Yes, No, Maybe?: Legal & Ethical Considerations on Informed Consent in Data Sharing and Integration

Amy Hawn Nelson, Research Faculty, Director of Training and Technical Assistance, AISP

Deja Kemp, Research Faculty, Director of Legal Policy, AISP

What We Do

- **Convene** and advocate on behalf of communities that are sharing and using cross-sector data for good
- **Connect** to innovations, best practices, and research and funding opportunities that support ethical data sharing
- **Consult** with data sharing collaborations to build the human and technical capacity to share data and improve lives

Why We Do It

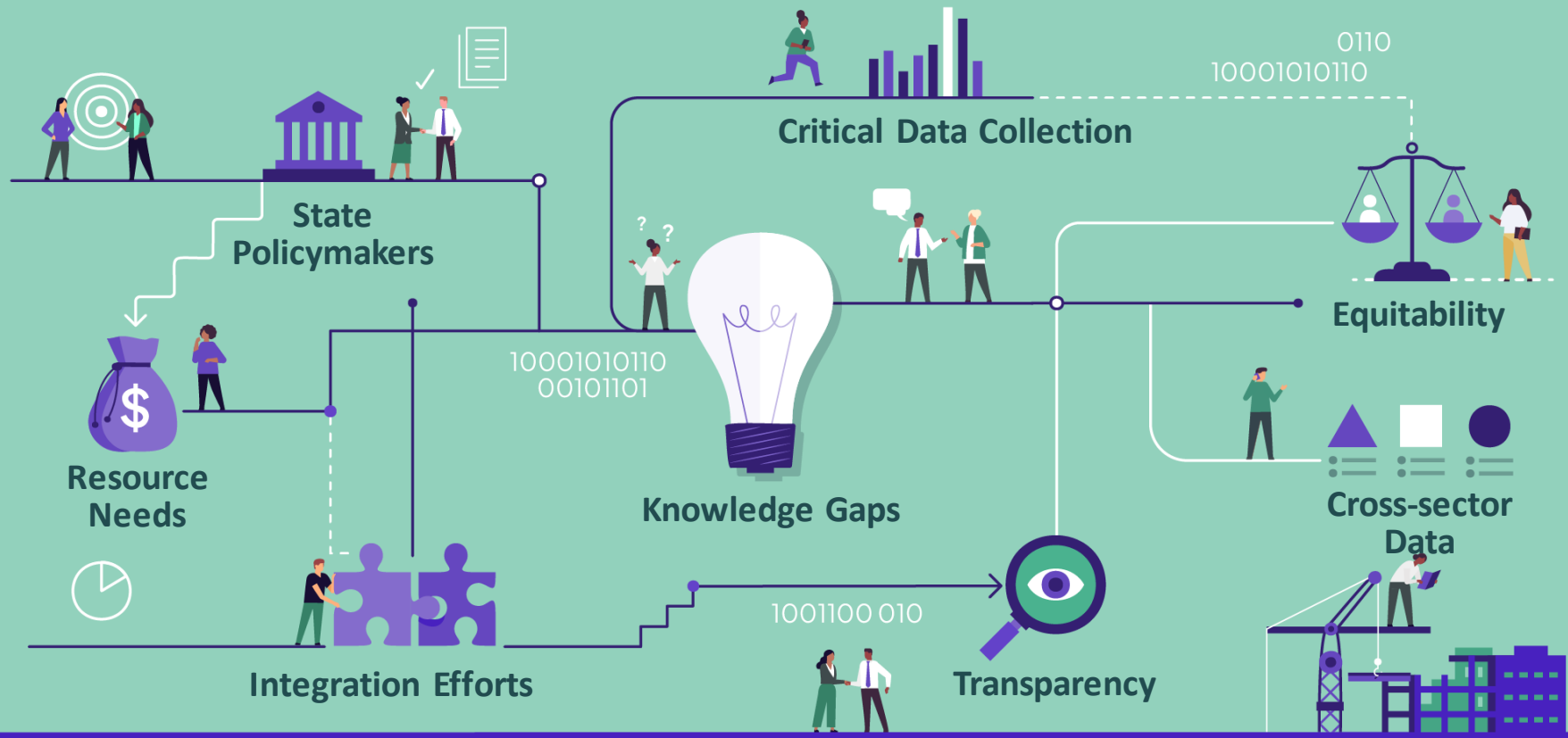
When communities bring together cross-sector data safely and responsibly, policy-makers, practitioners, and schools are better equipped to:

- Understand the complex needs of individuals and families
- Allocate resources where they're needed most to improve services
- Measure long-term and two-generation impacts of policies and programs
- Engage in transparent, shared decision-making about how data should (and should not) be used

AISP

www.aisp.upenn.edu

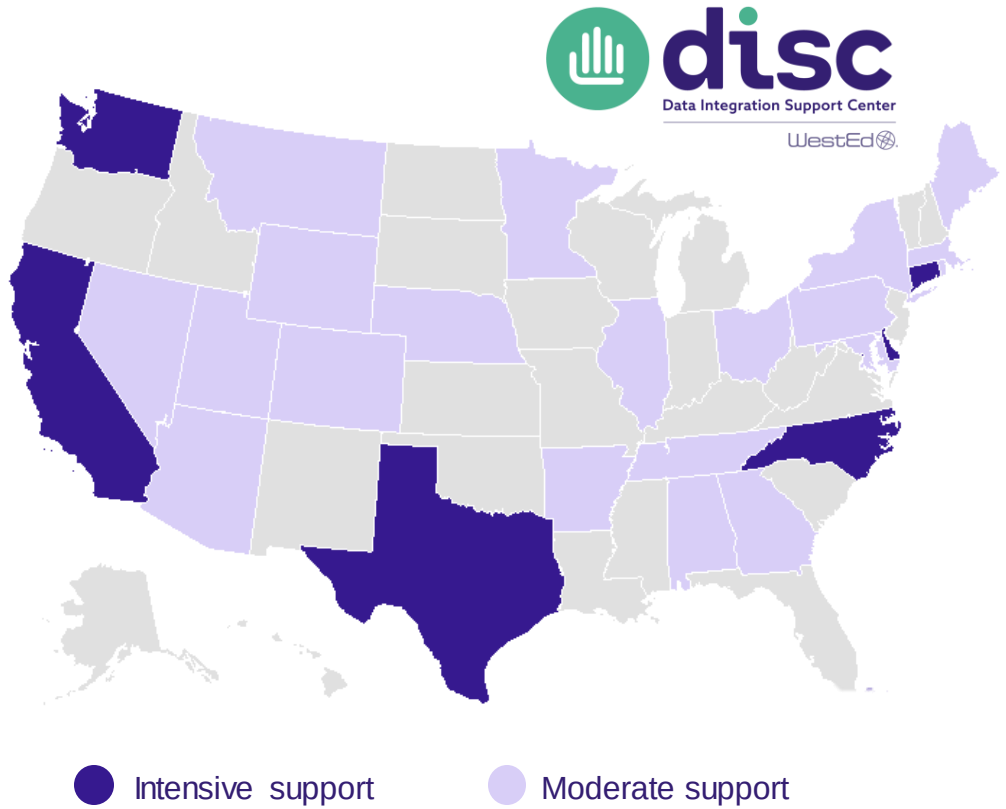
The Data Integration Support Center (DISC) at WestEd provides expert integrated data system planning and user-centered design, policy, privacy, and legal assistance for public agencies nationwide.



Our roles

We are:	We are not:
Data evangelists	Data holders or intermediaries
Connectors, community builders, thought partners, cheerleaders, and data sharing therapists	A vendor or vendor recommenders
Focused on ethical data use for policy change	Focused on academic research

Our Networks



Our approach

Data sharing is as relational as it is technical.

We don't just need to integrate data;

we need to integrate people.

LEGAL DISCLAIMER

- Not Legal Advice
- Training will only cover **federal law**
- Laws change. This content is based on the law at the time of the workshop
- Consult your general counsel for specific legal questions

In the Chat….

How many of you have ever used Amazon?

How many of you have ever checked a box like this (for Amazon or some other service) without reading?

Please Share

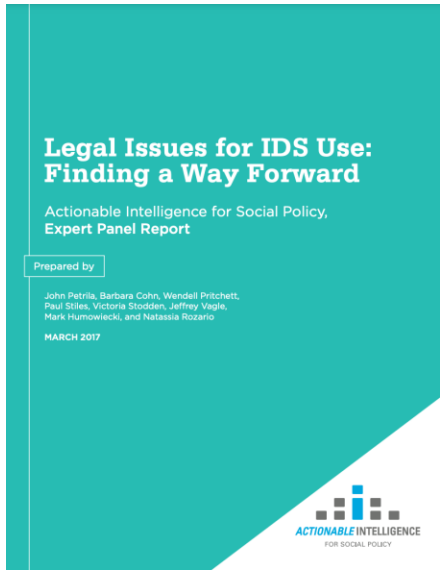
Have you ever “checked a box” to give consent without reading? Why? What did you stand to gain? What did you stand to lose if you did not give consent?

How often do you think non-lawyers “check a box” without reading?

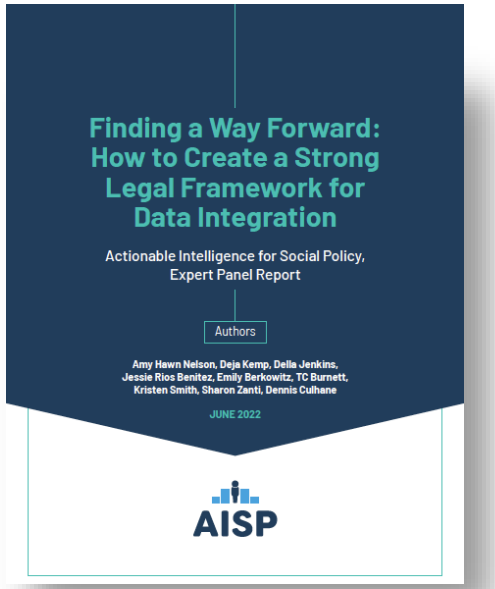
Essential Questions

- What are some technical alternatives to consent?
- What are the legal, ethical, and practical challenges associated with obtaining and managing consent in data-sharing and integration efforts?
- What are the major federal laws governing informed consent in the sharing of personally identifiable information, and how do they impact data-sharing practices?
- What best practices can organizations adopt to ensure consent processes align with legal requirements, ethical standards, and operational needs?

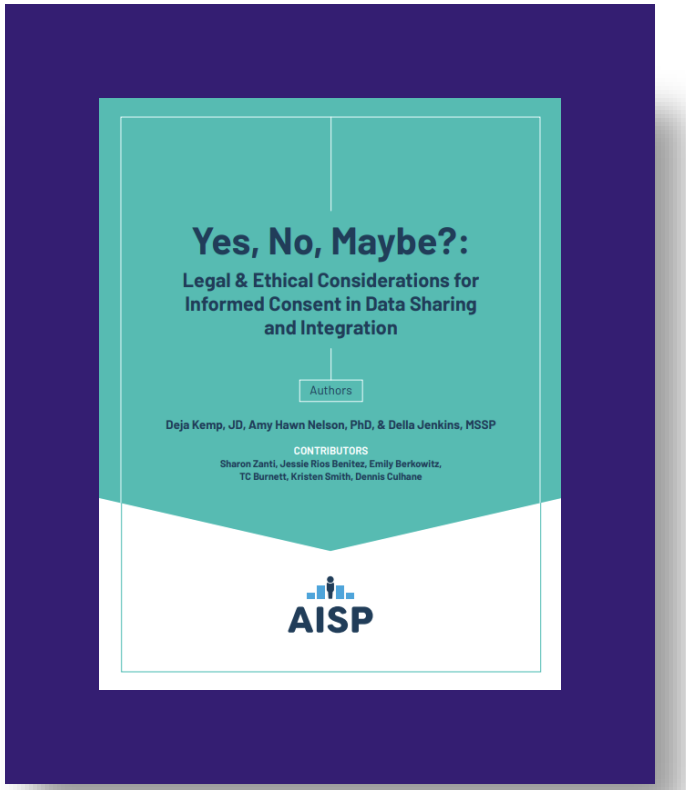
Legal Publications



2017



2022



2023

Legal Standards

Authority & Access

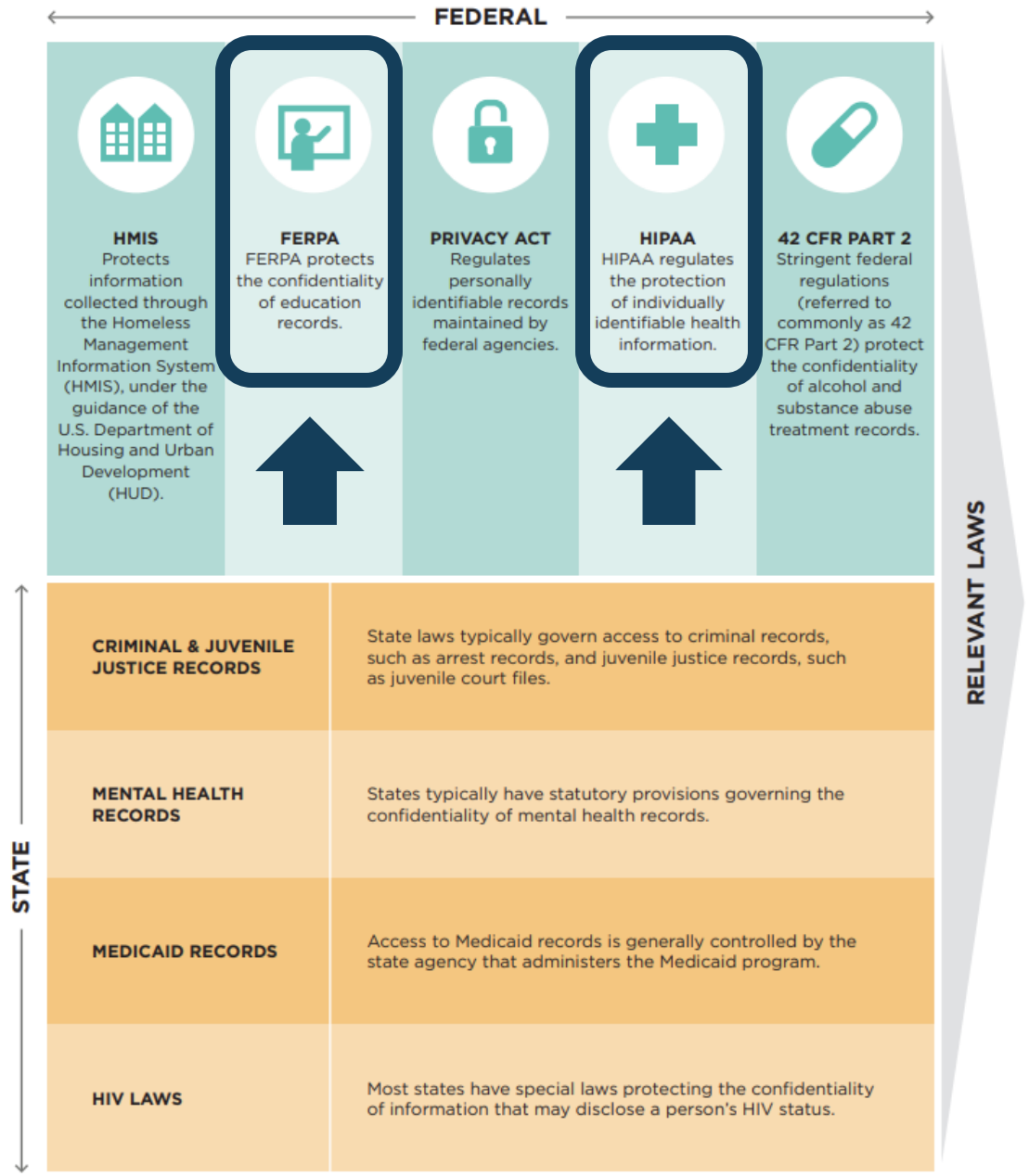
Legal Authority

Data Classification

Open Data	Data that can be shared openly, either at the aggregate or individual level, based on state and federal law.
Restricted Data	Data that can be shared, but only under specific circumstances with appropriate safeguards in place.
Unavailable Data	Data that cannot or should not be shared, because of legal restriction or another reason (e.g., data quality concerns).

13

State & Federal Laws



What is consent?

What we are NOT talking about

Consent for Medical Treatment

Consent to participate in a study

What we ARE talking about

Consent to share data that contains personal identifiers

When consent is optional or where the law is unclear

When is consent required?

Generally, personally identifiable data cannot be shared unless:

you have consent

or

pursuant to an enumerated purpose or exception

When is consent NOT required?

What are the exceptions to consent to use student data from education records?

- **Properly de-identified an/or aggregated data**
- **School Official**
- **Audit & Evaluation**
- **Studies**
- **Directory Information**

PII can be shared without consent to….

Who is a “school official?”

- **Performs a service/function that an employee for the school would otherwise perform**
- **Is under the direct control of the school/district pertaining to records**
- **Legitimate educational interest**

Teachers, counselors, principals, attorney, accountants, etc. are all “school officials” under FERPA

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

What is the “audit & evaluations” exception?

Data can be shared without consent with “authorized representatives” to:

- Audit or evaluate a federal or state education program, or
- Enforce or comply with federal legal requirements

Written agreement required

(34 CFR §§ 99.31(a)(3), 99.35)

What is the “studies” exception?

Data can be shared without consent to conduct studies for or on behalf of schools, school districts, or postsecondary institutions

Studies must be for the purpose of:

- Developing, validating, or administering predictive tests
- Administering student aid programs
- Improving instruction

Written agreement required

Does the study have to be initiated by the education unit?	NO!
Does the unit have to agree with the findings?	NO!

(34 CFR §§ 99.31(a)(3), 99.35)

Directory Information

PII that would not be considered an invasion of privacy or harmful if disclosed

- Schools must provide notice about what items are "directory information"
- Parents can opt out
- Directory information is shared for things like yearbooks, PTO, class rings, scholarship directories

Examples of Directory Information

- student's name
- address
- telephone listing
- email address
- photograph
- date and place of birth
- major field of study
- grade level
- dates of attendance,
- participation in sports,
- awards and honors,
- most recent school or district attended

(34 C.F.R. § 99.3)

What are the exceptions to consent to use protected health information?

- **De-identified or Aggregate Data**
- **TPO (Treatment, Payment, Operations)**
- **Public Health Activities**
- **Health Oversight**
- **Research**
- **Avert Serious Threat to Health or Safety**

PHI can be shared without authorization for….

De-Identified & Aggregate Data

Under HIPAA, health information is de-identified if it does not identify an individual and if the covered entity has no reasonable basis to believe it can be used to identify an individual

(45 CFR 164.514(a))

Treatment, Payment & Operations (TPO)

Treatment

- Provision, coordination, or management of health care and related services for a patient (includes consultation, referrals) (45 CFR § 164.506)

Payment

- Obtain payments, premiums, determine coverage and provision of benefits, obtain reimbursement for health care (45 CFR § 164.506)

Health care operations

- Quality assessment and improvement activities, performance evaluation, credentialing, and accreditation; medical reviews, audits, or legal services, and compliance programs; insurance functions, such as underwriting, risk rating, and reinsuring risk; business planning, development, management, and administration; and administrative activities (de-identifying protected health information, creating a limited data set, and certain fundraising for the benefit of the covered entity) (45 CFR § 164.506)

Public Health Activities

PHI can be disclosed without consent to public health authorities and certain individuals for:

- Public Health Surveillance
- Preventing Child Abuse or Neglect
- Quality, safety or effectiveness of a product or activity regulated by the FDA
- Persons at risk of contracting or spreading a disease
- Workplace medical surveillance

Note: Some state laws restrict/do not allow PHI to be shared for these activities.

(45 CFR § 164.512)

What is a Public Health Authority?

An agency or authority of a federal, state, local, territorial or tribal government that is responsible for public health matters as part of its official mandate (includes agents and contractors of the public health authority)

(45 CFR § 164.501)

Health Oversight Activities

PHI can be disclosed to Health Oversight Agencies for oversight activities of:

1. The health care system
2. Eligibility determinations for government benefit programs
3. Compliance with government regulatory programs
4. Compliance with civil rights laws where PHI is necessary to determine compliance

Oversight Activities can include:

- audits
- civil, administrative, or criminal investigations
- inspections
- licensure or disciplinary actions;
- civil, administrative, or criminal proceedings or actions

45 CFR § 164.512(d)

Research

PHI can be shared without consent…

In preparation for research
(45 CFR § 164.512(i)(2))

Institutional Review Board (IRB) approval of waiver of authorization
(45 CFR § 164.512(i)(1))

Research on Decedents
(45 CFR § 164.512(i)(3))

Research Distinctions

Area of Distinction	HIPAA Privacy Rule	HHS Protection of Human Subjects Regulations Title 45 CFR Part 46	FDA Protection of Human Subjects Regulations Title 21 CFR Parts 50 and 56
Permissions for Research	Authorization	Informed Consent	Informed Consent
IRB/Privacy Board Responsibilities	Requires the covered entity to obtain Authorization for research use or disclosure of PHI unless a regulatory permission applies. Because of this, the IRB or Privacy Board would only see requests to waive or alter the Authorization requirement. In exercising Privacy Rule authority, the IRB or Privacy Board does not review the Authorization form.	The IRB must ensure that informed consent will be sought from, and documented for, each prospective subject or the subject's legally authorized representative, in accordance with, and to the extent required by, HHS regulations. If specified criteria are met, the IRB may waive the requirements for either obtaining informed consent or documenting informed consent. The IRB must review and approve the Authorization form if it is combined with the informed consent document. Privacy Boards have no authority under the HHS Protection of Human Subjects Regulations.	The IRB must ensure that informed consent will be sought from, and documented for, each prospective subject or the subject's legally authorized representative, in accordance with, and to the extent required by, FDA regulations. If specified criteria are met, the requirements for either obtaining informed consent or documenting informed consent may be waived. The IRB must review and approve the Authorization form if it is combined with the informed consent document. Privacy Boards have no authority under the FDA Protection of Human Subjects Regulations.

Source: Protecting Personal Health Information in Research: Understanding the HIPAA Privacy Rule, NIH 03-5388

Serious Threat to Health or Safety

PHI can be shared to prevent a serious and imminent threat to a person or the public, when disclosure is made to someone they believe can prevent or lessen the threat (including the target of the threat)

(45 CFR § 164.512(j))

How do I get consent?

How do I get permission under HIPAA?

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]

How do I get authorization under HIPAA?

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

How do I get consent under FERPA?

Figure 3: FERPA Elements for Consent

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

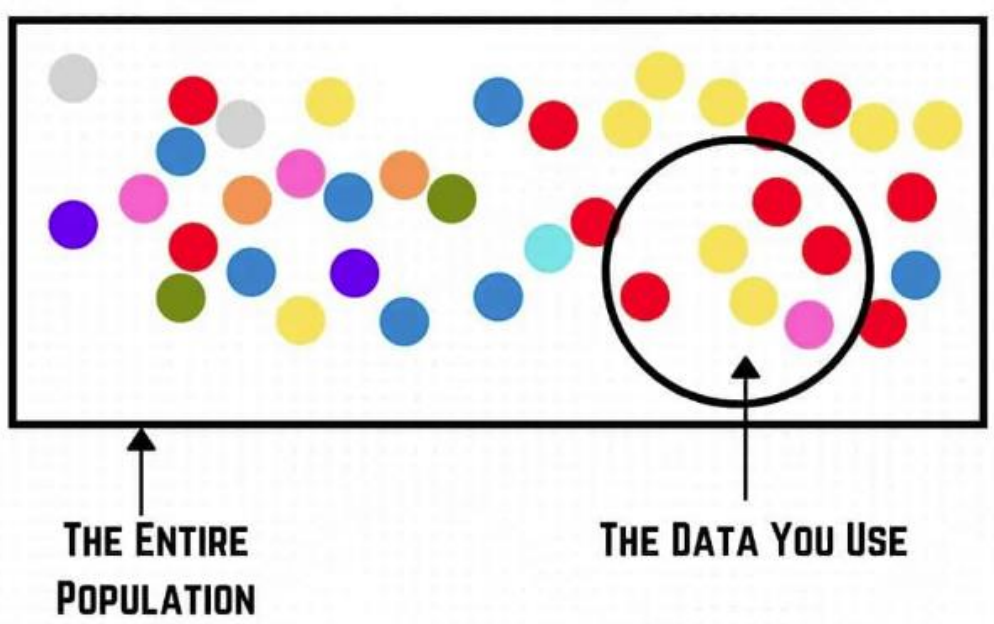
- Signature and date
- The purpose of the disclosure
- Description of the records that may be disclosed
- The name of the party or class of parties to whom the disclosure may be made

Practical & Ethical Problems of Consent

Practical Problems

Bias

Consent management



Ethical Problems

- **Erasure**
- **Surveillance**
- **Comprehension**
- **Undue Influence**
- **Coercion**

RESPECT FOR PERSONS	JUSTICE	BENEFICENCE
Privacy must be protected	Risks and benefits must be fairly distributed	Benefits must outweigh risks

Racial Equity & Consent

The New York Times

Indian Tribe Wins Fight to Limit Research of Its DNA

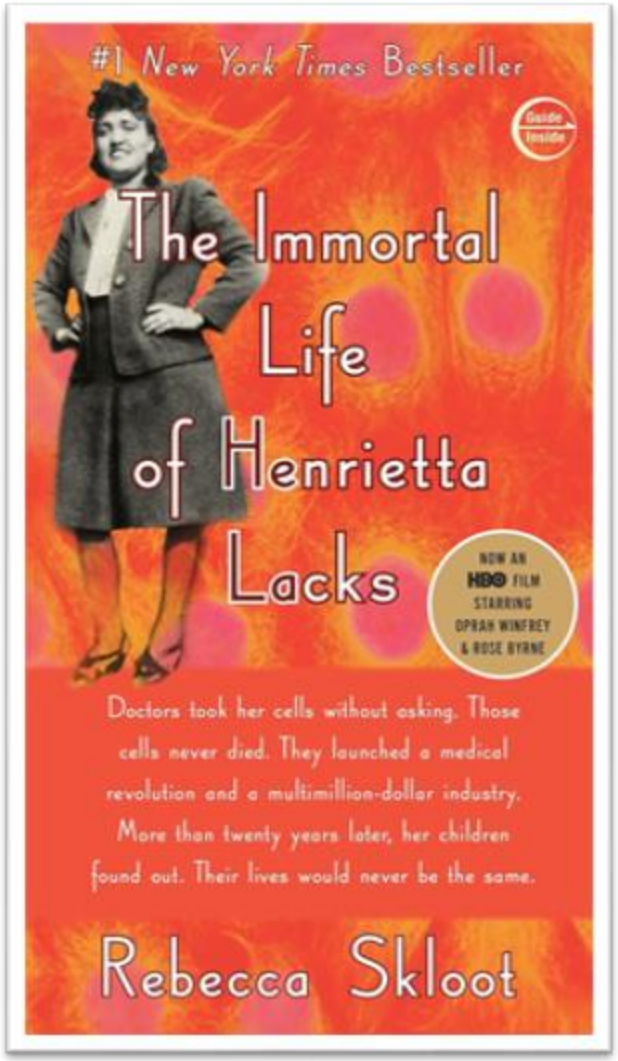
Give this article 321

Edmond Tilousi, 56, who can climb the eigh miles to the rim of the Grand Canyon in three hours.
Jim Wilson/The New York Times

By Amy Harmon
April 21, 2010

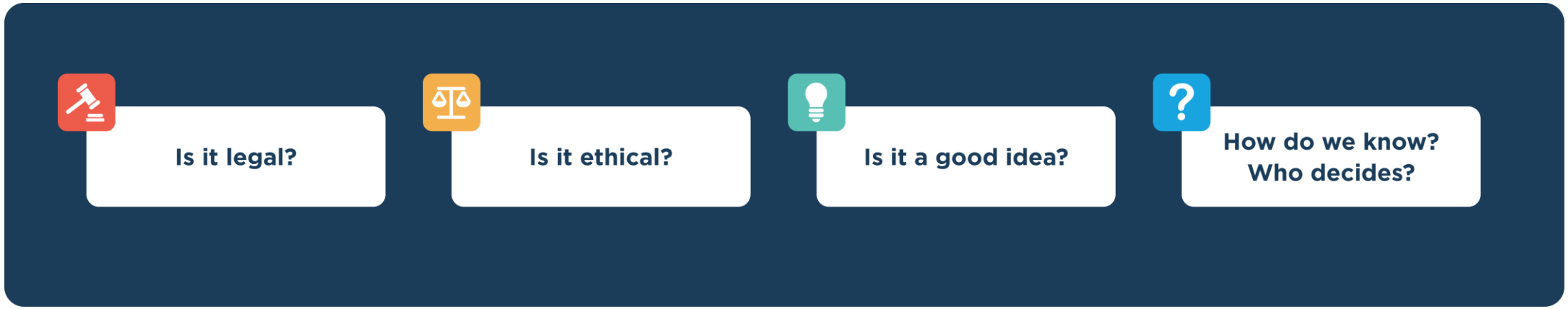
See how this article appeared when it was originally published on NYTimes.com.

SUPAI, Ariz. — Seven years ago, the Havasupai Indians, who live amid the turquoise waterfalls and red cliffs miles deep in the Grar Canyon, issued a "banishment order" to keep Arizona State University employees from setting foot on their reservation — an ancient punishment for what they regarded as a genetic-era betrayal.



What might ethical consent look like?

Why: The Four Questions



The Four Questions

	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]

Consent Framework

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

Alternatives to Consent

Anonymization & De-identification

Apply techniques to remove or obscure personal identifiers to prevent re-identification of individuals.

Balancing Risk and Use

Adapted from A Visual Guide to Practical De-Identification, FPF.org

DEFINITION

What are **privacy preserving technologies?**

Privacy Preserving Technologies

Also referred to as privacy-enhancing technologies (PETs), PPTs are technical approaches that **minimize use of and need for personal data**, including identifiers, **while supporting record linkage through privacy techniques**.

Common Privacy Enhancing Technologies

Secure Multiparty Computation

parties jointly compute a query on their datasets, without seeing the other's underlying data, using encryption

Secure Enclave

virtual computing workspace that enables authorized users to access sensitive data and securely conduct analysis

Differential Privacy

method for obscuring identities or attributes in the underlying record-level data by infusing results or statistics with noise

Secure Hashing

an algorithm that replaces sensitive information with a random string of characters (hash) unique to each original record in the data

MAY 15, 2025

1:00 PM ET

JOIN US for **Demystifying Privacy Enhancing Technologies** Workshop

Questions?

Thank you.

Amy Hawn Nelson
AISP
ahnelson@upenn.edu

Deja Kemp
AISP
dejak@upenn.edu

A Project of WestEd

Penn University of Pennsylvania