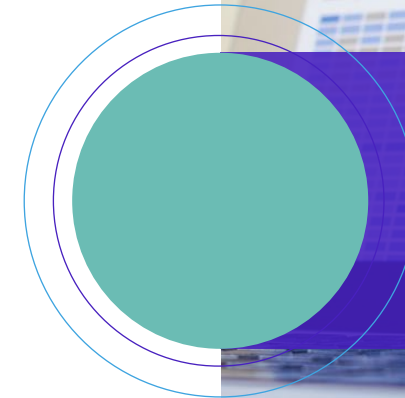




# Federal Privacy Basics: HMIS 101 & Privacy Act 101

---

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



URL or other link here optional

*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 HMIS (25 minutes)
- Nuts & Bolts of Privacy Act (25 minutes)
- Questions (5 minutes)



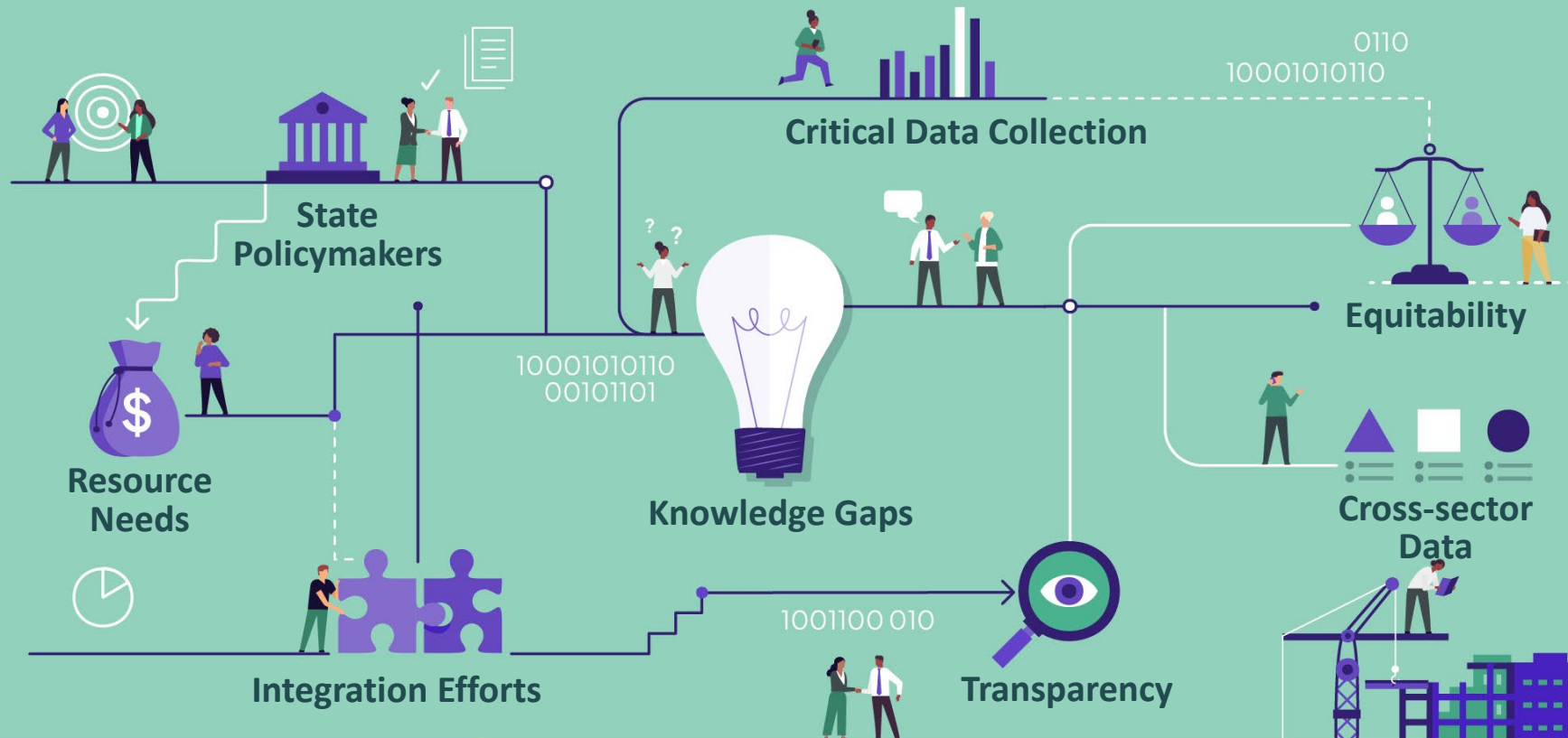
**Helping state and  
local governments  
collaborate and  
responsibly use  
data to improve  
lives.**

**LEARN MORE** →

[www.aisp.upenn.edu](http://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:

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

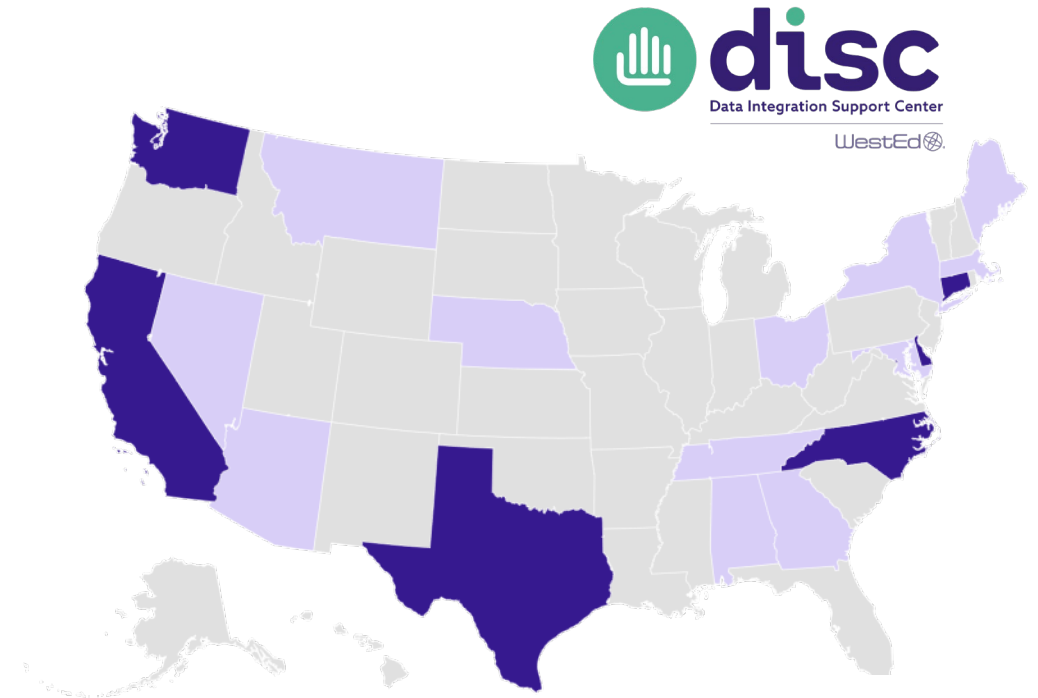
A vendor or vendor recommender

Focused on academic research

# Our Networks



● Network Sites    ● Developing Sites



● Intensive TA support    ● Moderate TA support



# What we do

## AISP

Peer Network

Guidance & Standards

Training & Consulting

Advocacy & Communications

Actionable Research

## DISC

Planning & User-Centered Design

Legislative Analysis

External Legal Supports

Privacy

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

---

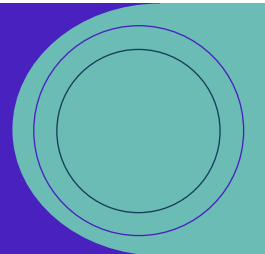
# LEGAL DISCLAIMER

- 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

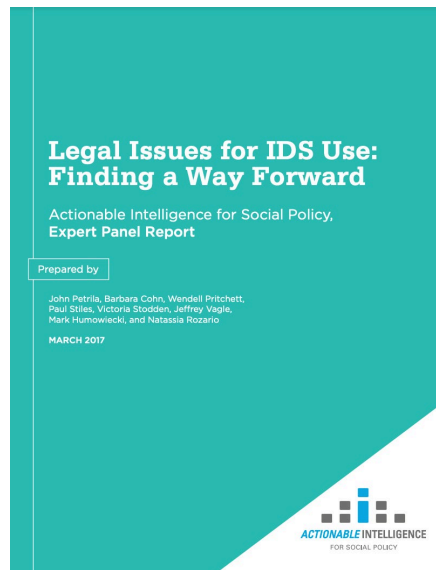


# Road Map

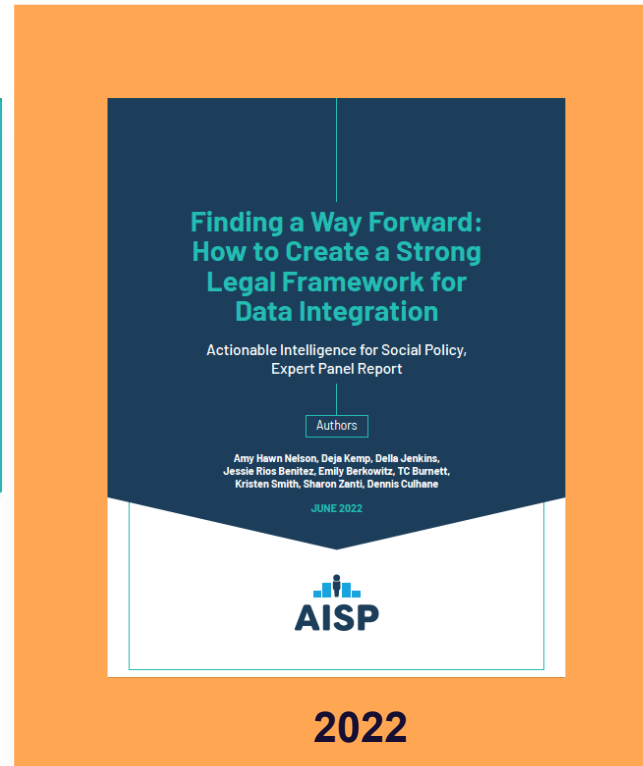
---



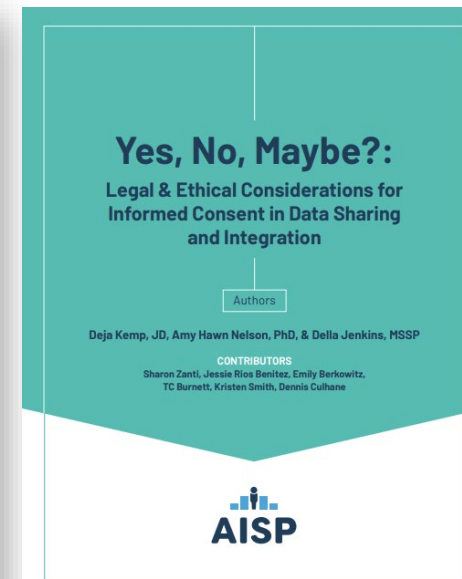
# Legal Publications



2017

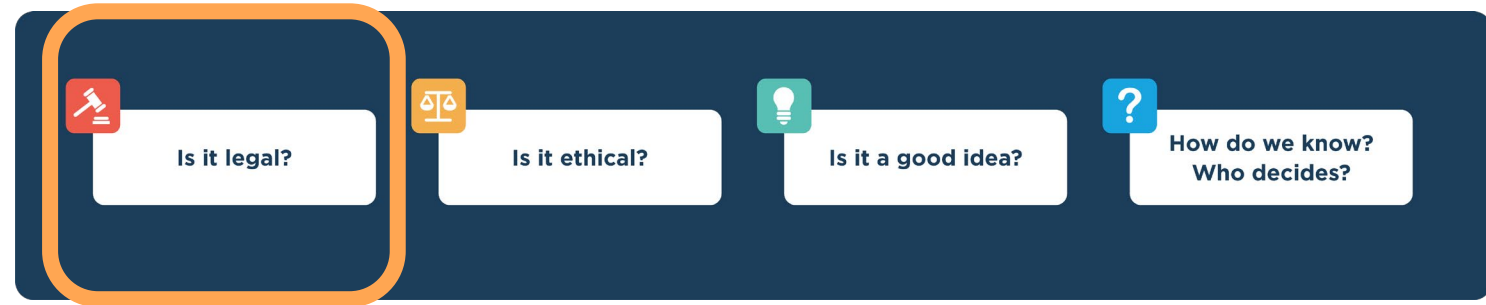


2022



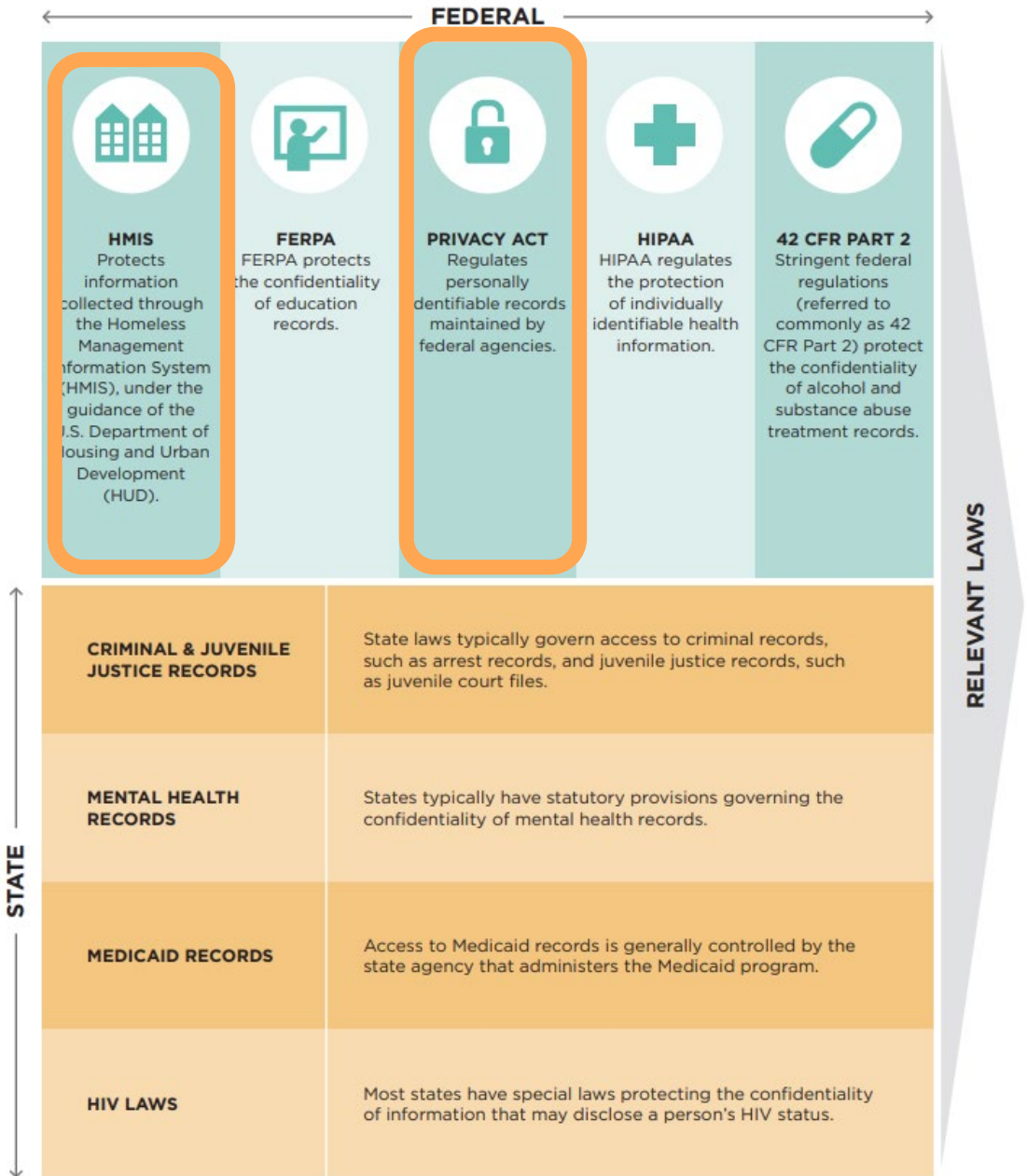
2023

# Why: The Four Questions





# State & Federal Laws



# ESSENTIAL QUESTIONS



What are Homeless Management Information Systems (HMIS) and what rules have the Housing and Urban Development (HUD) set to protect private information in HMIS?



What types of data does the HUD HMIS regulations protect?



In what circumstances can personal information under the HUD rules be shared without consent?



What is the Privacy Act?



What types of data does the Privacy Act protect?

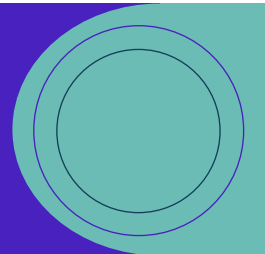


How can you share personal information under the Privacy Act without consent?



# NUTS & BOLTS OF HMIS

---



# What are Homeless Management Information Systems (HMIS)? What rules apply to HMIS?

- Homeless Management Information Systems (HMIS) are community-based systems to collect counts of individuals and families experiencing homelessness
- Homeless Emergency Assistance and Rapid Transition to Housing (HEARTH) Act of 2009 (Pub. L. No. 111-22, 123 Stat. 1669 (2009))
- HMIS Privacy and Security Standards (69 FR 45888)
- Protects the **confidentiality of personal information**
- Guarantees parents and eligible students certain **rights over their education records**



# What do the HUD rules protect ?

Protected **personal information (PPI)** that is created or maintained by or for a covered homeless organization about a living homeless individual

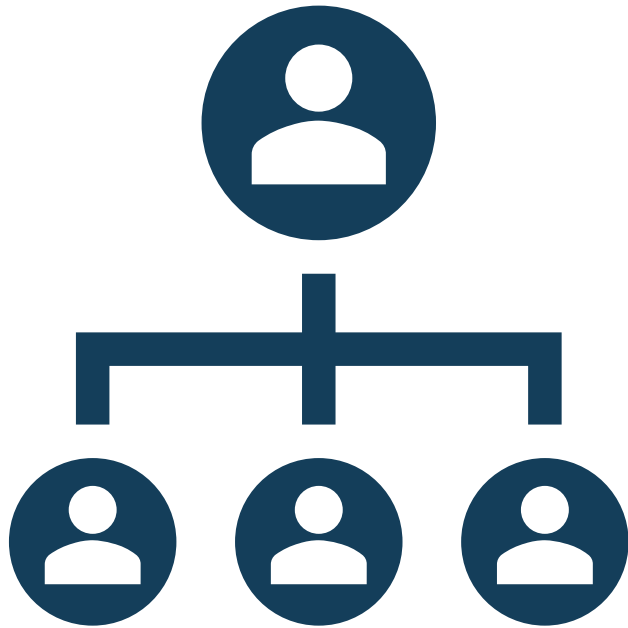
(Section 4.1.1 of HMIS Privacy Standards)

# What is “PPI”?

- 1) Identifies, either directly or indirectly, a specific individual;**
- 2) can be manipulated by a reasonably foreseeable method to identify a specific individual; or**
- 3) can be linked with other available information to identify a specific individual.**

**(Section 4.1.1 of HMIS Privacy Standards)**





## What is a “covered homeless organization” (CHO)?

**Any homeless organization that “records, uses or processes protected personal information on homeless clients for an HMIS.”**

**(Section 4.1.1 of HMIS Privacy Standards)**



# What is NOT covered under the HUD rules?



## De-identified & Aggregate Data



## PHI held by covered entities



Section 4.1.2 of HMIS Privacy Standards)

# When can someone other than a participant access PPI?

## Consent



## Exception



# Violence Against Women Act (VAWA) 34 U.S.C. 12291(b)(2)



**VAWA requires all grantees and subgrantees receiving VAWA funding from the Department of Justice, Office on Violence Against Women, to protect the confidentiality and privacy of persons receiving services**

**Can only share information in these three circumstances**

- Consent (written, informed, time limited)
- Statute
- Court Order

# Conflict of Law

## VAWA V. HUD

A Domestic violence shelter is subject to both VAWA and HUD rules. Which would trump and why?

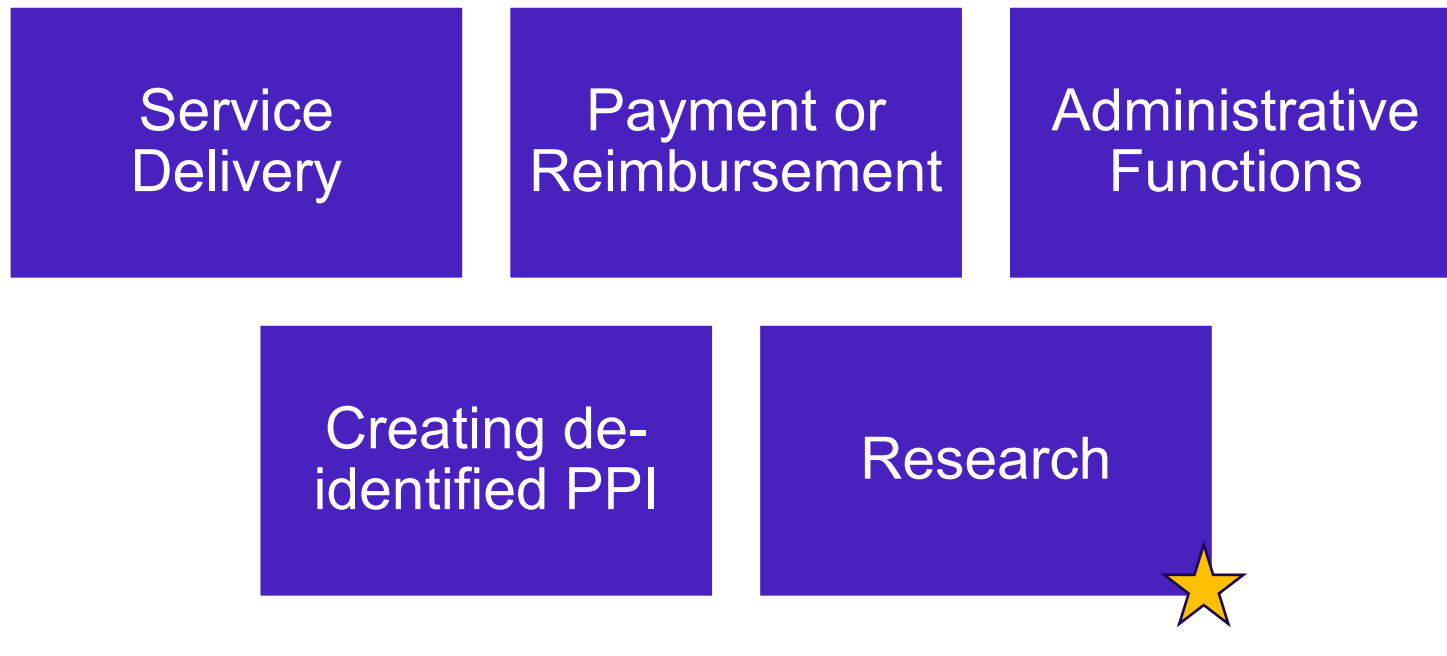
## Conflict of Law

- **VAWA preempts HUD rules because they are more restrictive**

### VAWA V. HUD

A Domestic violence shelter is subject to both VAWA and HUD rules. Which would trump and why?

# Exceptions to Consent under HMIS Rules



Section 4.1.3 of HMIS Privacy Standards)



## Creating De-Identified PPI

**PPI can be shared without consent for creating de-identified PPI.**

**(Section 4.1.3 of HMIS Privacy Standards)**



# De-identification & Aggregate Data

## Eight universal data elements


The HUD rules do not specify a process to render PPI de-identified.

### Universal Data Elements

- Name
- Social Security Number
- Date of Birth
- Zip code
- Program Entry Date
- Program Exit Date
- Unique Personal identification number
- Program identification Number


# De-Identification & Aggregation Case Study

CHARLOTTE-MECKLENBURG  
FAMILY HOMELESSNESS  
SNAPSHOT  
2014-2015



March 2017

McKinney-Vento | 2014/2015 School year

 POPULATION: Students that are sheltered, unsheltered, doubled up, living in a motel or hotel and identified as McKinney-Vento.  
TIME FRAME: 2014/2015 School year  
SOURCE: Charlotte-Mecklenburg Schools

**4,388**  
CMS students identified as MKV in the 2014/2015 school year

**SNAPSHOT**

**RACE / ETHNICITY**  
87% Black

**GENDER**  
51% Female 49% Male

**LIVING SITUATION**  
3,882 494 9  
Doubled up Shelter Unsheltered  
Hotel/motel

**GRADE**  
52% 23% 25%  
Elementary Middle High

**CONTEXT**

- Limited data on MKV students are collected and when changes in a child's situation occurs, it overwrites the old data so that changes throughout the year cannot be tracked.
- Once a student is identified as MKV, they remain MKV until the end of the school year even if their housing situation stabilizes.
- The number of students identified as experiencing homelessness or housing instability is generally understood to be underreported by MKV numbers. Students experiencing homelessness or housing instability may not be identified as MKV for a variety of reasons such as lack of knowledge about the program, lack of self-report due to fear or embarrassment, or the unawareness of school staff of where a child is residing.
- It is estimated that transportation needs are a trigger for the identification of MKV students.

34 | Charlotte-Mecklenburg estimates of family homelessness

# Service Delivery

**PPI can be shared without consent to provide or coordinate services to an individual.**

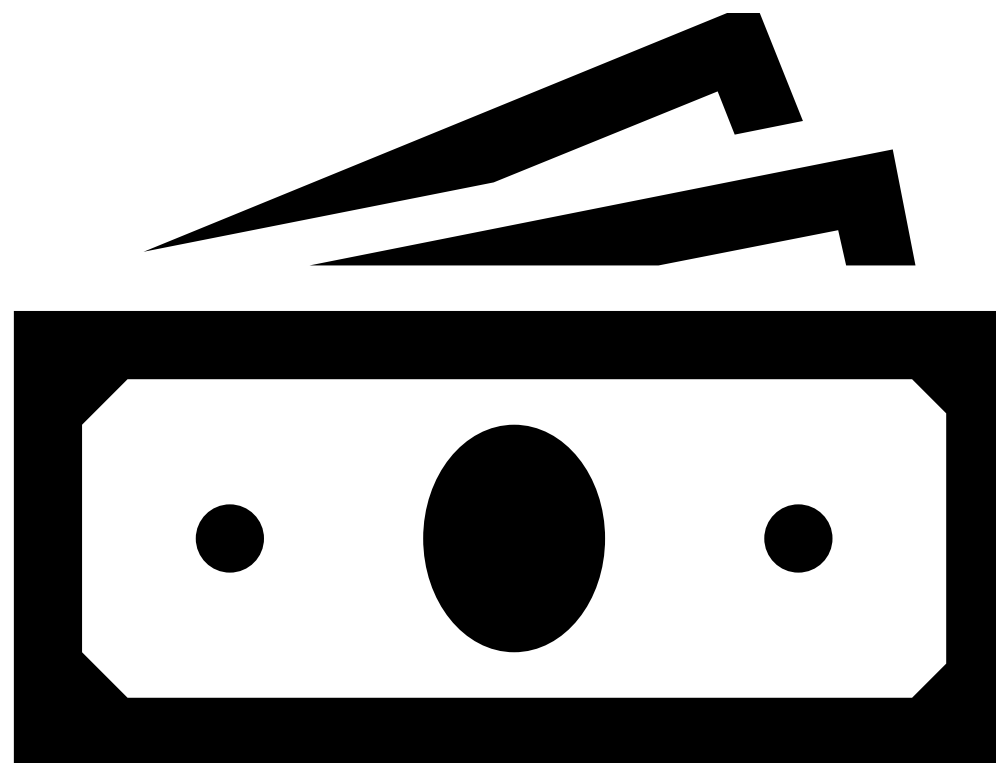
(Section 4.1.3 of HMIS Privacy Standards)



# Payment or Reimbursement

**PPI can be shared without consent for functions related to payment or reimbursement for service.**

(Section 4.1.3 of HMIS Privacy Standards)



# Administrative Functions

PPI can be shared without consent to carry out **administrative functions**, including but not limited to **legal, audit, personnel, oversight and management functions**.

(Section 4.1.3 of HMIS Privacy Standards)



PPI can be disclosed without consent for **academic research** if...

**Research is conducted by:**

- An **individual employed by or affiliated with the CHO** for use in a research project
- By **an institution**

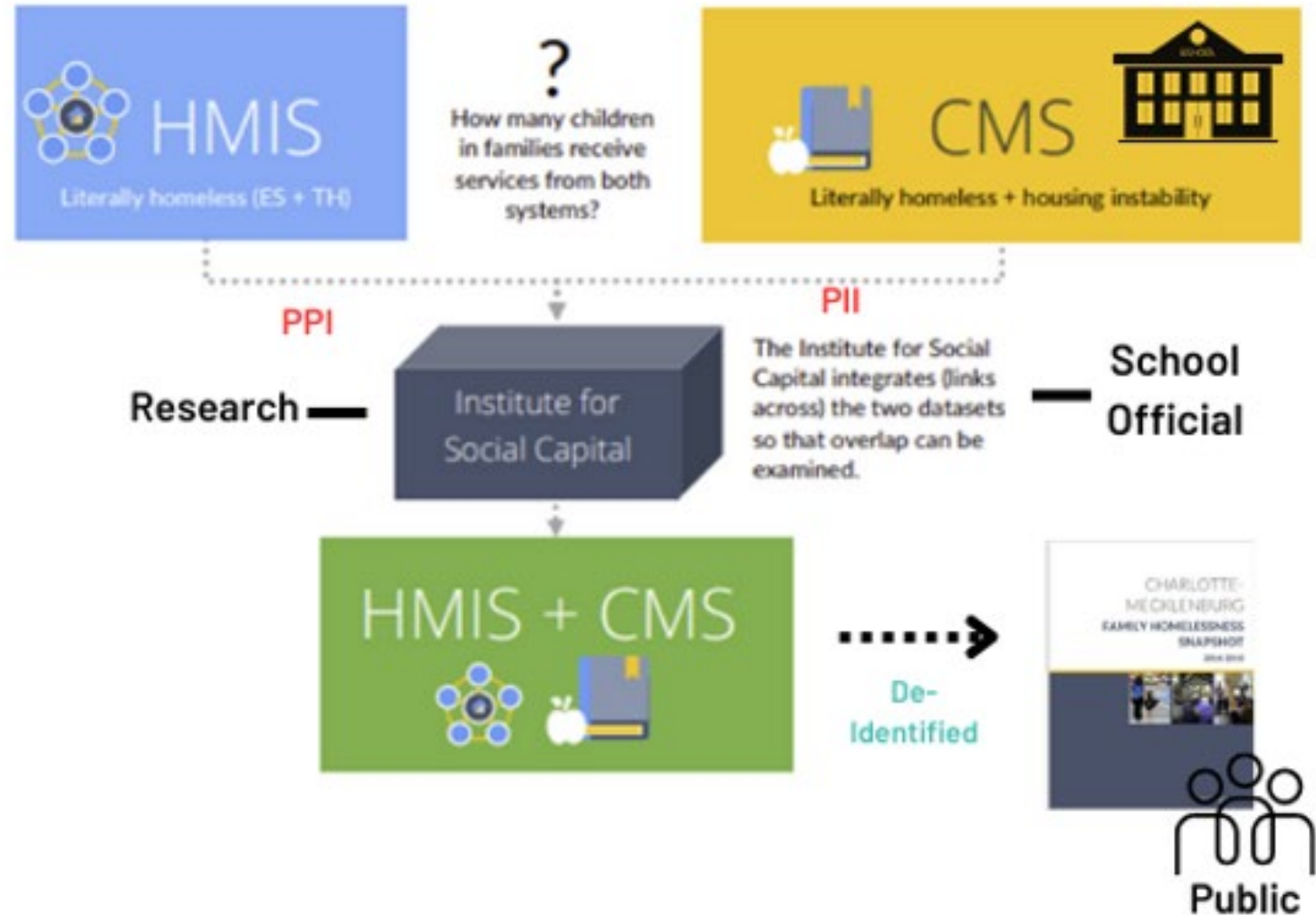
**With a written agreement**

(Section 4.1.3 of HMIS Privacy Standards)

**The written agreement must:**

- Establish rules and limitations for the processing and security of PPI
- Provide for the return or proper disposal of all PPI at the conclusion of the research
- Restrict additional use or disclosure of PPI
- Require that the recipient comply with all terms and conditions of the agreement

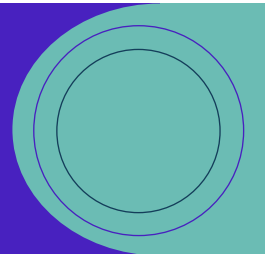
# Use Case





# NUTS & BOLTS OF PRIVACY ACT

---





# What is the Privacy Act?

The Privacy Act of 1974, 5 U.S.C. § 552a

Computer Matching and Privacy Protection Act of 1988

Governs how the **federal government** handles personal information

**Limits** what the federal government can **collect**, protects the **confidentiality** of personal information and guarantees a **right of access**

Federal agencies must promulgate their own regulations to exempt records



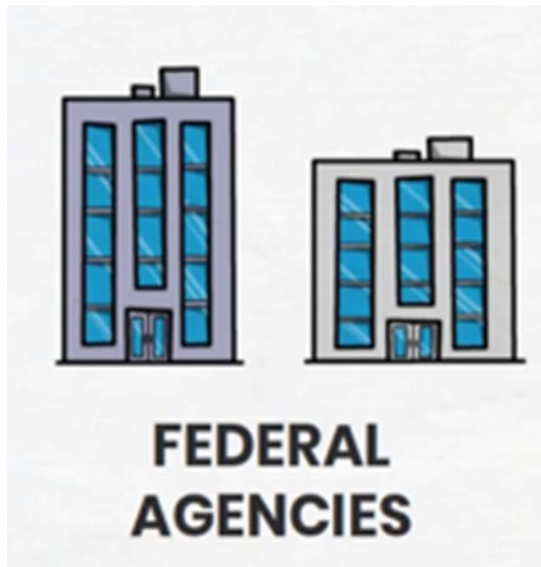
## History of the Privacy Act

**“...[i]f we have learned anything in this last year of Watergate, it is that there must be limits upon what the Government can know about each of its citizens.” -Judiciary Chairman Senator Sam Ervin**

# What does the Privacy Act protect?

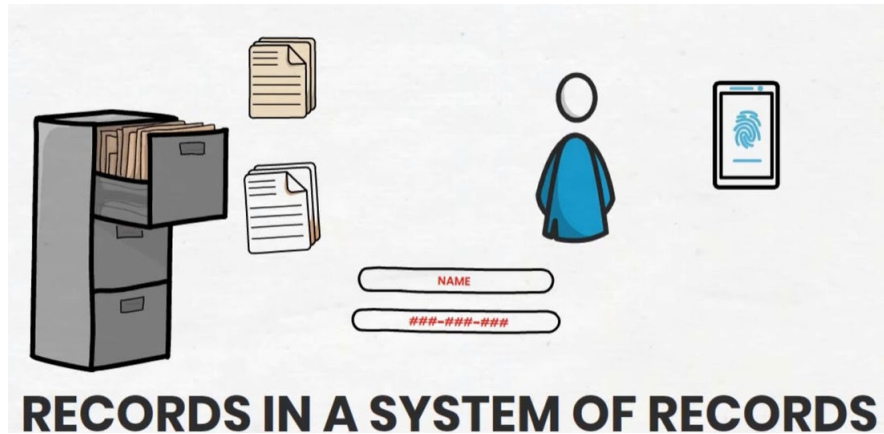
Records about individuals **retrieved by personal identifiers** maintained by federal agencies in a **system of records**. 5 U.S.C. § 552(b)

# Who does the Privacy Act apply to?



<https://www.fpc.gov/privacy-act-1974/>

# What are a “system of records”?



**Group of records** from which information is **retrieved** by use of a **personal identifier**, such as a person's name, Social Security Number, biometrics (fingerprint, facial recognition), medical record number or other unique identifier. 5 U.S.C. § 552(a)

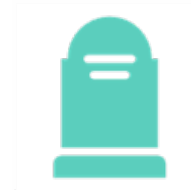
# What is NOT covered under the Privacy Act?



Data held by state, tribal and local governments



Non-citizen data



Decedent Data



Non-people (organizations, businesses, corporations)

## How to Get Consent



The OMB 1975 Guidelines caution that “the consent provision was not intended to permit a blanket or open-ended consent clause, i.e., one which would permit the agency to disclose a record without limit,” and that, “[a]t a minimum, the consent clause should state the general purposes for, or types of recipients [to,] which disclosure may be made.” 40 Fed. Reg. at 28,954

## Exceptions under the Privacy Act

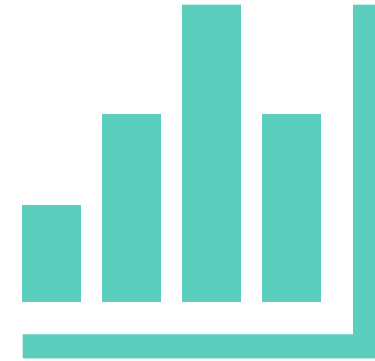
### Data can be disclosed without consent for:



Routine Use



Need to know within  
the agency

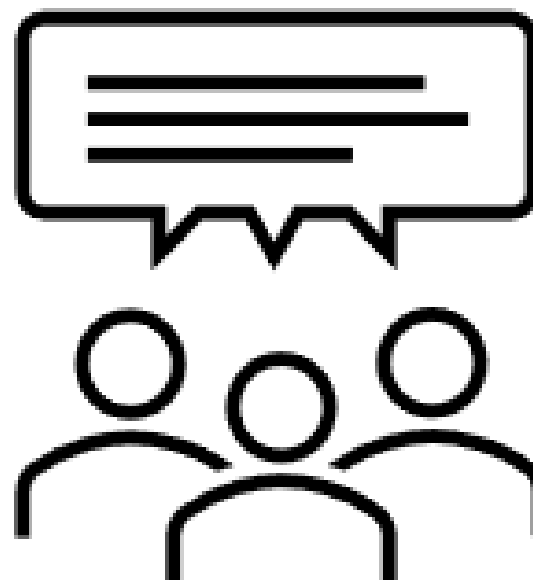


Statistical Research



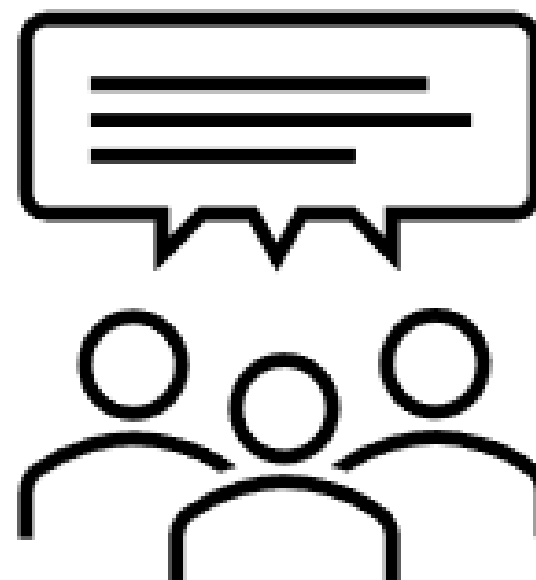
# Routine Use

- Data can be used with consent for a “routine use”
- Routine use means “with respect to the disclosure of a record, the **use** of such record for a purpose which is **compatible with the purpose for which it was collected.**” 5 U.S.C. § 552(a)(7)
- Example: processing an individual’s application for a benefit, program participation, or a position
- The routine use disclosure exception requires an agency to publish the routine use in the Federal Register (System of Records Notice)



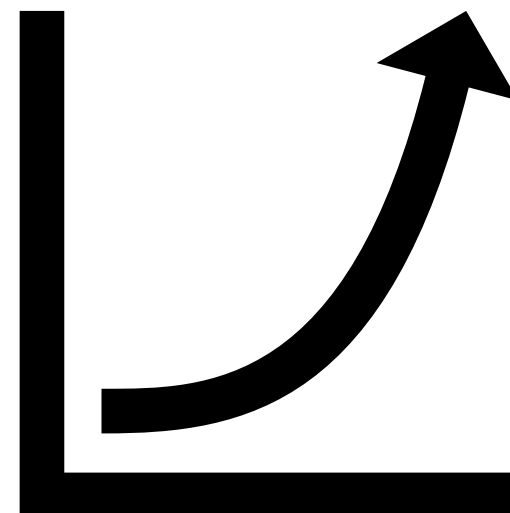
# Need to Know within Agency

**Data can be disclosed without consent to officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties. 5 U.S.C. § 552a(b)(1)**



# Statistical Research

Data can be disclosed without consent “to a recipient who has provided the agency with advance adequate **written assurance** that the record will be **used solely as a statistical research** or reporting record, and the record is to be transferred in a form that is not individually identifiable.”  
5 U.S.C. § 552a(b)(5).



# What about de-identified/aggregate data?

The definition would appear to exclude de-identified data from protection

However, *Calvillo Manriquez v. Devos*, 345 F.Supp.3d 1077, 1099 (2018) (“... even if there is an exception that allows agencies to share aggregate statistical data, the Privacy Act expressly forbids the use of that aggregate statistical data to make determinations about individuals.”).

De-identified data can be used for:

- A statistical purpose
- Such data may not be used to make decisions concerning the rights, benefits, or privileges of specific individuals

# Computer Matching and Privacy Protection Act (Pub. L. 100-503)

- **Agencies must provide notice to the individual that their data may be subject to verification through matching programs**
- **Publish a notice in the Federal Register, at least 30 days before conducting the data match, describing the purpose of the match, the records and individuals covered, and other relevant information.**

# Questions?

# Closing Reflections

*TELL US IN THE CHAT:*  
What is a key idea  
that you are taking  
away from this  
training?





Thank you.

---

**Deja Kemp, JD**

AISP Director of Legal Policy

[dejak@upenn.edu](mailto:dejak@upenn.edu)

A Project of

Copyright and Boilerplate copy here.