Federal Privacy Basics: FERPA 101 & HIPAA101

Deja Kemp, JD
Director of Legal Policy
Actionable Intelligence
for Social Policy (AISP)

Sean Cottrell
Director
Data Integration Support
Center (DISC) at WestEd

TELL US IN THE CHAT:
What do you hope to get out of today's training?

Agenda

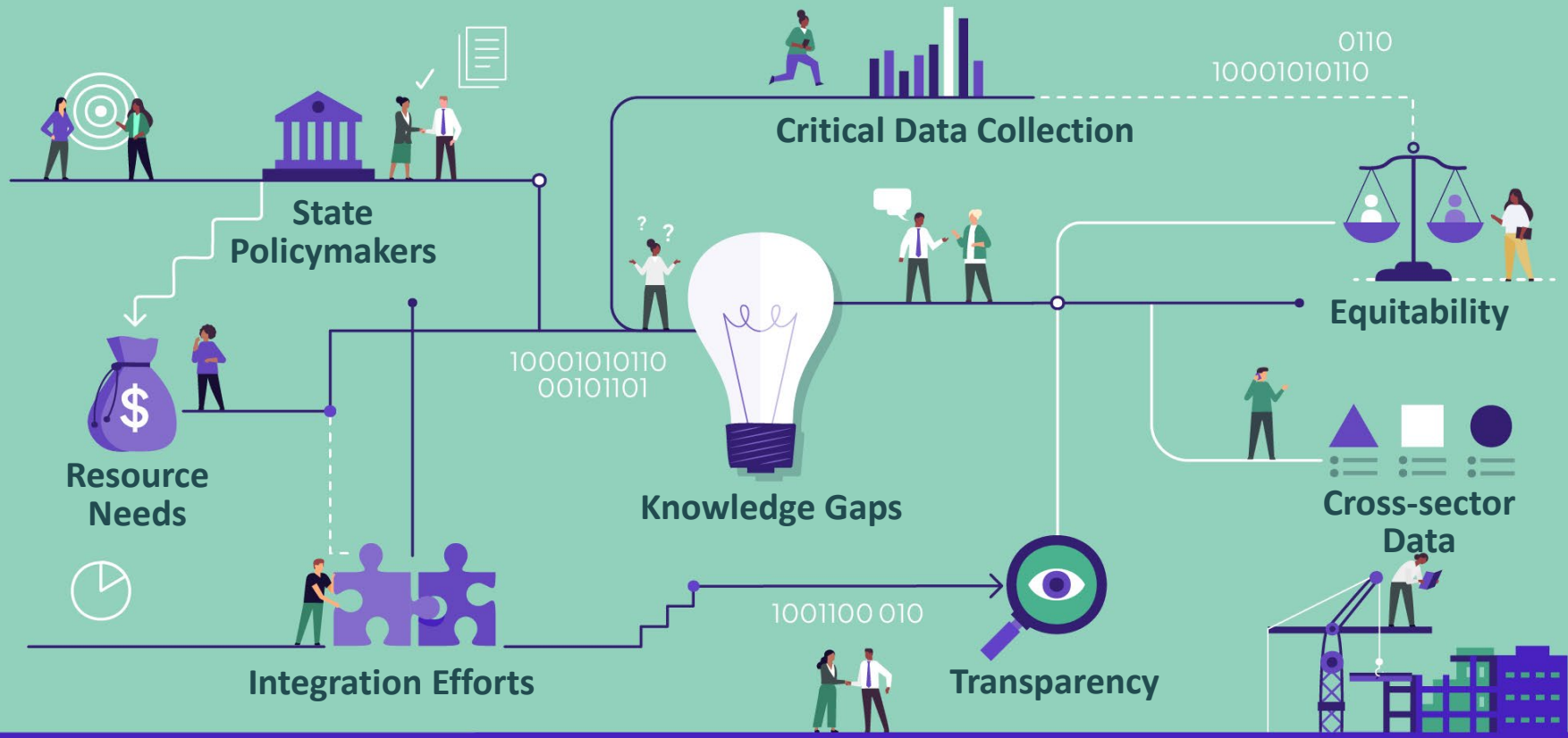
- Introductions and Overview of AISP & DISC (3 minutes)
- Disclaimer & Roadmap (2 minutes)
- Nuts & Bolts of FERPA (25 minutes)
- Nuts & Bolts of HIPAA (25 minutes)
- Questions (5 minutes)


Helping state and local governments collaborate and responsibly use data to improve lives.
LEARN MORE →
www.aisp.upenn.edu

AISP

disc
Data Integration Support Center
WestEd

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.

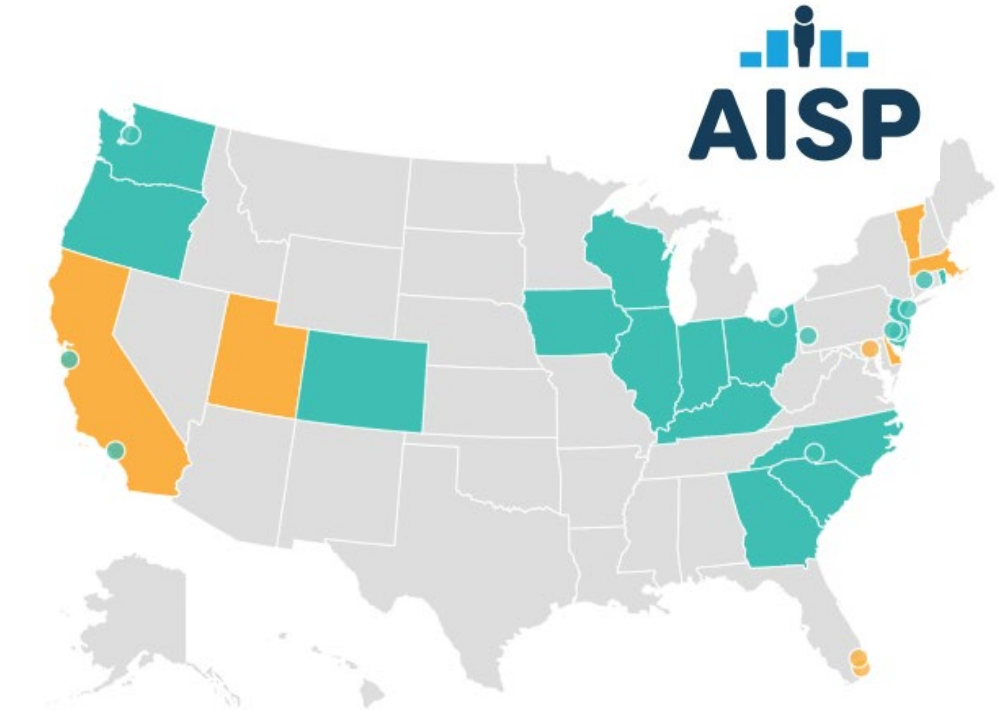


Our roles

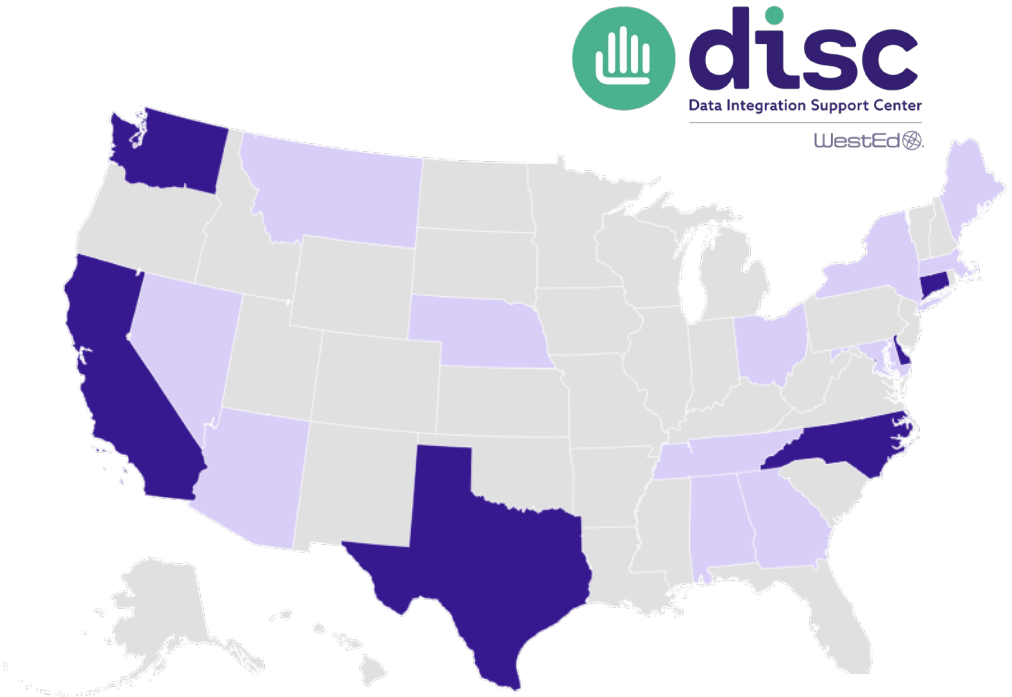
We are:
Data evangelists
Connectors, community builders, thought partners, cheerleaders, and data sharing therapists
Focused on ethical data use for policy change

We are not:
Data holders or intermediaries
A vendor or vendor recommender
Focused on academic research

Our Networks



Network Sites Developing Sites



Intensive TA support Moderate TA support

What we do

AISP	DISC
Peer Network	Planning & User-Centered Design
Guidance & Standards	Legislative Analysis
Training & Consulting	External Legal Supports
Advocacy & Communications	Privacy
Actionable Research	System Security

Our approach

Data sharing is as relational as it is technical.

We don't just need to integrate data;

we need to integrate people.

When we talk about IDS, what do we mean?

We're talking about the whole person, not tech solutions

Efforts that link administrative data across sectors or agencies and over time

Efforts that curate data that are relevant and high-quality

Efforts that serve as a public utility (not research for research's sake)

Efforts that have defined governance structures (data only used for approved uses)

When we bring data together, we can better:

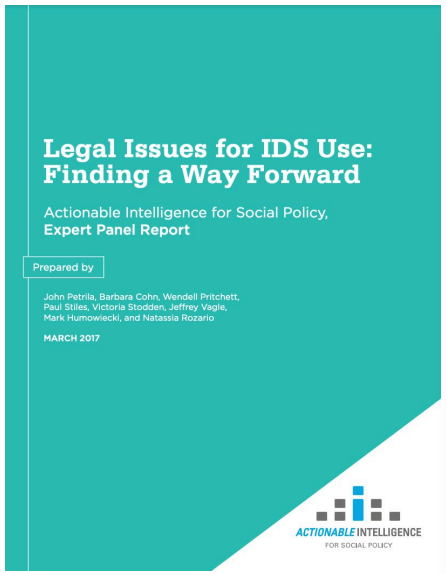
- Understand the complex needs of individuals and families
- Allocate resources where they're needed most to improve quality and equity of services
- Measure long-term impacts of policies and programs
- Engage in transparent, shared decision-making about how data should (and should not) be used

LEGAL DISCLAIMER

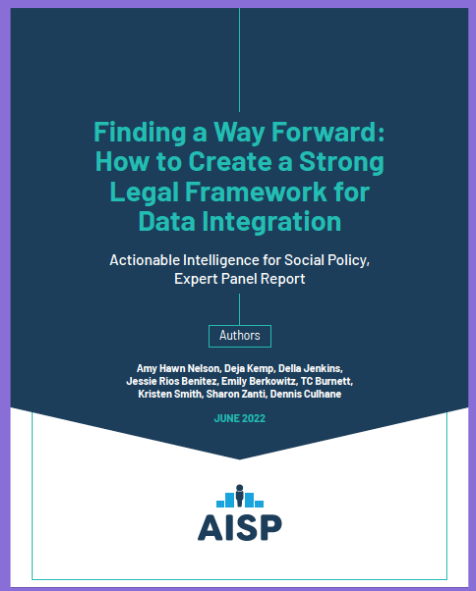
- Not Legal Advice
- Training will only cover **federal law**
- Laws change, this is based on the law at the time of the training
- Consult your general counsel for specific legal questions

Road Map

Legal Publications



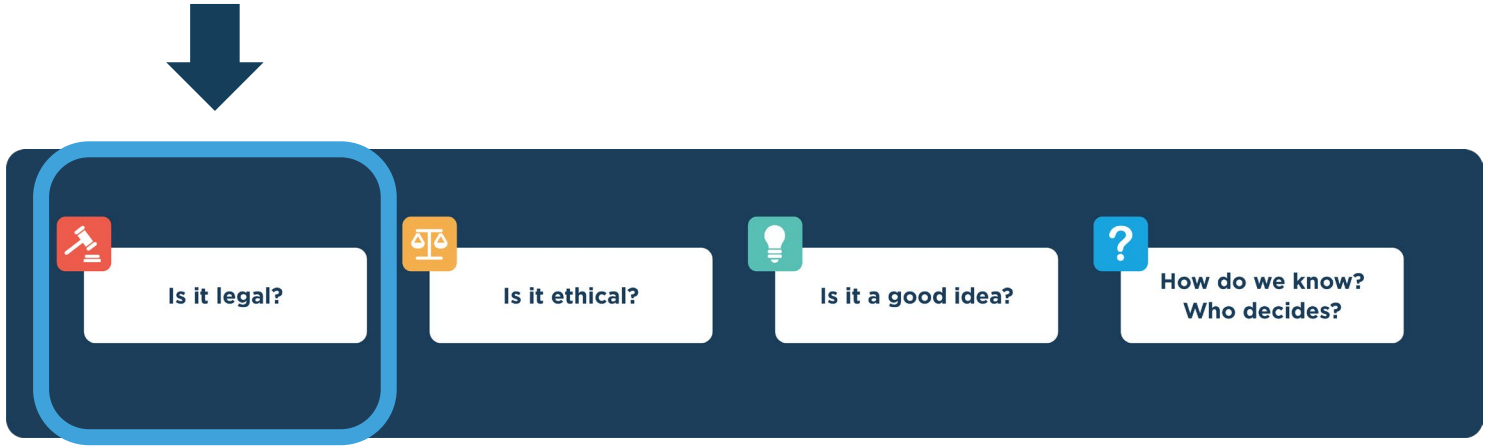
2017



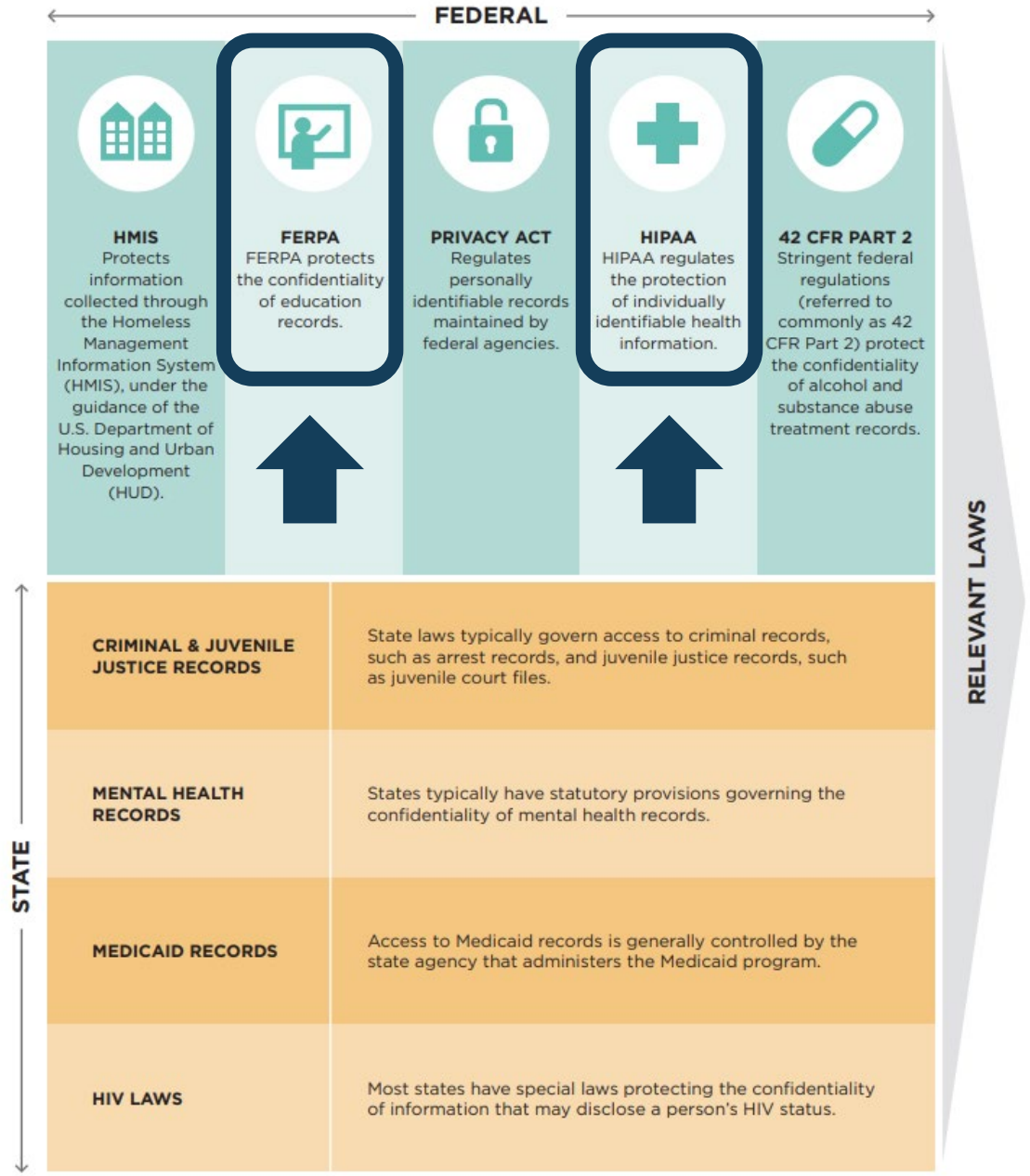
2022

2023

Why: The Four Questions



State & Federal Laws



ESSENTIAL QUESTIONS

What is FERPA and how does it impact data sharing and integration?

What types of data does FERPA protect?

How can you work with student data without consent?

What is HIPAA and how does it impact data sharing and integration?

What types of data does HIPAA protect?

How can you work with health data without consent?

NUTS & BOLTS OF FERPA

Sean Cottrell

What is FERPA?

Family Educational Rights Privacy Act (20 U.S.C. §1232g & 34 CFR Part 99)

Protects the confidentiality of education records

Guarantees parents and eligible students certain rights over their education records

What does FERPA protect?

Personally identifiable information (PII) in education records

What is “PII”?

Personally identifiable information that is linked or linkable to a specific student (34 C.F.R. § 99.3)

Includes Direct & Indirect Identifiers

Direct	Indirect
Name	Place of Birth
Unique Identification Numbers	Race
Address	Religion
Date of birth	Weight

What is an “education record”?

Directly related to the student

Maintained by (or on behalf of) an educational agency or institution

20 U.S.C.A. § 1232g(a)(4)(A)(i)-(ii)

What is an “education record”?

Education Records *protected under FERPA*	**Not Education Records** *not protected under FERPA*
Transcripts	Records that are kept in the sole possession of the maker and used only as personal memory aids
Disciplinary records	Law enforcement unit records
Standardized test results	Grades on peer-graded papers before they are collected and recorded by a teacher
Health and family history records	Records created or received by a school after an individual is no longer in attendance and that are not directly related to the individual’s attendance at the school
Records on services provided to students under the Individuals with Disabilities Education Act (IDEA)	Employee records that relate exclusively to an individual in that individual’s capacity as an employee
Records on services and accommodations provided to students under Section 504 of the Rehabilitation Act of 1973 and Title II of the Americans with Disabilities Act (ADA)	Information obtained from a school official’s personal knowledge/observation

Source: National Center for School Safety

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

(34 C.F.R. § 99.3)

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

When can someone other than a parent or eligible student access PII?

Consent

Exception

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

How can I work with student data from education records without consent?

- **Properly de-identified or Aggregate data**
- **School Official**
- **Audit & Evaluation**
- **Studies**

PII can be shared without consent to….

De-identification Techniques

Redaction

Suppression

Blurring

Masking

Subsampling

No required de-identification technique under FERPA

Table of De-Identification Techniques

Name of Technique	Description / Examples	Pros	Cons
Redaction	**Erasing or expunging** sensitive data from a record.	Reduces risk if data are disclosed inadvertently or through unauthorized access; useful when the erased data elements are not needed for analysis (typical with direct identifiers).	Not effective if done improperly (e.g., if the erasure can be reversed or if enough indirect identifiers remain).
Suppression	**Removing** data (e.g., from a cell or row in a table, or data element(s) in a record) prior to dissemination to prevent the identification of individuals in small groups or those with unique characteristics. Examples: • Suppressing the value of a single field, such as a field in a patient record containing a very rare disease. • Not reporting observations for those patients where the number of patients for any combination of zip code, age, and diagnosis is below a given threshold (e.g., 5 people).	Useful when multiple indirect identifiers pose a risk for re-identification. More easily done with tabular data. Helpful when presenting analysis of findings to the institution that provided the data. Helpful in public health reporting.	May result in minimal data being produced for small populations, and it usually requires additional suppression of non-sensitive data to ensure adequate protection of PII (e.g., complementary suppression of one or more non-sensitive cells in a table so that the values of the suppressed cells may not be calculated by subtracting the reported values from the row and column totals). Can be difficult to perform properly. Is less likely to be effective if there are additional data available elsewhere.
Blurring: • Aggregation • Generalization • Pixelation	**Reducing precision** of data **by combining** one or more data elements. **Aggregation:** combining individual subject data with a sufficient number of other subjects to disguise the attributes of a single subject (e.g., reporting a group	Minimizes risk of identification by focusing on collective data rather than individual data. Useful for "big picture" analyses.	Decreases reliability of data and increases potential for false conclusions. Aggregation: may not be possible with a small pool of subjects.

Who is a "school official?"

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

- 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

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
- Enforce or comply with federal legal requirements

**Written agreement required*

(34 CFR §§ 99.31(a)(3), 99.35)

What is an “education program”?

Any program principally engaged in providing education

Examples of an “Education Program”

- early childhood education
- elementary and secondary education
- postsecondary education
- special education
- job training
- career and technical education
- adult education
- any program administered by an educational agency or institution

(34 C.F.R. § 99.3)

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

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

Written agreement required

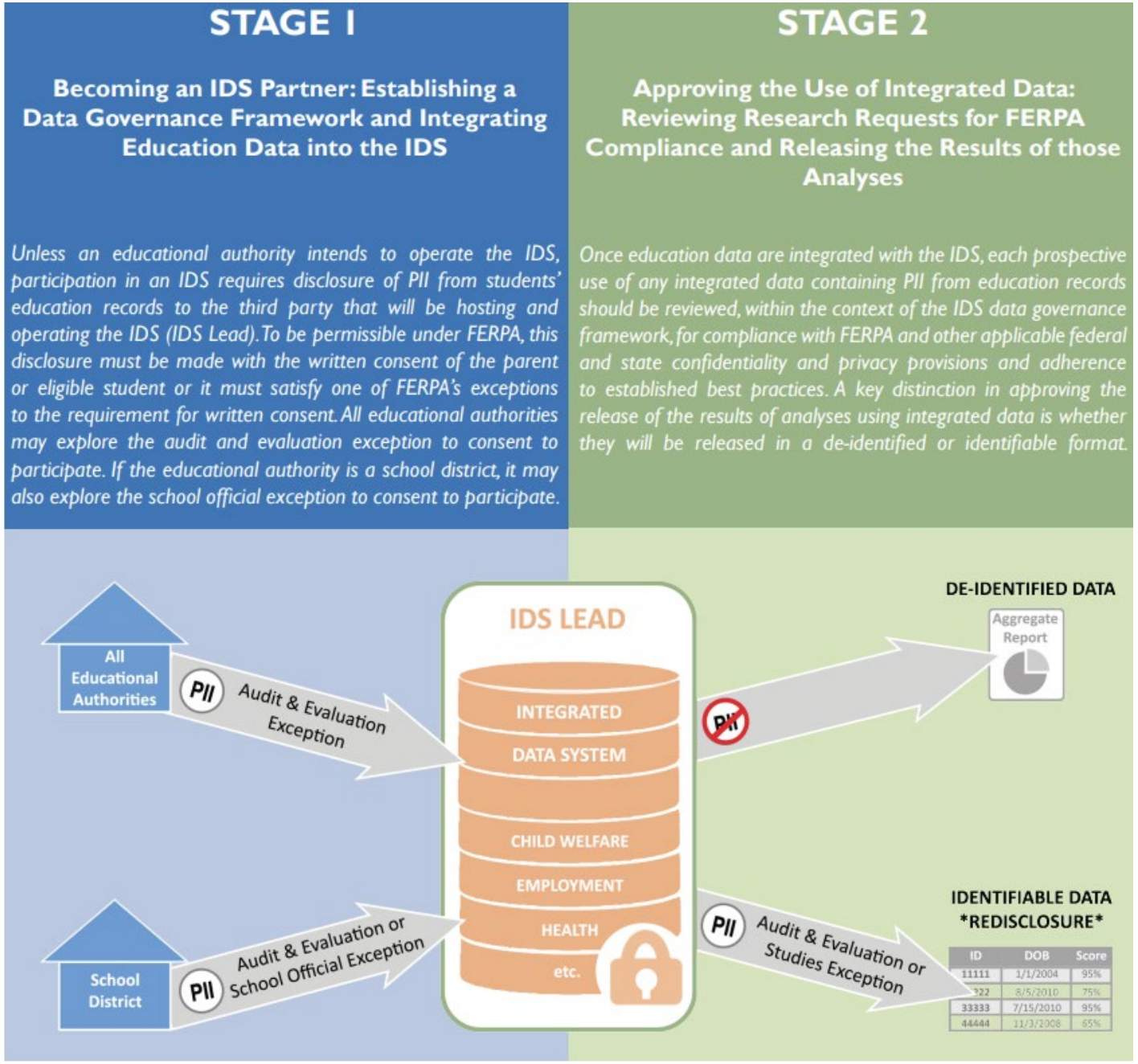
(34 CFR §§ 99.31(a)(3), 99.35)

REMEMBER

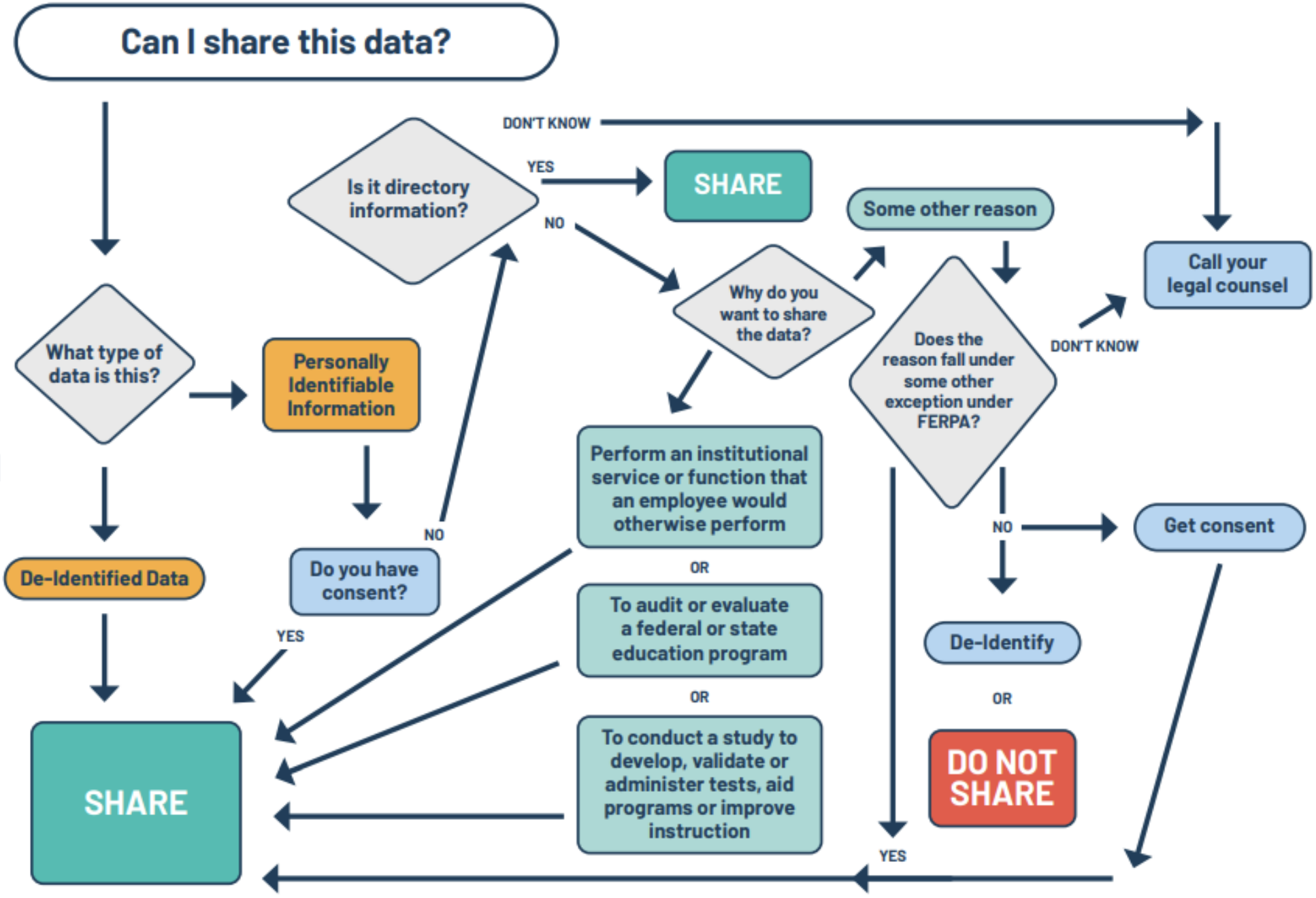
There is no “operational use” exception under FERPA

There is no “research exception” under FERPA

How do these exceptions work in the data sharing world?



Decision Matrix



NUTS & BOLTS OF HIPAA

Deja Kemp

What is HIPAA?

Health Insurance Portability and Accountability Act (Public Law 104-191. 42 U.S.C. §1320d

The Privacy Rule (45 CFR § §160, 164)

The Security Rule: 45 CFR Part 160 and Subparts A and C of Part 164;

The Enforcement Rule: 45 CFR Part160 Subparts C, D, and E.

Protects the confidentiality of individual health information

Gives patients a right to access their records

What does HIPAA protect?

Protected Health Information (PHI) that is created or received by a covered entity

What is a “covered entity”?

- **health plans**
- **health care clearinghouses**
- **health care providers who electronically transmit any health information in connection with transactions for which HHS has adopted standards.**

(45 CFR § 160.103)

(45 CFR § 160.103)

What is a “covered entity”?

A Covered Entity is one of the following:

A Health Care Provider	A Health Plan	A Health Care Clearinghouse
This includes providers such as: • Doctors • Clinics • Psychologists • Dentists • Chiropractors • Nursing Homes • Pharmacies ...but only if they transmit any information in an electronic form in connection with a transaction for which HHS has adopted a standard.	This includes: • Health insurance companies • HMOs • Company health plans • Government programs that pay for health care, such as Medicare, Medicaid, and the military and veterans health care programs	This includes entities that process nonstandard health information they receive from another entity into a standard (i.e., standard electronic format or data content), or vice versa.

Source: Covered Entities and Business Associates | HHS.gov

What is “PHI”

Individually identifiable health information held or transmitted by a covered entity or its business associate (45 CFR § 160.103)

What is “individually identifiable health information”?

Information, including demographic data, that relates to:

- the individual's past, present or future physical or mental health or condition,
- the provision of health care to the individual, or
- the past, present, or future payment for the provision of health care to the individual,
- and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual.

(45 CFR § 160.103)

Who is a “business associate?”

Performs a function/activity that involves the use of PHI (legal, actuarial, accounting, consulting, data aggregation, administrative, financial, management, accreditation)

An employee is NOT a business associate

(45 CFR § 160.103)

What is NOT covered under HIPAA?

De-identified & Aggregate Data

Education Records (ie. School Health Records)

Employment Records (Employee benefits)

PHI shared with non-covered entities (Mobile Health App)

(45 CFR § 160.103)

When can someone other than a patient access PII?

Permission (Authorization or Consent)

Permitted or required use (exception)

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?

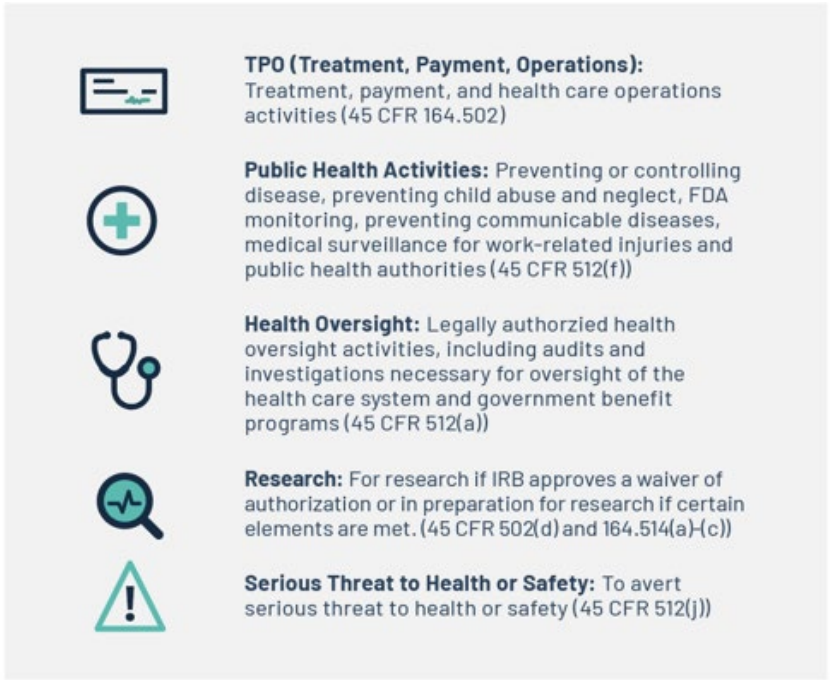
Figure 4: **HIPAA Elements for Authorization**

- 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 can I work with health data without consent?

- **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….



Limiting Uses and Disclosures to the Minimum Necessary

A covered entity must make reasonable efforts to use, disclose, and request only the minimum amount of protected health information needed to accomplish the intended purpose of the use, disclosure, or request.

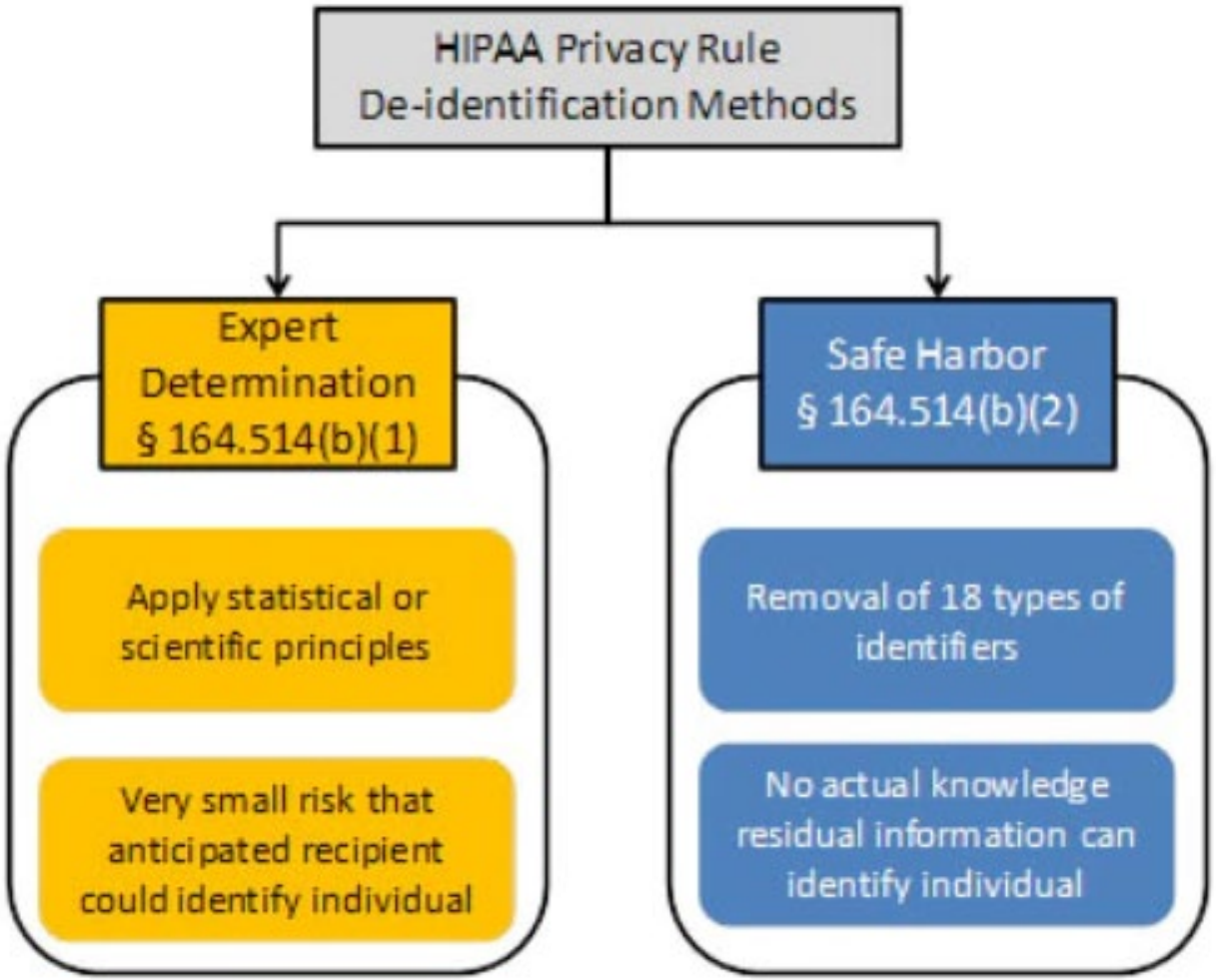
(45 CFR 164.502(b), 164.514(d))

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))

Methods for De-identification



Source: https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html#standard

Safe Harbor

PHI can be used without consent using the Safe Harbor Method, which involves the removal of 18 identifiers

Could a patient's initials or the last four digits of a SSN be disclosed under Safe Harbor?
No!

18 identifiers that must be removed under Safe Harbor:

1. Names
2. Account numbers
3. Biometric identifiers
4. Certificate and License numbers
5. Dates, such as discharge dates, except the year
6. Device identifiers and serial numbers
7. Email addresses
8. Fax numbers
9. Full face photos and comparable images
10. Geographic data, including geographic units, formed
11. Health plan beneficiary numbers
12. Internet protocol addresses
13. Medical record numbers
14. Social Security numbers
15. Telephone numbers
16. Vehicle identifiers and serial numbers, including license plates
17. Web URLs
18. Any unique identifying number characteristic or code

EXPERT DETERMINATION

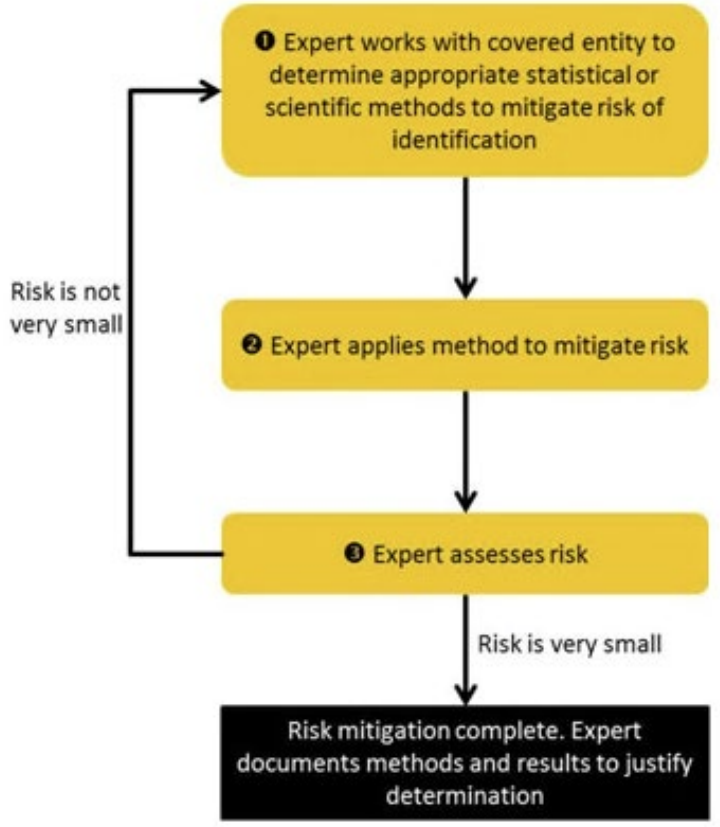
A method of identification where an expert applies statistical and scientific principals to determine that the risk of identification is very small and justifies that determination with documentation (45 CFR 164.514(b))

Who is an “expert”?

A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable.

There is no specific professional degree or certification program for designating who is an expert at rendering health information de-identified.

(45 CFR 164.514(b)(1))



Source: https://www.hhs.g professionals/privacy/special-topics/de-identification/index.html#standard

LIMITED DATA SET

Limited data sets may include only the following identifiers: Dates, such as admission, discharge, service, and date of birth, city, state, and zip code (not street address), age.

- Limited data set IS PHI.
- De-identified data ≠ Limited Data Set
- Needs a Data Use Agreement

(45 CFR 164.514(e)(1))

A Limited Data Set MUST exclude the following identifiers:

- Names
- Postal address information, other than town or city, State, and zip code
- Telephone numbers
- Fax numbers
- Electronic mail addresses
- Social Security numbers
- Medical record numbers
- Health-plan beneficiary numbers
- Account numbers
- Certificate and license numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers and serial numbers
- Web Universal Resource Locators (URLs)
- Internet Protocol (IP) address numbers
- Biometric identifies including fingerprints and voice prints
- Full-face photographic images and any comparable image

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: Many 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: https://privacyruleandresearch.nih.gov/pdf/HIPAA_Privacy_Rule_Booklet.pdf

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 these exceptions work in the data sharing world?

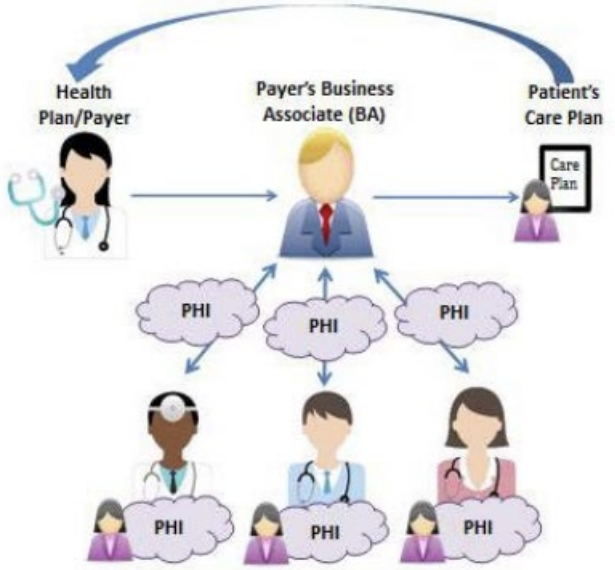


Figure 1: Case Management Scenario

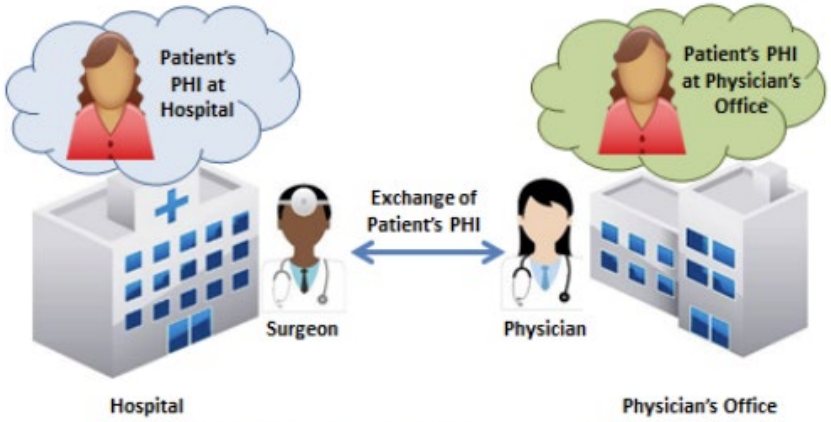
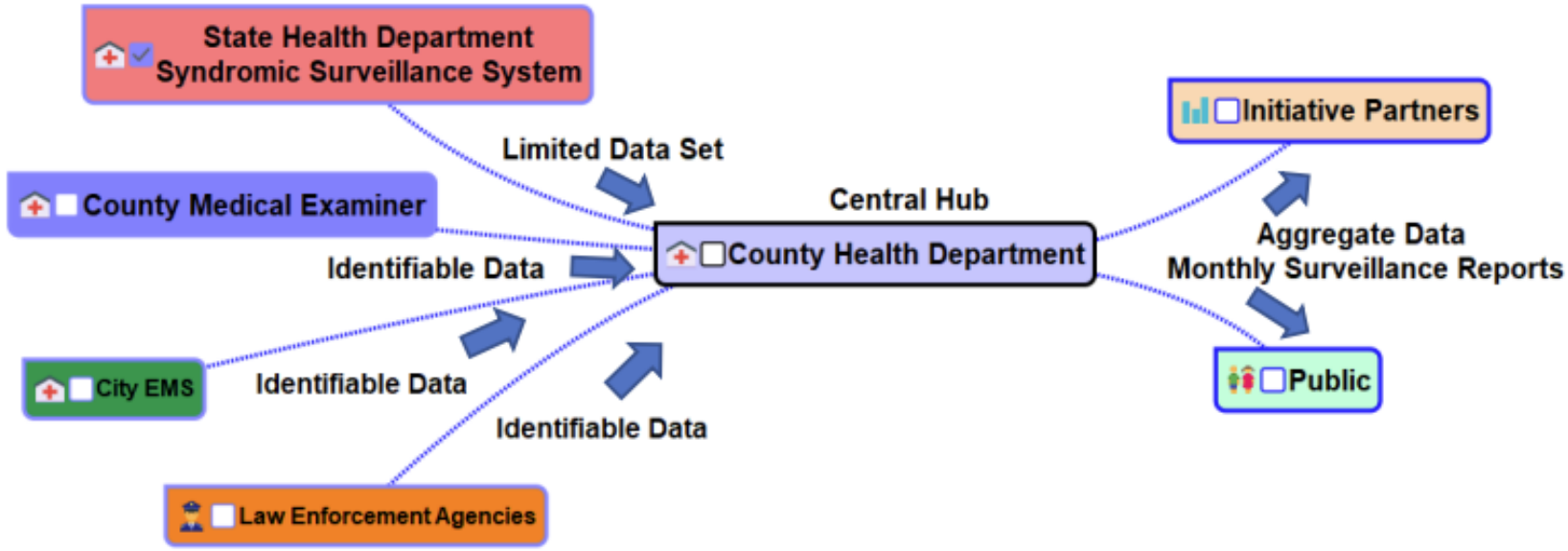


Figure 1: Hospital and Treating Physician exchange information scenario

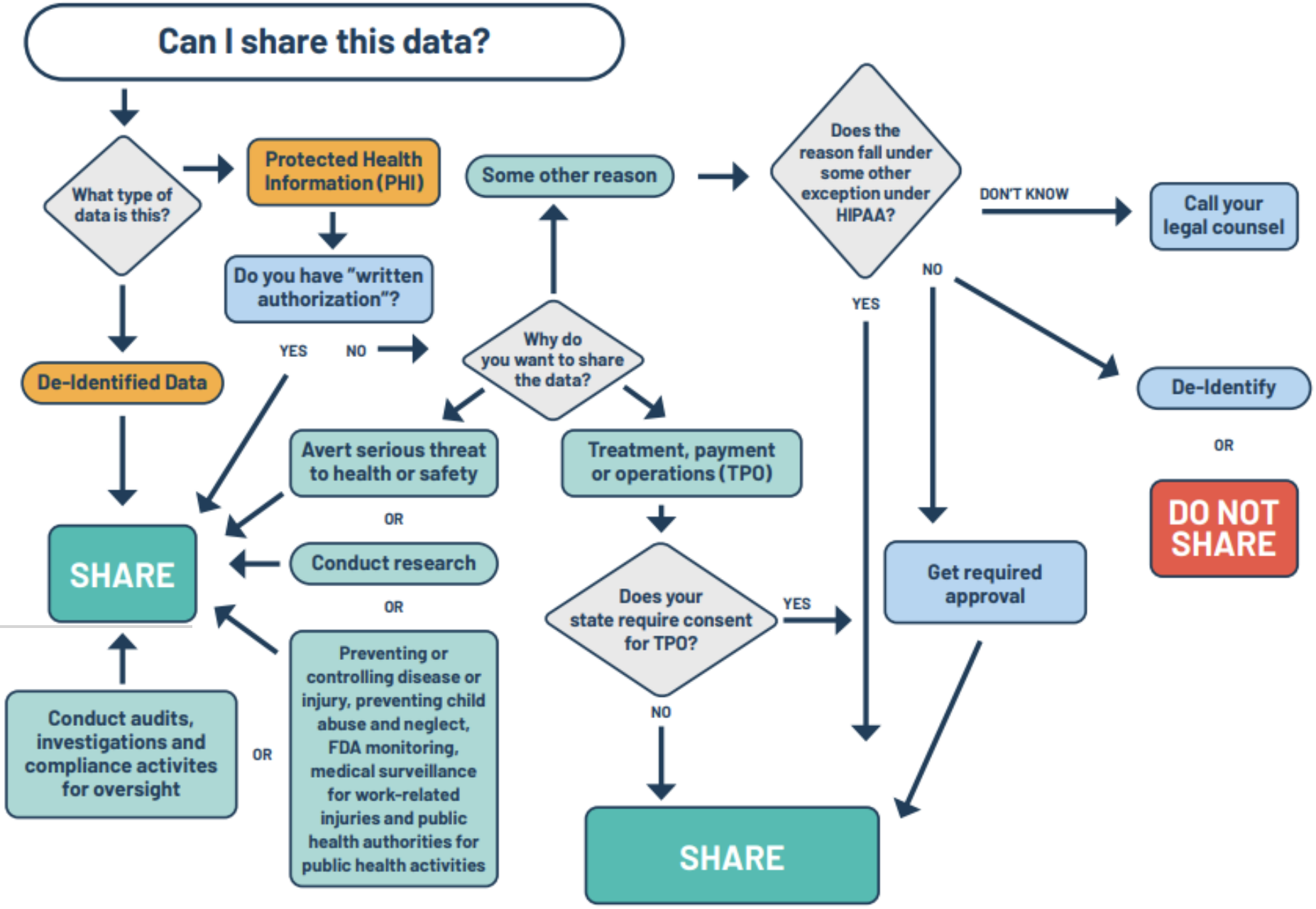
Source: https://www.hhs.gov/sites/default/files/exchange_treatment.pdf
https://www.hhs.gov/sites/default/files/exchange_health_care_ops.pdf

Example Use Case



Source: https://www.networkforphl.org/wp-content/uploads/2022/10/DASH_NPHL-Pathways_to_Yes-FINAL-PDF.pdf

Decision Matrix



Questions?

Closing Reflections

TELL US IN THE CHAT:

I used to think _____

but now I think _____.

Thank you.

Deja Kemp, JD

AISP Director of Legal Policy
dejak@upenn.edu

Sean Cottrell

DISC Director
scottrel@wested.org

A Project of