


National Human Services Data Consortium **2016 Spring Conference**
Los Angeles, CA
April 13-14, 2016

Demystifying Privacy law
Practical Advice for HMIS and Human Services System Administrators
Jeff Ugai
Matt Olsson



Advancing a Technology Culture in Human Services

National Human Services Data Consortium **2016 Spring Conference**
Advancing a Technology Culture in Human Services
Los Angeles, CA
April 13-14, 2016

Download the Slides:

homebase.box.com/NHSDCPrivacy

National Human Services Data Consortium **2016 Spring Conference**
Advancing a Technology Culture in Human Services
Los Angeles, CA
April 13-14, 2016

Introductions

About Us	About HomeBase
<ul style="list-style-type: none">• Jeff Ugai Attorney (CA), CIPP/US Kapaa, Hawaii• Matt Olsson Attorney (CA, MA) Oakland, California	<ul style="list-style-type: none">• HomeBase is a nonprofit public interest law firm dedicated to the social problem of homelessness.• Technical assistance provider for the US Department of Housing and Urban Development (HUD)

National Human Services Data Consortium | Advancing a Technology Culture in Human Services | **2016 Spring Conference**
Los Angeles, CA
April 13-14, 2016

An important disclaimer:

We created this presentation for informational purposes only. It neither legal advice nor a substitute for the advice of an attorney licensed in your state.

Powered by the National Human Services Data Consortium

National Human Services Data Consortium | Advancing a Technology Culture in Human Services | **2016 Spring Conference**
Los Angeles, CA
April 13-14, 2016

Fundamental Data Privacy Concepts

THE BASICS

Powered by the National Human Services Data Consortium

National Human Services Data Consortium | Advancing a Technology Culture in Human Services | **2016 Spring Conference**
Los Angeles, CA
April 13-14, 2016

Why privacy matters for human services organizations

- **Trust**
Our data is often self-reported information of a highly-personal and sensitive nature—trust is essential to successfully engaging clients and gathering accurate and complete responses.
- **Vulnerability**
Our clients are particularly susceptible to abuse and access to client information often raises legitimate safety concerns.
- **Collaboration**
Effective privacy controls can facilitate the exchange of information across mainstream systems.

Powered by the National Human Services Data Consortium

National Human Services Data Consortium | Advancing a Technology Culture in Human Services | **2016 Spring Conference** | Los Angeles, CA | April 13-14, 2016

Defining Privacy

Privacy encompasses the rights and obligations of individuals and organizations with respect to the collection, use, retention, disclosure and disposal of personal information —

The American Institute of Certified Public Accountants

National Human Services Data Consortium | Advancing a Technology Culture in Human Services | **2016 Spring Conference** | Los Angeles, CA | April 13-14, 2016

Information Lifecycle

The diagram illustrates the Information Lifecycle as a continuous cycle. It features five blue hexagonal nodes arranged in a circle: 'Collect' (top), 'Use' (right), 'Share' (bottom-right), 'Store' (bottom-left), and 'Destroy' (left). A green arrow points from 'Collect' to 'Use', and a black arrow points from 'Destroy' to 'Collect'. The nodes are interconnected by thin white lines, suggesting a continuous flow of information through these stages.

National Human Services Data Consortium | Advancing a Technology Culture in Human Services | **2016 Spring Conference** | Los Angeles, CA | April 13-14, 2016

Personal Information

Any information related to an identified or *identifiable* person.

National Human Services Data Consortium | Advancing a Technology Culture in Human Services | **2016 Spring Conference** | Los Angeles, CA | April 13-14, 2016

Personal Information

General Personal Information	Sensitive Personal Information
<ul style="list-style-type: none">NameDate of Birth (Age)CitizenshipVeteran StatusDisabled StatusContact Information (Address, Number, Email, etc...)	<ul style="list-style-type: none">Social Security NumberDriver's License NumberMedical Records (Including Mental Health and Substance Abuse)Educational RecordsFinancial Information

National Human Services Data Consortium | Advancing a Technology Culture in Human Services | **2016 Spring Conference** | Los Angeles, CA | April 13-14, 2016

General Principles

Notice and Consent	Accuracy and Completeness
Information Security	System Administration

National Human Services Data Consortium | Advancing a Technology Culture in Human Services | **2016 Spring Conference** | Los Angeles, CA | April 13-14, 2016

Notice and Consent (a/k/a the Release of Information)

Notice Description of how personal information is collected, stored, used and shared.	Consent Client's agreement to the use of his or her personal data.
---	--

National Human Services Data Consortium | Advancing a Technology Culture in Human Services | **2016 Spring Conference** | Los Angeles, CA | April 13-14, 2016

Notice and Consent (a/k/a the Release of Information): Drafting Tips

- **Plain English**
Client releases should minimize jargon and clearly explain how and why personal information is collected, stored, used and shared.
- **Demonstrate Value**
Outline the benefits of participation (and the consequences of non-participation)
- **Lay the Foundation for Collaboration**
Collaborate with other systems of care to develop a common framework for sharing and collaboration

National Human Services Data Consortium | Advancing a Technology Culture in Human Services | **2016 Spring Conference** | Los Angeles, CA | April 13-14, 2016

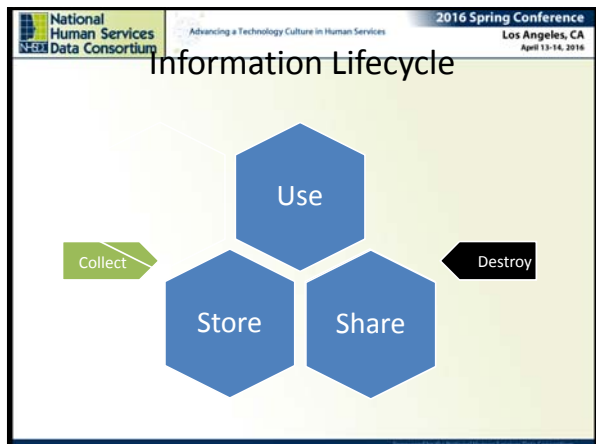
Accuracy and Completeness

- **Up to the Task**
Personal information is relevant and timely for the purpose (as defined in notice)
- **Access and Verification**
Ability for subject to review and verify personal information (upon verification of identity)
- **Means to Update**
Policies support the ability of participating clients and programs to update and correct personal information.

National Human Services Data Consortium | Advancing a Technology Culture in Human Services | **2016 Spring Conference** | Los Angeles, CA | April 13-14, 2016

System Administration: Tips

- **Written Policies and Procedures**
System policies and procedures should include clearly documented and defined privacy policies and procedures, including roles and responsibilities of personnel.
- **Maintain an Archive**
A well-organized archive of past policies, documents and communications helps maintain compliance in an evolving privacy landscape.
- **Provide Support**
Ensure each user has access to the support and training resources necessary to understand the privacy component of their job.



Information Security (More later...)

- **Confidentiality**
Access granted on a need to know basis
- **Integrity**
Controls in place to ensure accuracy
- **Availability**
Information available when and where its needed

Icons made by FreePik on Flat Icon

MAJOR LAWS

National Human Services Data Consortium | Advancing a Technology Culture in Human Services | **2016 Spring Conference** | Los Angeles, CA | April 13-14, 2016

Clearing a few things up

“Generally, privacy laws...”

- “... prevent the sharing of data across systems of care”
Privacy laws create a framework for the sharing and integration of homeless data across systems of care.
- “...only apply to healthcare data”
Privacy law is more than HIPAA—HMIS and other system administrators should be mindful of laws and regulations even if they only store basic client data.

National Human Services Data Consortium | Advancing a Technology Culture in Human Services | **2016 Spring Conference** | Los Angeles, CA | April 13-14, 2016

HMIS-Specific Privacy Guidance and Regulations

HMIS DATA

National Human Services Data Consortium | Advancing a Technology Culture in Human Services | **2016 Spring Conference** | Los Angeles, CA | April 13-14, 2016

HMIS-Specific Privacy Guidance

- The **HMIS Proposed Rule** sets forth basic requirements around privacy and security of client-level data and HMIS systems.
- HUD is in the process of finalizing a draft **HMIS Privacy and Security Notice** that will be released later this year for public comment
- In the interim, communities are expected to continue to use the **2004 Data and Technical Standards Notice** to implement their HMIS

National Human Services Data Consortium | Advancing a Technology Culture in Human Services | **2016 Spring Conference**
Los Angeles, CA
April 13-14, 2016

HUD 2004 Data And Technical Standards Notice

- Seeks to protect the confidentiality of personal information while allowing for reasonable, responsible, and limited uses and disclosures of data.
- Based on principles of fair information practices and security standards recognized by information privacy and security communities.
- Developed after careful review of the Health Insurance Portability and Accountability Act (HIPAA) standards for securing and protecting patient information.

National Human Services Data Consortium | Advancing a Technology Culture in Human Services | **2016 Spring Conference**
Los Angeles, CA
April 13-14, 2016

HUD's Privacy Standard: Protected Personal Information

- Any information maintained by an organization contributing data to HMIS about a living homeless person that:
 - Identifies, directly or indirectly, a specific person; or
 - Can be manipulated to identify a specific person; or
 - Can be linked with other available information to identify a specific person


National Human Services Data Consortium | Advancing a Technology Culture in Human Services | **2016 Spring Conference**
Los Angeles, CA
April 13-14, 2016

The Health Insurance Portability and Accountability Act (HIPAA)

HEALTHCARE DATA

National Human Services Data Consortium | Advancing a Technology Culture in Human Services | 2016 Spring Conference | Los Angeles, CA | April 13-14, 2016

HIPAA: Covered Entities



- Providers
- Insurers
- Clearinghouses
- Business Associates

Icons made by Freekik on Flat Icon

National Human Services Data Consortium | Advancing a Technology Culture in Human Services | 2016 Spring Conference | Los Angeles, CA | April 13-14, 2016

HIPAA: "Health Information"

"Any information" that (1) "is created or received by a healthcare provider, health plan, public health authority, employer, life insurer, school, university or healthcare clearinghouse" and (2) relates to the physical or mental health or condition or the provision of care.

National Human Services Data Consortium | Advancing a Technology Culture in Human Services | 2016 Spring Conference | Los Angeles, CA | April 13-14, 2016

HIPAA: "(Electronic) Protected Health Information"

- **Protected Health Information (PHI)**
Any health information that is explicitly linked to an individual or which can reasonably identify a person when combined with other data elements.
- **Electronic Protected Health Information (ePHI)**
Protected health information that is stored or transmitted electronically

National Human Services Data Consortium | Advancing a Technology Culture in Human Services | **2016 Spring Conference** | Los Angeles, CA | April 13-14, 2016

HIPAA: Privacy Rule

- **Notice**
Must provide client with a detailed privacy notice at the time of first service delivery
- **Consent/Authorization**
Client requirements depend on how PHI is used:
 - *Treatment, Payment, Operations and Compliance*: Authorized by HIPAA itself
 - *Other Uses*: Opt-In Authorization Required
- **Minimal Use**
Outside of treatment, a reasonable effort must be made to limit the use and disclosure of PHI to the minimum amount necessary

National Human Services Data Consortium | Advancing a Technology Culture in Human Services | **2016 Spring Conference** | Los Angeles, CA | April 13-14, 2016


HIPAA: Privacy Rule

- **Access/Disclosure**
Right to access a copy of PHI and an accounting of certain disclosures
- **Reasonable Safeguards**
Administrative, physical and technical safeguards to reasonable protect the confidentiality and integrity of PHI
- **Accountability**
Covered entities must designate a Privacy Officer responsible for developing and implementing compliant privacy policies and procedures

National Human Services Data Consortium | Advancing a Technology Culture in Human Services | **2016 Spring Conference** | Los Angeles, CA | April 13-14, 2016

HIPAA: Privacy Rule – Exceptions

1. De-identification
2. Research
3. Required by Law




National Human Services Data Consortium | Advancing a Technology Culture in Human Services | **2016 Spring Conference**
Los Angeles, CA
April 13-14, 2016

HIPAA: De-Identification

Specified Elements Certification

17



Powered by the National Human Services Data Consortium

National Human Services Data Consortium | Advancing a Technology Culture in Human Services | **2016 Spring Conference**
Los Angeles, CA
April 13-14, 2016

HIPAA: Research

- De-Identified Data
- Consent
- Approval of Instructional Review Board

Powered by the National Human Services Data Consortium

National Human Services Data Consortium | Advancing a Technology Culture in Human Services | **2016 Spring Conference**
Los Angeles, CA
April 13-14, 2016

HIPAA: Security Rule

- Maintain the Confidentiality, Integrity, and Availability of all PHI
- Protect against reasonably anticipated threats
- Protect against reasonably anticipated uses/disclosures
- Ensure staff compliance

Powered by the National Human Services Data Consortium

National Human Services Data Consortium | Advancing a Technology Culture in Human Services | **2016 Spring Conference** | Los Angeles, CA | April 13-14, 2016

HIPAA: Security Rule

Requirements <ul style="list-style-type: none">• Maintain the Confidentiality, Integrity, and Availability of all PHI• Protect against <i>reasonably anticipated</i> threats• Protect against <i>reasonably anticipated</i> uses/disclosures• Ensure staff compliance	Considerations <ul style="list-style-type: none">• Size, Complexity and Capability of Covered Entity• Cost/Difficulty• Probability and potential harm
---	--

National Human Services Data Consortium | Advancing a Technology Culture in Human Services | **2016 Spring Conference** | Los Angeles, CA | April 13-14, 2016

HIPAA: Business Associates

Any individual or organization that performs services or activities involving the use or disclosure of Protected Health Information for a HIPAA covered entity.

National Human Services Data Consortium | Advancing a Technology Culture in Human Services | **2016 Spring Conference** | Los Angeles, CA | April 13-14, 2016

HIPAA: Business Associates

- **HIPAA Applies**
HITECH applies HIPAA privacy and security rules directly to Business Associates
- **Business Associate Agreements**
In addition, covered entities must sign a written agreement passing privacy and security requirements down to the contracting party.

National Human Services Data Consortium | Advancing a Technology Culture in Human Services | **2016 Spring Conference**
Los Angeles, CA
April 13-14, 2016

HIPAA: Enforcement

- **Serious Consequences**
Some HIPAA infractions carry criminal penalties
- **Civil Enforcement**
Department of Health and Human Services enforces HIPAA regulations. State attorneys general granted enforcement by HITECH.

Sponsored by the National Human Services Data Consortium

National Human Services Data Consortium | Advancing a Technology Culture in Human Services | **2016 Spring Conference**
Los Angeles, CA
April 13-14, 2016

EDUCATION DATA

Sponsored by the National Human Services Data Consortium

National Human Services Data Consortium | Advancing a Technology Culture in Human Services | **2016 Spring Conference**
Los Angeles, CA
April 13-14, 2016

Two Key Laws:

- Family Educational Rights and Privacy Act
- Pupil Rights Amendment of the General Educational Provisions Act

Sponsored by the National Human Services Data Consortium

National Human Services Data Consortium | Advancing a Technology Culture in Human Services | 2016 Spring Conference | Los Angeles, CA | April 13-14, 2016

FERPA

- The Family Educational Rights and Privacy Act of 1974 (also called the Buckley Amendment)
- Protects the privacy of student educational records
- Applies to educational institutions that receive funds under Department of Education programs
- ed.gov/fpco

National Human Services Data Consortium | Advancing a Technology Culture in Human Services | 2016 Spring Conference | Los Angeles, CA | April 13-14, 2016

Educational Records Under FERPA

- Records that directly relate to a student and that are maintained by an educational agency or institution or by a party acting for the agency or institution. 20 USC § 1232g(4)(A)

National Human Services Data Consortium | Advancing a Technology Culture in Human Services | 2016 Spring Conference | Los Angeles, CA | April 13-14, 2016

Educational Records Under FERPA

- Records that directly relate to a student and that are maintained by an educational agency or institution or by a party acting for the agency or institution. 20 USC § 1232g(4)(A)
- Any record that contains **personally identifiable information** that is **directly related to the student** is an educational record under FERPA

National Human Services Data Consortium | Advancing a Technology Culture in Human Services | **2016 Spring Conference** | Los Angeles, CA | April 13-14, 2016

What's Not an Educational Record

- Campus police records
- Medical records (subject to privacy regulations under other laws)
- **Statistical data compilations that contain no mention of personally identifiable information about any specific student.**

National Human Services Data Consortium | Advancing a Technology Culture in Human Services | **2016 Spring Conference** | Los Angeles, CA | April 13-14, 2016

Two Types of Educational Records

Directory Information	Non-Directory Information
Written consent advisable but not required; Parent/adult student has right to limit disclosure (opt-out) <ul style="list-style-type: none"> • Name • Address • Phone number and email address • Dates of attendance • Degree(s) awarded • Enrollment status • Major field of study 	Written consent required (opt-in) <ul style="list-style-type: none"> • Social Security numbers • Student identification numbers • Race, ethnicity, or nationality • Gender • Transcripts; Grades

National Human Services Data Consortium | Advancing a Technology Culture in Human Services | **2016 Spring Conference** | Los Angeles, CA | April 13-14, 2016

What data can schools share with CoCs?

- **Aggregate Info**
Schools may disclose aggregate student information that does not include any PII for research and evaluation purposes
- **Directory Info**
Directory information, as long as the parent or eligible student has not opted out
- **Homeless Statistics**
The number of students experiencing homelessness at the time of the PIT count, including information about grade level, primary nighttime residence, race, and gender, *as long as that data does not include PII*
- **De-Duplication Support**
Schools may view PII to de-duplicate their count of homeless students, but may not disclose PII to a CoC for de-duplication

National Human Services Data Consortium | Advancing a Technology Culture in Human Services | **2016 Spring Conference** | Los Angeles, CA | April 13-14, 2016

What is PPRA?

- Protection of Pupil Rights Amendment of the General Educational Provisions Act
- Governs administration of certain types of surveys to students

National Human Services Data Consortium | Advancing a Technology Culture in Human Services | **2016 Spring Conference** | Los Angeles, CA | April 13-14, 2016

PPRA

<p>Protected Areas</p> <p>Subjects protected under PPRA include:</p> <ul style="list-style-type: none"> • Mental or psychological problems of student or student's family • Sexual behaviors or attitudes • Illegal, anti-social, self-incriminating or demeaning behavior 	<p>Notification Requirements</p> <ul style="list-style-type: none"> • Direct notification of parents or adult students • Provide opportunity to opt-out
--	--

National Human Services Data Consortium | Advancing a Technology Culture in Human Services | **2016 Spring Conference** | Los Angeles, CA | April 13-14, 2016

CRIMINAL JUSTICE

National Human Services Data Consortium | Advancing a Technology Culture in Human Services | **2016 Spring Conference**
Los Angeles, CA
April 13-14, 2016

Disclosures to Law Enforcement

- **Court Order Required**
There is no general exemption for disclosures to law enforcement, and administrators may face liability for disclosures without a valid court or other lawful order
- **Limited Exceptions**
Narrowly defined exceptions exist for extraordinary circumstances

National Human Services Data Consortium | Advancing a Technology Culture in Human Services | **2016 Spring Conference**
Los Angeles, CA
April 13-14, 2016

Criminal Records

- **Generally Public**
Criminal and civil court records are generally open and public
- **Juvenile, Financial and Medical Records**
May be subject to additional protections and/or redaction
- **Potential for Abuse**
Be mindful of the potential for the abuse and/or discrimination

National Human Services Data Consortium | Advancing a Technology Culture in Human Services | **2016 Spring Conference**
Los Angeles, CA
April 13-14, 2016

INFORMATION SECURITY

National Human Services Data Consortium | Advancing a Technology Culture in Human Services | **2016 Spring Conference** | Los Angeles, CA | April 13-14, 2016

Information Security

[Picture]

- **Confidentiality**
Access granted on a need to know basis
- **Integrity**
Controls in place to ensure accuracy
- **Availability**
Information available when and where its needed

National Human Services Data Consortium | Advancing a Technology Culture in Human Services | **2016 Spring Conference** | Los Angeles, CA | April 13-14, 2016

InfoSec: Determining Need

- **Threat/Risk Assessment**
What are your system's threats and vulnerabilities?
- **Obligations**
What are your contractual and regulatory obligations?
- **Goals**
What are your policies and objectives?

National Human Services Data Consortium | Advancing a Technology Culture in Human Services | **2016 Spring Conference** | Los Angeles, CA | April 13-14, 2016

Data Breach, Incident Management, and Notification Laws

WOOPSIE

National Human Services Data Consortium | Advancing a Technology Culture in Human Services | **2016 Spring Conference**
Los Angeles, CA
April 13-14, 2016

Incident Management 101

- 1. Confirm**
Determine there was actually a breach
- 2. Contain**
Prevent further damage and understand what happened
- 3. Communicate**
Notify impacted parties of the breach

National Human Services Data Consortium | Advancing a Technology Culture in Human Services | **2016 Spring Conference**
Los Angeles, CA
April 13-14, 2016

Data Breach Notification Laws

- **(Almost) Every State**
Every state has enacted notification laws except for three holdouts: New Mexico, South Dakota and Alabama (2014)
- **Fines and/or Shame**
Notification laws incentivize effective information security by attaching financial and reputational harm to public disclosure.
- **High Standards May Minimize Liability**
Many states include exemptions for data protected by encryption or similar technology

National Human Services Data Consortium | Advancing a Technology Culture in Human Services | **2016 Spring Conference**
Los Angeles, CA
April 13-14, 2016

OTHER LAWS

National Human Services Data Consortium | Advancing a Technology Culture in Human Services | **2016 Spring Conference**
Los Angeles, CA
April 13-14, 2016

A few highlights...

- **State-Specific Laws**
Many states have additional laws which go above and beyond the federal regulatory framework.
- **Credit and Financial Information**
Fair and Accurate Credit Transaction Act (FACTA) regulates organizations that collect credit information on consumers or employees.

National Human Services Data Consortium | Advancing a Technology Culture in Human Services | **2016 Spring Conference**
Los Angeles, CA
April 13-14, 2016

Q&A
