. (2020b). ***Introduction to Data Sharing and Integration***. Actionable Intelligence for Social Policy. University of Pennsylvania.

Hawn Nelson, A., Kemp, D., Jenkins, D., Rios Benitez, R., Berkowitz, E., Burnett, T., Smith, K., Zanti, S., Culhane, D. (2022). ***Finding a Way Forward: How to Create a Strong Legal Framework for Data Integration***. Actionable Intelligence for Social Policy. University of Pennsylvania.

Heath, S. (2016, July 11). ***Should a Health Information Exchange Be Opt-In or Opt-Out?*** Health IT Security.

Jenkins, D., Berkowitz, E., Burnett, T., Culhane, D., Hawn Nelson, A., Smith, K., and Zanti, S. (2021). ***Quality Framework for Integrated Data Systems***. Actionable Intelligence for Social Policy. University of Pennsylvania.

Lee, U., & Toliver, D. (2017). ***Building Consentful Tech***. Allied Media Projects.

Melo, F. (2019, January 28). ***St. Paul, Ramsey County to End Youth Data-sharing Agreement after Withering Criticism***. Pioneer Press.

Norton, T. B. (2016). **The Non-Contractual Nature of Privacy Policies and a New Critique of the Notice and Choice Privacy Protection Model**. *Fordham Intellectual Property, Media & Entertainment Law Journal*, 27.

Office for Civil Rights. (2020, June 8). ***Individual Choice Principle in the Privacy and Security Framework*.** US Department of Health & Human Services Guidance Portal.

Office for Civil Rights. (2022, October 25). ***Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule***. US Department of Health & Human Services.

Office for Civil Rights. (2022, December 28). ***What Is the Difference between "Consent" and "Authorization" under the HIPAA Privacy Rule?*** US Department of Health & Human Services.

Office for Human Research Protections. (n.d.). ***Informed Consent FAQs***. US Department of Health & Human Services.

O'Hara, A., & Bean, A. (2022). Key Topics in Privacy Preserving Technology: What Is PPT and How Can It Support Integrated Data Sharing Efforts? [PowerPoint slides]. AISP Network Meeting.

Pierce West, S. (2016). **They['ve] Got Eyes in the Sky: How the Family Educational Rights and Privacy Act Governs Body Camera Use in Public Schools**. *American University Law Review* 65, 1533–1567.

Privacy Technical Assistance Center. (2013, May). ***Data De-identification: An Overview of Basic Terms***. US Department of Education.

Privacy Technical Assistance Center. (2017, January). ***Integrated Data Systems and Student Privacy***. US Department of Education.

Privacy Technical Assistance Center. (n.d.). ***What Is FERPA?*** U.S. Department of Education.

Privacy Technical Assistance Center (n.d.). ***What Must a Consent to Disclose Education Records Contain?*** US Department of Education.

Rothstein, M. A., & Shoben, A. B. (2013). **Does Consent Bias Research?** *American Journal of Bioethics* 13(4), 27–37.

Solove, D. (2013). **Privacy Self-Management and the Consent Dilemma**. *Harvard Law Review*, 1880.

Stein, D., Handspicker, B., Bishop, M., Alibrandi, C., Bernstein, J., Chavez, D., Babbrah, P., Solomon, M., Jahn, E., St. Clair, J., Kratz, M., Taylor, A., (2021). ***Modernizing Consent to Advance Health and Equity***. Stewards of Change Institute.

Sullivan, J. M., & Hartsfield, S. B. (2020). ***HIPAA: A Practical Guide to the Privacy and Security of Health Data*** (2nd ed.). American Bar Association, Health Law Section.

Wolford, B. (n.d.). ***What Is GDPR, the EU's New Data Protection Law?*** GDPR EU.

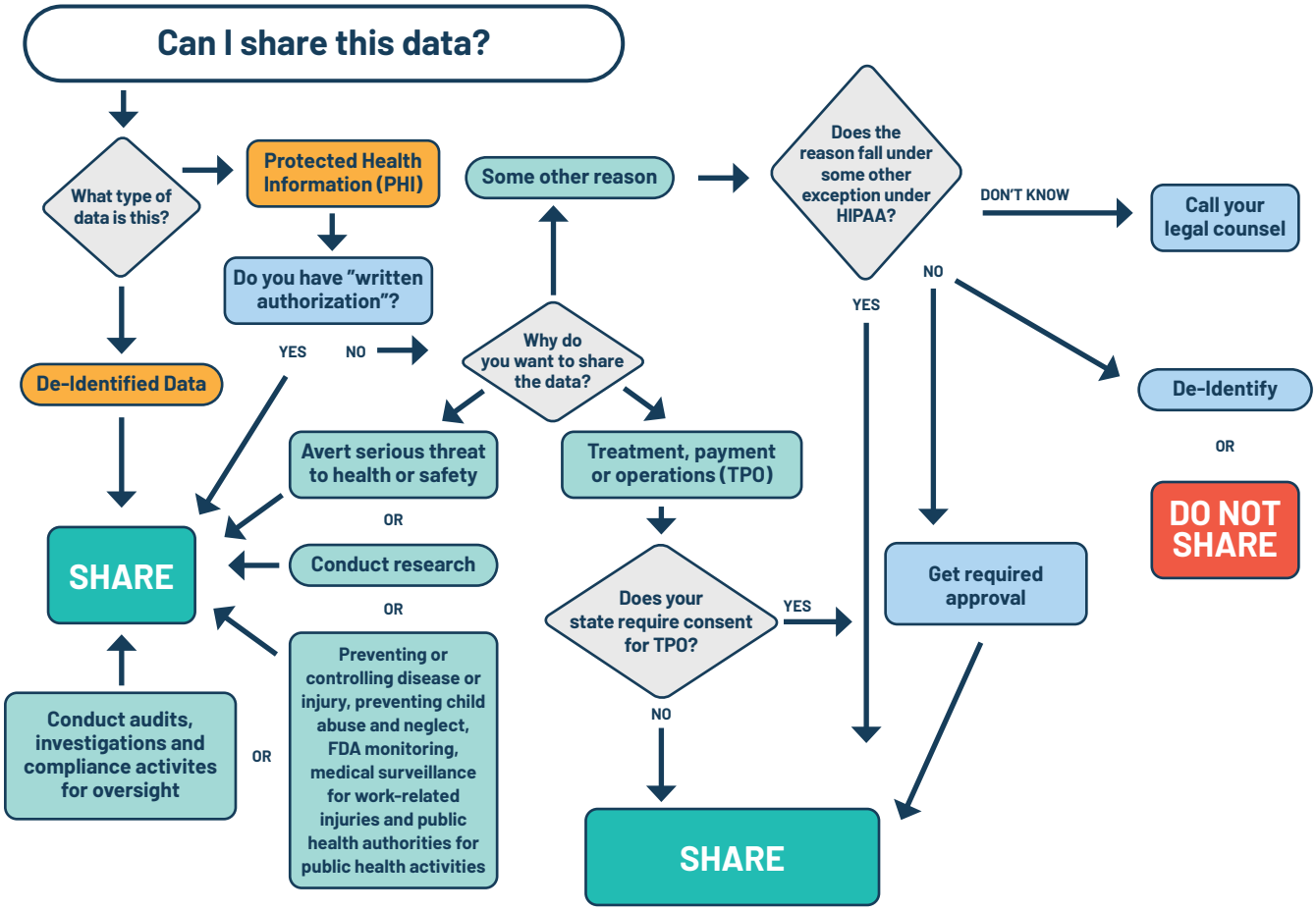
Actionable Intelligence for Social Policy
University of Pennsylvania
3701 Locust Walk, Philadelphia, PA 19104
www.aisp.upenn.edu

AISP

Health Data

Getting Started

Cross-sector data sharing and integration has become more routine and commonplace, as cross-sector data provide valuable insights to inform resource allocation and evaluate policies. Importantly, as health data is frequently shared and integrated, practitioners must decipher the Health Insurance Portability and Accountability Act (HIPAA) legal safeguards for sharing and integrating health data. The following matrix was designed to help practitioners begin to understand legal safeguards under HIPAA. To learn more about HIPAA and other legal considerations for data sharing, check out AISP's ***Finding A Way Forward: How to Create a Strong Legal Framework for Data Integration*** and ***Yes, No, Maybe? Legal and Ethical Considerations for Informed Consent in Data Sharing and Integration***.



IS THIS LEGAL?

This decision matrix provides a broad overview of key questions to ask to begin to answer the question of "Is it legal?" This matrix assumes the organization is a "covered entity" and HIPAA applies. This matrix is just a starting point and does not address all the potential scenarios, including any pertinent state laws, in which health data can or cannot be disclosed, as such it is always important to consult your legal counsel.

- **HIPAA protects the confidentiality of individual health information**
- **This matrix highlights common HIPAA exceptions for data sharing and integration**
- **This matrix is not intended as legal advice**

HIPAA Decision Matrix

If you selected this:

Avert serious threat to health or safety

Then your use likely falls within the Health or Safety Exception

Health or Safety Exception

PHI can be disclosed to prevent or lessen an imminent threat to the public or a person when made to someone that can lessen the threat.

(45 CFR § 512(j))

If you selected this:

Conduct research

Then your use likely falls within the Research Exception

Research Exception

Under this exception, PHI can be disclosed to a researcher:

- if a waiver of authorization is approved by IRB;
- to prepare research protocol or purpose preparatory to research and the PHI is necessary;
- for research on decedents and PHI is necessary.

There are also additional requirements that a researcher must meet under this exception.

(45 CFR §§ 502(d) and 164.514(a)-(c))

If you selected this:

Treatment, payment or operations (TPO)

Then your use likely falls within the TPO Exception

TPO Exception

PHI can be disclosed for treatment, payment and health care operations. Under this exception, PHI can be shared to coordinate treatment, including referrals and consultations; billing, collection, preauthorization; and operational activities like quality assessments, legal services, auditing, etc. Note, that under this exception a Business Associate Agreement might be required and certain states might also require consent.

(45 CFR § 164.502)

If you selected this:

Then your use likely falls within the Health Oversight Exception

Conduct audits, investigations and compliance activities for oversight

Health Oversight Exception

PHI can be disclosed for health agency oversight activities authorized by law that include audits; civil, administrative, or criminal investigation; inspections; disciplinary actions; or civil, administrative or criminal actions to ensure compliance with government regulatory programs.

(45 CFR § 512(a))

If you selected this:

Then your use likely falls within the Public Health Activity Exception

Preventing or controlling disease or injury, preventing child abuse and neglect, FDA monitoring, medical surveillance for work-related injuries and public health authorities for public health activities

Public Health Activity Exception

Under this exception, PHI can be shared to:

- prevent or control disease, injury, or disability;
- prevent child abuse and neglect;
- FDA monitoring (such as product recalls);
- contact individuals exposed to communicable disease;
- work-place injury or illness surveillance;
- public health authorities for public health activities.

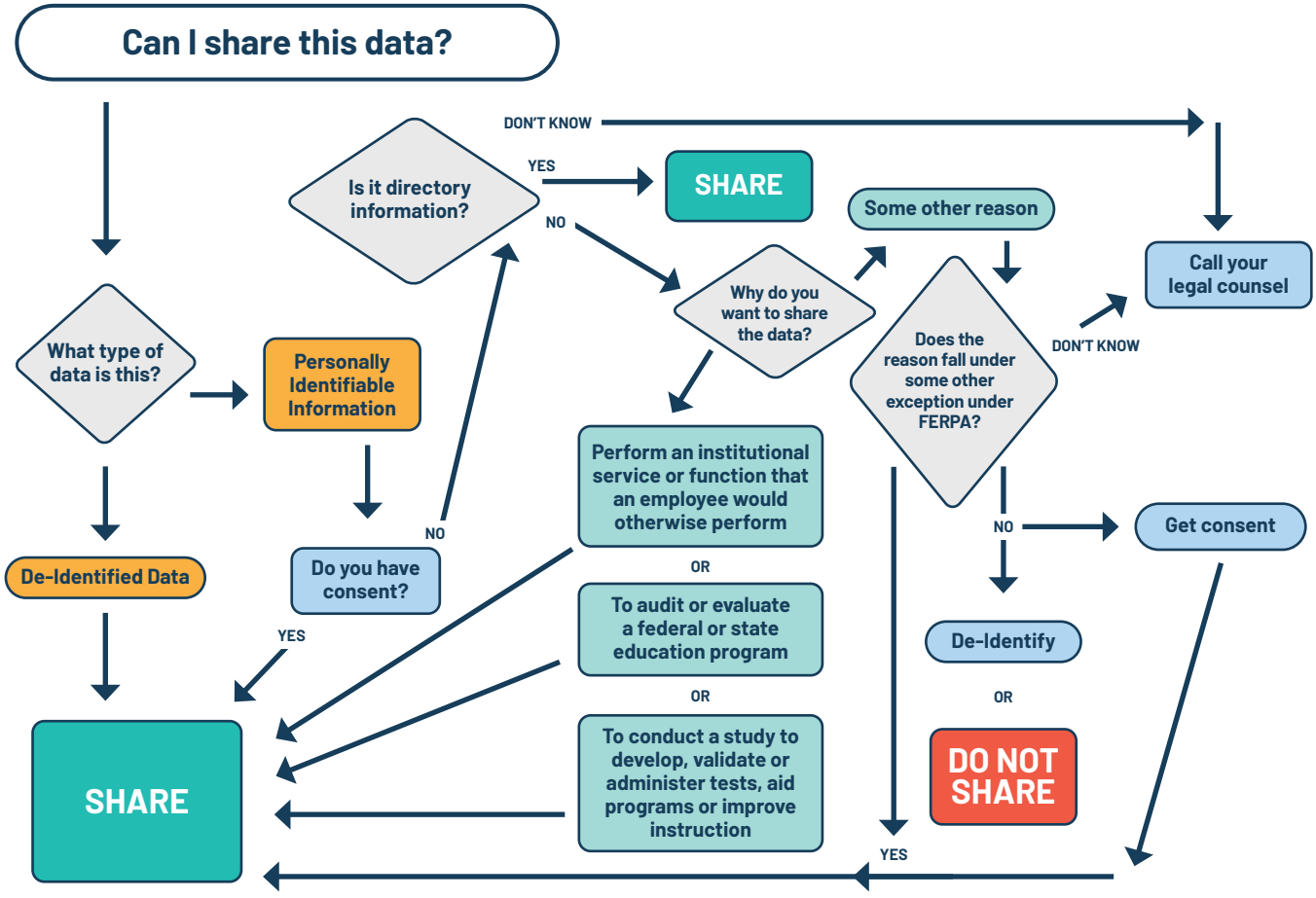
(45 CFR § 512(f))

AISP

Education Data

Getting Started

Cross-sector data sharing and integration has become more routine and commonplace, and for good reason. When governments and their partners bring together data safely and responsibly, policymakers and practitioners are better equipped to understand student needs and improve schools. Importantly, as education data is frequently shared and integrated, practitioners must decipher the Family Educational Rights & Privacy Act's (FERPA) legal safeguards for sharing and integrating education data. The following matrix was designed to help practitioners begin to understand legal safeguards under FERPA. To learn more about FERPA and other legal considerations for data sharing, check out AISP's ***Finding A Way Forward: How to Create a Strong Legal Framework for Data Integration*** and ***Yes, No, Maybe? Legal and Ethical Considerations for Informed Consent in Data Sharing and Integration***.



IS THIS LEGAL?

This decision matrix provides a broad overview of key questions to ask to begin to answer the question of "Is it legal?" The matrix assumes the organization is an educational institution that is subject to FERPA. This matrix is just a starting point and does not address all the potential scenarios in which education data can or cannot be disclosed, as such it is always important to consult your legal counsel.

- **FERPA protects the confidentiality of education data**
- **This matrix highlights 3 key FERPA exceptions**
- **This matrix is not intended as legal advice**

FERPA Decision Matrix

If you selected this:

Perform an institutional service or function that an employee would otherwise perform

Then your use likely falls within the School Official Exception

School Official Exception

Institutions can designate third-parties (such as contractors, consultants or volunteers) as school officials and share education data, if the third party:

- performs an institutional function or service that an employee would otherwise perform;
- is under direct control of the institution regarding the use and maintenance of the data;
- complies with requirements under the law for use and redisclosure.

34 CFR §§ 99.31(a)(1), 99.7(a)(3)(iii))

If you selected this:

To audit or evaluate a federal or state education program

Then your use likely falls within the Audits & Evaluations Exception

Audits & Evaluations Exception

Education data can be disclosed to a) audit or evaluate a federal or state supported education program or b) enforce or comply with federal legal requirements related to the program. There are also requirements regarding the intended data recipient.

(34 CFR §§ 99.31(a)(3), 99.35)

If you selected this:

To conduct a study to develop, validate or administer tests, aid programs or improve instruction

Then your use likely falls within the Studies Exception

Studies Excepton

Education data can be disclosed to:

- develop, validate or administer predictive tests;
- administer student aid programs;
- improve instruction.

Disclosure must be for, or on behalf of, an educational institution. Data must be destroyed when no longer needed for the study and cannot permit identification of individual students or parents to others outside the organization.

(34 CFR § 99.31(a)(6))