

# *Colorado Children and Youth Information Sharing Summits*

# Agenda

- CCYIS – Background and Overview
- Fitting in the Family Voice
- Identifying Barriers to Information Sharing
- HIPAA and 42 CFR
- Personal Identifiable Information and Family Educational Rights and Privacy Act or FERPA
- Process Change and Implementation of the Authorization/Consent Form
- Closing –
  - Questions and Answers
  - Resources
  - Training and Technical Assistance
  - Evaluations

# CCYIS – Overview

# CCYIS Establishment



- Created from a need for information sharing out of two state initiatives in 2007:
  - Collaborative Management Program (CMP or HB 1451)
  - Prevention Leadership Council (PLC)
- Prioritized through the MOU process for CMP and PLC executed by Executive Directors of CDHS, CDPHE, CDPS, CDE, HCPF as well as the CO State Court Administrator

# Purpose of CCYIS



“The main purpose of children and youth information sharing is to structure policy and procedures for efficient, appropriate and timely sharing of accurate information between children and youth serving agencies at the state and local levels to improve services and outcomes of children, youth and families involved in services.”

# CCYIS Vision And Mission



## **Vision:**

Children, youth and families experience seamless and collaborative services and supports that are responsive to their interests and needs. This is facilitated by information sharing that safeguards their privacy at both the state and local level.

## **Mission Statement:**

To develop strategies for sharing information to optimize services available and delivered to children, youth and families in Colorado.

# CCYIS – Major Goals



- Establish a foundation of an effective, cross-discipline collaborative governing body to improve information sharing for children and youth in Colorado.
- Manage a comprehensive assessment of data, legal authority, technology and related policies of participating agencies.
- Develop a children and youth information sharing strategic plan.
- Develop cross-system protocols and explore technological solutions for information sharing.

# Other Information Sharing Initiatives



- Working with CDHS on their Interoperability Grant- Colorado Client Information Sharing System (CCISS)
- Working with CDE on their LINKS project



# Anticipated CCYIS Outcomes



- Data sharing agreements between State agencies that provide access to information for policy, program, service, and resource decisions;
- Access to client level information on a “need to know basis” through secure methods by government and nongovernment agencies to better coordinate and determine effective services;
- Improved access to information by youth and families regarding information that is collected about them; and
- Improved health, safety and general well-being of Colorado’s children, youth and families.

# Fitting in the Family Voice

**Margie Grimsley**  
**Federation of Families for Children's Mental Health**  
**Colorado Chapter**

# CCYIS and Families

*Since it began, the CCYIS has been committed to including a family member, a family-driven organization, community and youth representatives as part of the process to develop effective information sharing practices.*

# National Information Sharing Guidelines and Family Engagement



## Governance Guidelines for Juvenile Information Sharing **ESSENTIAL**

National Juvenile Information Sharing Initiative - NJISI

In Cooperation  
With



Office of Juvenile  
Justice  
and Delinquency  
Prevention



Office of Justice  
Programs

[Return to the  
NJISI Website](#)

[About the  
Guidelines](#)

[The Tools](#)

[JIS Readiness  
Self-Assessment](#)

[Glossary](#)



[Prev](#) | [Home](#) | [Next](#)

## Guideline 2 **Engage youth and family representatives in the JIS collaborative.**

Youth and family-centered practice focuses on the healthy growth and development of children and youth within a family context. This strength-based approach is based on a core set of values, beliefs and principles that recognize that youth and families can actively participate in and contribute to all aspects of services and outcomes. An essential component of this [evidence-based practice](#) is engaging youth and families in designing all aspects of the policies, services and eventual evaluations. This enables them to participate in developing solutions that affect their lives.

Another benefit of engaging and learning from youth and families is that agency decision makers can learn from youth and family experiences navigating between various systems and agencies that collect similar information. This leads to better decision making. Additionally, youth and families know that when agency decision-makers have the information needed to make good decisions, they receive the services and assistance they need. For example, if a judge has accurate information from schools and services, court orders can then reflect a youth's current school performance and involvement in behavioral health treatment.

To help identify potential youth and family representatives, contact JIS collaborating agencies and youth or family advocacy organizations, community and policy making organizations.

[guidelines](#)

<sup>1</sup> <http://www.childwelfare.gov/famcentered/casework/youth.cfm>

<sup>2</sup> <http://www.uiowa.edu/~nrcfcp/>

# Supporting the Family Voice



- Serving at the CCYIS Collaborative meetings
- Serving on the Leadership Team
- Serving on the Privacy and Confidentiality Committee
- Establishing a Family Youth Involvement Committee
- Holding Family Focus Groups-
  - Asking questions
  - Listening and documenting real life experiences
  - Educating and Spreading the word:  
<http://www.juvenileis.org/publications.html>
- Being here today!
- Video time: Mae and the Governor

# Questions to Consider – Family Perspective



## *Listen and Learn*

- What information is confidential, and what is not?
- What exemptions exist to the confidentiality requirements?
- What information can be released with consent, and what are the requirements for such a release of information?
- What other mechanisms are available for sharing confidentiality information?

Solar, M., A., & Bell, J. (1993). Glass walls: Confidentiality provisions and interagency collaborations. San Francisco Youth Law Center

# Confidentiality Does Not Need to Hamper Service Coordination



## 1) **The principal of limited information**

*Julie Krow: Finding that balance...sharing information that is helpful...not cause bias towards this family and their youth.....*

## 2) **Agency gatekeeper**

*Jim Davis: "Can't do our job with only half the picture, or sometimes less sometimes"*

## 3) **Confidentiality oaths**

*Mae Washam: Told they will not share my information with other agencies.*

# Listening and Understanding Key Messages



- The legal mandates, at the national, state and local levels.
- The reason for ensuring confidentiality of information about children and families.
- Why agencies need individual family information.



# Key Messages-continued



- The purpose of information sharing among agencies.
- The need for sensitivity to language and cultural issues.
- The requirements of informed consent, and the necessary elements for written releases.

Solar, M., A., & Bell, J. (1993). Glass walls: Confidentiality provisions and interagency collaborations. San Francisco Youth Law Center

# Messages to Remember



- *"It is critical to share information with other partners in the community...to keep children safe."*  
**Julie Krow: (Dir. of the Office of Children, Youth and Families; Dept. of Human Services)**
- *"That people come together to get the right information."*  
**Dr. Keith Owen (Deputy Commissioner Dept. of Education)**
- *"Most important shift is to look at the people that we are working with. Get to a point where people understand that it is vital to have the entire picture when making decisions."*  
**Jim Davis (Executive Director of Public Safety)**

IT TAKES A VILLAGE...

Sig K



TEACHER

TRUANT  
OFFICER

HUMAN SERVICES  
CASEWORKER

POLICE

RESPONSIBLE  
PARENT



JUDGE

PROBATION  
OFFICER

# ***BEWARE OF THE HALF TRUTH. YOU MAY HAVE GOTTEN HOLD OF THE WRONG HALF.***

“To Every Dog there is a Season-Lessons for Life”

---

**Marjorie Grimsley**

**Federation of Families for Children's Mental Health -  
Colorado Chapter**

**[m\\_grimsley@msn.com](mailto:m_grimsley@msn.com)**

# Identifying the Barriers to Information Sharing

**Stephanie Rondenell, Executive Director –  
National Juvenile Information Sharing Initiative**

**[Stephanie.Rondenell@acq-online.net](mailto:Stephanie.Rondenell@acq-online.net)**

**303.979.8722**

# Myths and Other Issues

- You can share any information, at any time with anyone *within* your organization
- Sharing information is dependent upon **who** you know
- You always need **consent** to share
- Security and privacy are the same thing
- HIPAA is a barrier to cross agency information sharing
- Agencies that work together and that already have our information ‘already share it’ –
- If its FERPA related – you cannot share it!



# Use Case Activity

## MacKenzie C. Use Case

- Review the Use Case
- Answer the questions
- Use the flip charts to:
  - Document the barriers – why you cannot share
  - Identify someone at your table to ‘report out’ after the break

# Privacy and Confidentiality Laws – An Overview

**Kathleen Foo**

HIPAA Privacy and Security Officer, CIPP/US, CIPP/G-US,  
Certified ISO/IEC 27001 Lead Auditor  
Department of Human Services



# HIPAA and 42 CFR Part 2



- Health Insurance Portability and Accountability Act (HIPAA)
- Federal Drug & Alcohol Confidentiality Law (42 CRF, Part 2 )

# HIPAA and 42 C.F.R. Part 2



If two federal laws regulate the same subject, such as **health privacy**, the rule is to give effect to both laws if at all possible. If not, the most recently enacted law prevails.

- However, an earlier enacted law that deals with a **narrow, precise, or specific subject** will prevail over a later enacted law that treats the subject more generally.
- The rationale for this rule is that Congress generally does not enact inconsistent provisions when it is aware of a **previously existing law**, without expressly recognizing the inconsistency.

# HIPAA

```
graph TD; HIPAA --> HPHS[Health Privacy and Health Security]; HIPAA --> PHMH[Physical Health and Mental Health Information];
```

Health Privacy and  
Health Security

Physical Health  
and  
Mental Health  
Information

# 42 CFR Part 2

```
graph TD; CFR[42 CFR Part 2] --> ADA[Alcohol and Drug Abuse Information];
```

Alcohol and Drug  
Abuse Information

# Examples

Many HIPAA provisions *permit*, but do not mandate, the disclosure of health information; while 42 CFR Part 2 *prohibits* all disclosures except those specifically allowed by the regulations.

- Example 1. HIPAA requires a covered program to give an individual access to his or her own health information, while 42 CFR, Part 2 permits patients to access their own records.

## HIPAA

- Example 2. HIPAA permits disclosures without patient consent for the purposes of TPO as long as a notice of privacy practices was given to the individual; while 42 CFR, Part 2 prohibits these disclosures without direct patient consent.

**42 CFR Part 2 (narrow, precise, or specific subject)**

# Understanding Health Information Privacy



The HIPAA Privacy Rule provides federal protections for personal health information (PHI) held by covered entities (CE), business associates (BA), and their subcontractors.

- Gives patients an array of rights (controls and access) with respect to their information.
- Protect individually identifiable medical information from threats of loss or disclosure.
- Simplifies the administration of health insurance claims and generates lower costs.
- **Balanced so it permits the disclosure of PHI needed for patient care and other important purposes.**

# What is HIPAA?

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 is Federal legislation enforcing:

- the **portability** of health care coverage;
- the **security and privacy** of health information; and
- **an accounting** of how individual health care information is handled and protected.

H

Health

I

Insurance

P

Portability and

A

Accountability

A

Act of 1996

If a state or federal law contains stricter requirements than HIPAA, the more restrictive law takes precedent.

# Confidentiality, Integrity and Availability



Must ensure the *confidentiality, integrity, and availability* of all electronic Protected Health Information (PHI) we create, receive, maintain, or transmit.

## **Confidentiality**

PHI is accessible only by authorized people and processes.

## **Integrity**

Secure processes for the transfer and storage of all PHI, ensuring that information is not altered, destroyed, or used/disclosed inappropriately.

## **Availability**

PHI can be accessed as needed by an authorized person.

# Understanding Health Information Security



The Security Rule specifies a series of safeguards for covered entities (CE), business associates (BA), and their subcontracts:

To secure the privacy of electronic protected health information (PHI) thru standards:

**ADMINISTRATIVE**

**PHYSICAL**

**TECHNICAL**



# Security Rule Standards



## ADMINISTRATIVE SAFEGUARDS

- Security Management Process
- Assigned Security Responsibility
- Workforce Security
- Information Access Management
- Security Awareness and Training
- Security Incident Procedures
- Contingency Plan
- Evaluation
- Business Associate Contracts and Other Arrangements

## PHYSICAL SAFEGUARDS

- Facility Access Controls
- Workstation Use
- Workstation Security
- Device and Media Controls

## TECHNICAL SAFEGUARDS

- Access Control
- Audit Controls
- Integrity
- Person or Entity Authentication
- Transmission Security

# Protected Health Information?

**Examples of PHI include but are not limited to the following:**

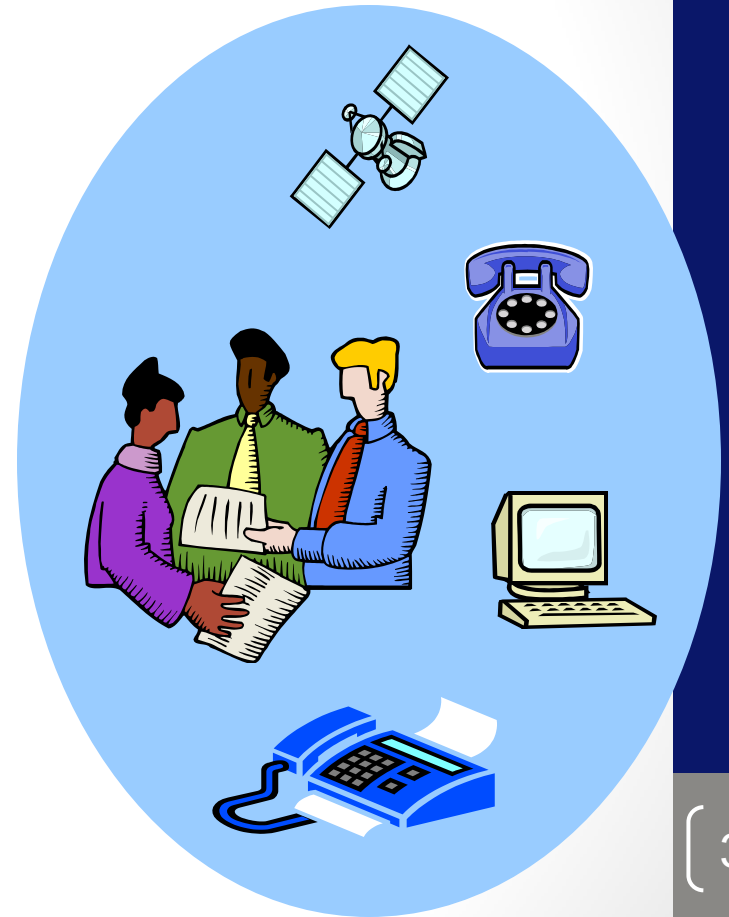
- Names
- Address
- Social Security number
- Family History
- Telephone number
- Fax number
- Account numbers
- Medical record number
- E-mail address
- Dates (birthday, admission/discharge)
- Certificate/license numbers
- Vehicle ID (license plate, serial number)
- Personal Assets
- Device identifiers and serial numbers
- Biometric (finger or voice print)
- Photographs
- Geographic indicators (zip codes for areas with 20,000 or less people)
- Any unique identifying number, code or characteristic

# What Form Does PHI Take?

**PHI can be in many forms or types of media.**

**Examples include:**

- **Paper copies / printed copies**
- **Telephone calls and voice mail**
- **Photos / videos**
- **Verbal communication**
- **Fax transmissions**  
**(copper wire vs. wireless)**
- **Information transmitted over the Internet / Intranet**
- **E-mail**



# Privacy Rule – Use of New Form, Minimum Necessary Rule



When using, disclosing or requesting PHI from another covered entity using the **Authorization for Consent Form developed by CCYIS, remember:**

A covered entity must make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

# Policies and Procedures – HIPAA Privacy Rule



State of Colorado, HIPAA Privacy Policies and Procedural Manual @ [www.colorado.gov/cdhs](http://www.colorado.gov/cdhs) or [Click Here](#)

## **Table of Contents**

Identifying when Routine Health Information Becomes Protected Health Information

Where Is The Policy in the Privacy Rule (Title 45, Part 164)?

§164.103 - Definitions

§164.501 - Definitions

Minimum Necessary

45 C.F.R. §§164.502(b) & 164.514(d)

Disclosing and Requesting only the Minimum Amount of Protected Health Information Necessary

45 C.F.R. §§164.502(b) & 164.514(d)

Authorizations

45 C.F.R. §164.508

Obtaining Authorizations for Use and Disclosure of PHI

# Policies and Procedures – HIPAA Security Rule



COLORADO  
CHILDREN & YOUTH  
INFORMATION SHARING COLLABORATIVE

**All state agencies and anyone doing business with the State of Colorado are required to follow the Cyber Security Policies @**

**[www.colorado.gov/cybersecurity](http://www.colorado.gov/cybersecurity)**

Cyber Security Planning	Physical Security
Incident Response	Data Classification, Handling, and Disposal
IT Risk Management	Personnel Security
Disaster Recovery	System Access and Acceptable Use
Vendor Management	Online Privacy
Network Operations	Security Training and Awareness
Systems and Applications	Self Assessment
Security Operations	Security Metrics and Measurement
Access Control	Mobile Computing
Change Control	Wireless Security

# HIPAA / HITECH Final Rule – (The Omnibus Rule)



- Implements HITECH Act (Health Information Technology and Economic & Clinic Health)
- Modifies HIPAA's Statutes:
  - Breach Rule
  - Security Rule
  - Privacy Rule
  - Enforcement Rule
- Stays fairly consistent with proposed HITECH rule of 2009
- General Compliance Date: **September 23, 2013** (subject to a few exceptions)
- Implements underwriting nondiscrimination requirement of the Genetic Information Nondisclosure Act of 2008, (GINA )

# Difference Between

## “consent” and “authorization”

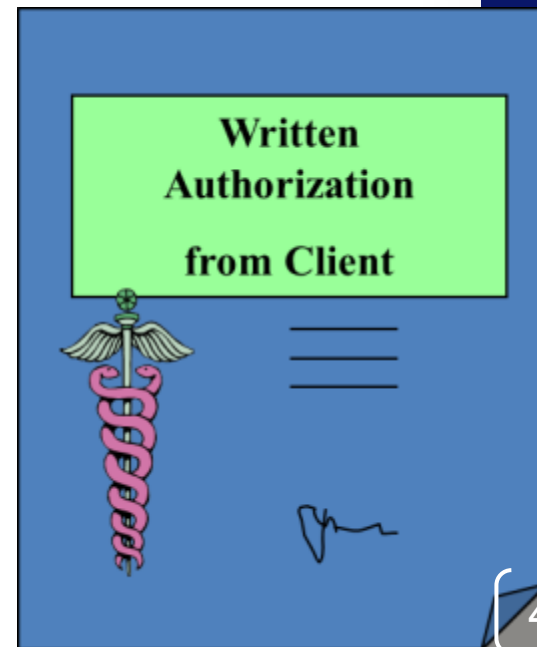


**Consent:** The HIPAA Privacy Rule permits, but does not require, a covered entity voluntarily to obtain patient consent for uses and disclosures of protected health information for treatment, payment, and health care operations, TPO.

Example: Notice of Privacy Practices (NPP).

**Authorization:** is required by the Privacy Rule for uses and disclosures of protected health information not otherwise allowed by the Rule.

Example: Uses and Disclosures without Authorizations @ 45 C.F.R. §164.512.





### **CONFIDENTIALITY PRACTICES AND USES**

CDHS, may access, use and or share medical information for:

**Treatment** - to appropriately determine approvals or denials of your medical treatment. For example, CDHS health care professionals who may review your treatment plan by your health care provider for medical necessity.

**Payment** - to determine your eligibility benefits and payment. For example, your health care provider may send claims for payment to the Medicaid fiscal agent for medical services provided to you, if appropriate.

**Health Care Operations** - to evaluate the performance of a health plan or a health care provider. For example, CDHS contracts with consultants who review the records of hospitals and other organizations to determine the quality of care you received.

# Allowed Disclosures without Authorization



## **DISCLOSURES NOT REQUIRING YOUR PERMISSION**

CDHS can make the following disclosures only if it is directly related to running of the medical assistance programs, a court orders CDHS to disclose the information, or another law requires CDHS to disclose the information.

**Other Government Agencies and/or Organizations Providing Benefits, Services or Disaster Relief** - to disclose information with other government agencies and/or organizations for you to receive those benefits and/or services offered.

**Public Health** - to disclose medical information to agencies for public health activities for disease control and prevention, problems with medical products or medications, and victims of abuse, neglect or domestic violence.

**Health Oversight Activities** - to disclose information to approved government agencies responsible for the Medicaid program, the U. S. Dept. of Health and Human Services, and the Office of Civil Rights.

**Judicial and Administrative Hearings** - to disclose specific medical information in court and administrative proceedings.

**Law Enforcement purposes** - to disclose specific medical information for law enforcement purposes.

**Coroners, Medical Examiners, and Funeral Directors** - to disclose specific medical information to authorized persons who need it to administer their work.

# Allowed Disclosures without Authorization, cont.



**Research Purposes** - in certain circumstances, and under supervision of a privacy board, we may disclose medical information to assist medical/psychiatric research.

**Organ Donation and Disease Registries** - to disclose specific medical information to authorized organizations involved with organ donation and transplantation, communicable disease registries, and cancer registries

**To Avert Serious Threat to Health, Safety or Emergency Situation** - to disclose specific medical information to prevent a serious threat to the health and safety of an individual or the public.

**Specialized Government Functions** - to disclose medical information for national security, intelligence and/or protective services for the President. CDHS may also disclose health information to the appropriate military authorities if you are or have been a member of the U. S. armed forces.

**Correctional Institutions** - to disclose medical information to correctional facility or law enforcement officials to maintain the health, safety and security of the corrections system.

**Workers' Compensation** - to disclose medical information to workers' compensation programs that provide benefits for work-related injuries or illness without regard to fault.

**Disclosures to Family, Friends, and Others**- CDHS may disclose information to your family or other persons who are involved in your care. You have the right to object to the sharing of this information.



# NEW - Notice of Privacy Practices

Content must now include:

- Statements regarding **sale of PHI**, marketing, and other purposes that require authorization
- Statement that individual can **opt out** of fundraising communications
- Statement that CE must agree to restrict disclosure to health plan if individual **pays out of pocket** in full for health care service
- Statement about individual's right to **receive breach notifications**
- For plans that underwrite, statement that **genetic information** may not be used for such purposes

**Covered Entity:** a health plan, health care clearinghouse or health care provider who transmits any health information with respect to a covered transaction in electronic form.

**Hybrid Entity:** a single legal entity:

- (1) That is a covered entity;
- (2) Whose business activities include both covered and non-covered functions; and
- (3) That designates health care components in accordance with paragraph §164.105(a)(2)(iii)(C).

# Are you a Business Associates?



**NEW:** Creates, receives, maintains, or transmits PHI, on behalf of the Covered Entity or per the HIPAA Rules.

- BAs must comply with the technical, administrative, and physical safeguard requirements under the Security Rule, directly liable for violations.
- BAs must comply with the use or disclosure limitations expressed in BA contract and those in the Privacy Rule; directly liable for violations.
- Subcontractors of BA are now defined as BAs
  - BA liability flows to all subcontractors

# Are you a Subcontractor?

A subcontractor **creates, receives, maintains, or transmits** protected health information (PHI) on behalf of the business associate.

- Subcontractor + PHI = Business Associate
- Subcontractor = person to whom a business associate delegates a function, activity, or service
- Subcontractor  $\neq$  workforce member
- All the way down the chain

# Who Contracts with Whom?

- Covered entities must have business associate contracts with their direct business associates
- Business associates must have business associate contracts with their subcontractors
- Covered entities do not need business associate contracts with subcontractors



# The HIPAA Enforcement Rule



Contains provisions relating to compliance and investigations, the imposition of civil money penalties for violations of the HIPAA Administrative Simplification Rules, and procedures for hearings.

**ANYONE CAN FILE!** - a complaint alleging a violation of the Privacy or Security Rule using the [OCR Health Information Privacy Complaint Form Package](#).

**IMPORTANT:** Harmed Individuals to receive a percentage of the fine. Distribution of Penalties/Settlements estimate is 33% if total fine.

**HIPAA PROHIBITS RETALIATION** - Under HIPAA an entity cannot retaliate against you for filing a complaint. You should notify OCR immediately in the event of any retaliatory action.

# National Security Breach Notification Law, Sept 17, 2009



## The American Recovery and Reinvestment Act

Requires Covered Entities (CE) and their Business Associates (BA) to notify individuals whose **unsecured protected health information** has been breached. (PHI is presumed to have been accessed, acquired or disclosed.)

- This requires written notification by mail or, if specified by email.
- For large breaches (500+ residents in a particular area) a “prominent media outlet” must be notified of the breach.
- The U.S. Department of Health and Human Services (“HHS”) must be contacted, and
- Be posted on the **HHS website of shame @**  
**<http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html>**

# Data Breach Notification

## “Data Breach”

- Unauthorized acquisition, access, use, disclosure of **unsecured PHI**
- In a manner not permitted by the HIPAA Privacy Rule
- That compromises the security or privacy of the PHI
- CE is responsible for reporting to U.S. HHS

## Exceptions

- For inadvertent, harmless mistakes remain
- Exception for limited data sets without dates of birth & zip codes (removed)

# Definition of Breach

Harm standards removed:

- Was “no harm, no foul”
- Now “low probability of compromised PHI”

New Standard – impermissible use/disclosure of (unsecured) PHI ***presumed*** to require notification, unless CE/BA can demonstrate low probability that PHI has been compromised based on a risk assessment of at least:

1. Nature & extent of PHI involved
2. Who received/accessed the information
3. Potential that PHI was actually acquired or viewed
4. Extent to which risk to the data has been mitigated

# Enforcement Rule

## Fraud Enforcement and Accountability

- Criminal penalties for knowingly violating the Rules include monetary fines as well as potential for **imprisonment up to 10 years.**
- Civil penalties range from \$25,000 to \$1,500,000 million contingent on the intent of the violation.



# Increased Fines and Penalties, Feb 17, 2009



**Tier A (if the offender did not know, and by exercising reasonable diligence would not have known, that he or she violated the law):**

**\$100** for each violation, except that the total amount imposed on the person for all such violations of an identical requirement or prohibition during a calendar year may not exceed **\$25,000**.

**Tier B (if the violation was due to reasonable cause and not willful neglect):** **\$1,000** for each violation, ... may not exceed **\$100,000**.

**Tier C (if the violation was due to willful neglect but was corrected):** **\$10,000** for each violation, ...may not exceed **\$250,000**.

**Tier D (if the violation was due to willful neglect and was not corrected)** **\$50,000** for each violation, ...may not exceed **\$1,500,000**.

# Increased Enforcement

## Focus on Willful Neglect:

- Willful neglect: Conscious, intentional failure or reckless indifference
  - OCR will investigate all cases of possible willful neglect
  - OCR will impose penalty on all violations due to willful neglect
- Revised definition of **reasonable cause** (fills gap between “did not know ...” and willful neglect)
- **Greater OCR discretion to proceed directly to penalty without seeking informal resolution**

# OCR Guidance/Compliance Tools

## What's in the Works



Office for Civil Rights (OCR) is preparing:

- Fact Sheets/Q&A on New Provisions
- Breach Risk Assessment Tool
- Minimum Necessary Guidance
- Better Compliance Tools for Small Entities
- Adaptation of SAG Training for CEs
- Expanded Consumer Materials/Videos



# Student Immunization & Decedent Information



## Decedent Information

- No longer PHI after 50 year period
- CE may disclose decedent's PHI to family members & others involved in care/payment for care of decedent prior to death, unless inconsistent with prior expressed preference.

## Student Immunizations

- CE may disclosure proof of immunization of child to schools in States with school entry laws with oral or written agreement of parent.

## Compound Authorizations

- Single authorization form permitted for use/disclosure of PHI for conditioned & unconditioned research activities, with clear opt in for voluntary (unconditioned) component
- Flexibility permitted on ways to differentiate components

## Future Use Authorizations

- Permitted if authorization has adequate description....would be reasonable for the individual to expect his/her PHI could be used for the research.
- Aligns with Common Rule informed consent requirements.

- Expressly provides that genetic information is PHI.
- Prohibits the use or disclosure of genetic information for underwriting purposes by all health plans, except long-term care plans.
- Terms and definitions track regulations prohibiting discrimination in health coverage based on genetic information.

# Implement HIPAA Compliance Program



- Risk analysis/risk management
- Policies and procedures
  - Perform a gap analysis to determine what policies and procedures must be revisited
- Training
- Implement and consistently apply sanctions
- Address OCR guidance
- Continue – or make an increased effort – to take advantage of the safe harbor by **encrypting** PHI according to HHS' guidance

# Integrated Behavioral Health Proposed Rules (OBH), 3.26.2013



**Will follow both federal laws:**

- Federal Confidentiality Law **42 CFR Part 2,**

and

- Public Law No. 104-191, the Health Insurance Portability and Accountability Act of 1996 (**HIPAA**)

# OCR Guidance/Compliance Tools



- De-identification Guidance  
<http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/De-identification/guidance.html>
- Sample Business Associate Contract Language  
<http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html>
- Risk Analysis Guidance  
<http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidance.html>
- Security for Mobile Devices (video/web)  
<http://www.healthit.gov/mobiledevices>

# HIPAA / HITECH References



US Department of Health and Human Services

<http://www.hhs.gov/ocr/privacy/index.htm>

“Confidentiality and Communication, A guide to the Federal Drug & Alcohol Confidentiality Law and HIPAA.” Authored by: The Legal Action Center

State of Colorado, Department of Human Services

[www.colorado.gov/cdhs](http://www.colorado.gov/cdhs), go to HIPAA, or

<http://www.colorado.gov/cs/Satellite/CDHS-Ops/CBON/1251580598869>

# Personally Identifiable Information (PII) and FERPA



# Personally Identifiable Information (PII) and FERPA



- Colorado Consumer Protection Act, Notification of Security Breach of Personally Identifiable Information (PII), (CRS §6-1-716)
- Family Educational Rights and Privacy Act (FERPA)

# Colorado Consumer Protection Act

## Personally Identifiable Information (PII)



**PII:** a Colorado resident's **first name** or **first initial and last name** in combination **with any one** or more of the following data elements:

- Social security number;
- Driver's license number or ID card number;
- Account number or credit/debit card number,
  - in combination with any required security code, access code, or password that would permit access to a resident's financial account.

# PII continued



“That relate to the resident, when the data elements are **not encrypted, redacted, or secured** by any other method rendering the name or the element unreadable or unusable:

**K. Foo 652-123-5874**

**James Smith 422504187 3597 0002, expiration date 4-14-14**

**PII** - does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records or widely distributed media.

**Colorado Open Records Act – (CORA)**

# HIPAA

School-based  
health centers run  
by covered entities

Private schools  
that get no federal  
funding

School health care  
providers  
submitting  
payments  
electronically

# FERPA

Health care  
information  
entered by school  
staff

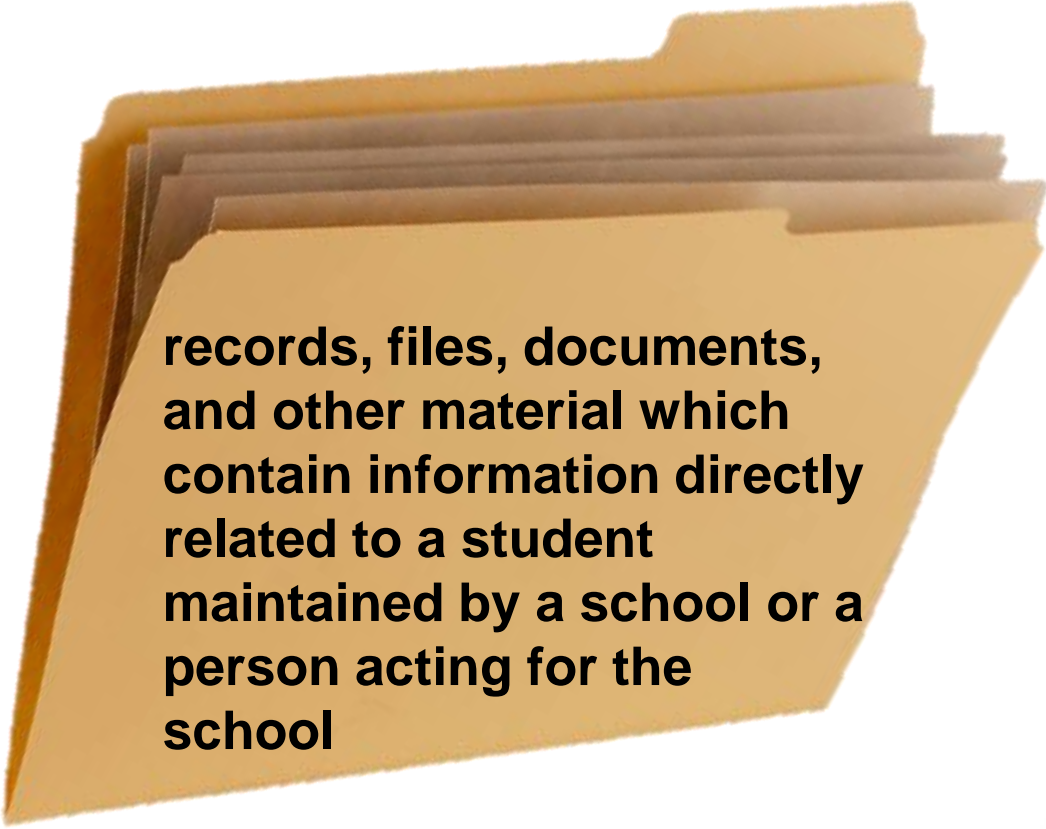
School health care  
centers

# What is FERPA's purpose?

- Protect privacy interests of students' education records
- Prohibits schools from disclosing personally identifiable information without consent of parent

# What does FERPA do?

Governs access to and release of educational records by public and private schools **that receive federal funding.**



**records, files, documents,  
and other material which  
contain information directly  
related to a student  
maintained by a school or a  
person acting for the  
school**

# Parental Access



Parent  
reviews

Parent  
releases

Student 18 or older → right of review and release

# Written Authorizations

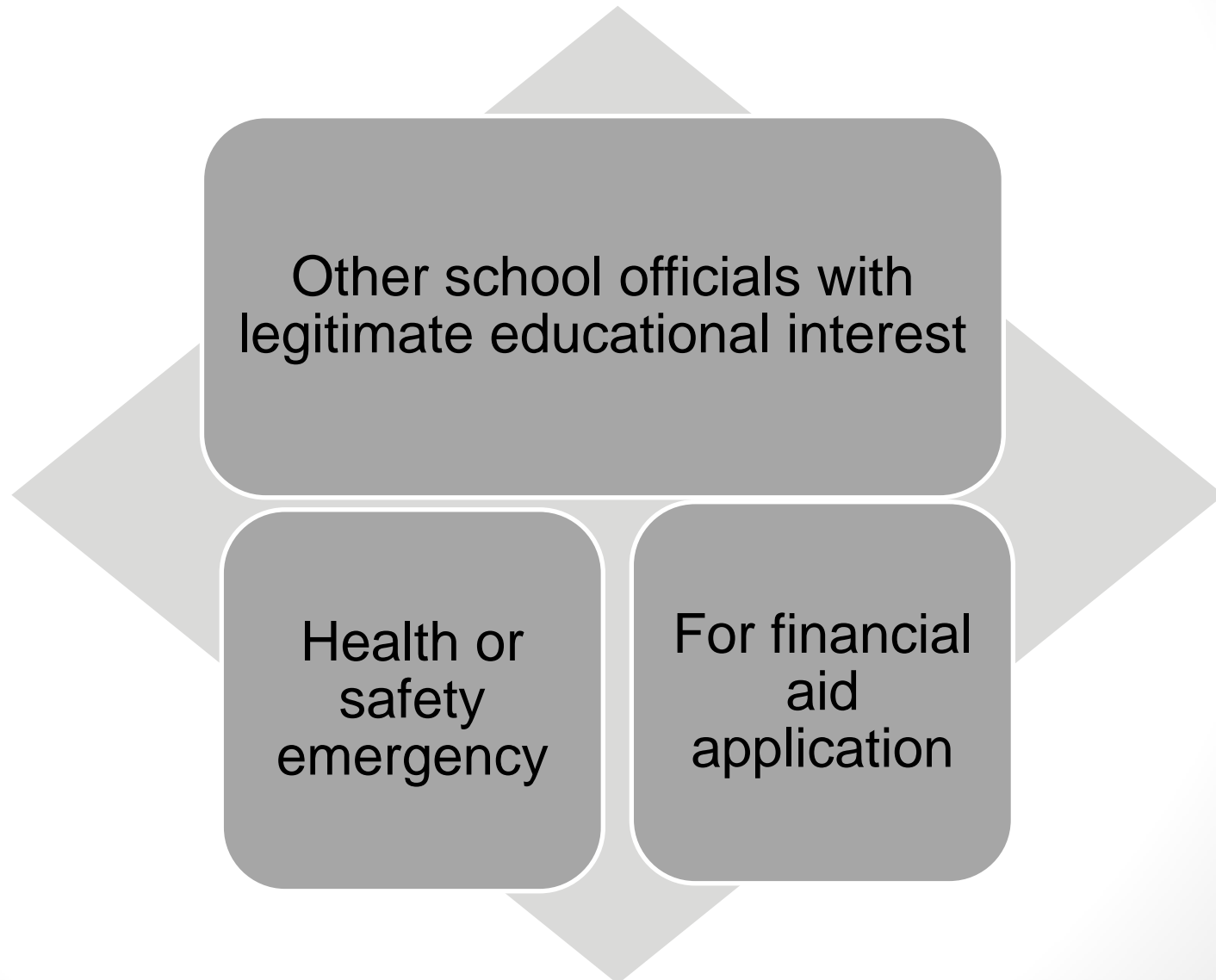
- Specify the records to be disclosed
- State the purpose of the disclosure
- Identify the party or class of parties to whom disclosure is to be made
- Signed and dated by the parent



# Subpoenas and Court Orders

Schools must make a “reasonable effort” to notify the parent of the order or subpoena before releasing the records.

# Permitted Disclosures without Authorization



# FERPA Compliance



- **Parental Consent Form**

- Must notify parent of what they are sharing and with whom, for what purpose and duration
- Writing must be clear and user friendly

- **Court Order**

- MUST be specific
- Individualized (CANNOT be blanket order)
- Reflect notice to FERPA Parent
- May limit scope of education records or use FERPA definition

- **Research Exception**

- For purpose of improving instruction
- Personally identifiable information protected
- Information destroyed when no longer needed for the research

School may disclose personally  
identifiable information only on the  
condition that the party to whom the  
information is disclosed

will not re-disclose the information  
without the prior consent of the parent or  
eligible student.

# FERPA Resources

- National Juvenile Information Sharing Initiative – website: [www.juvenileis.org](http://www.juvenileis.org)
  - Online Training: ***Re-disclosure of Children and Youth Information – HIPAA, FERPA and 42 CFR***
- National Center for Mental Health Promotion and Youth Violence Prevention
  - Navigating Information Sharing website: <http://sshs.promoteprevent.org/nis>
  - ***Learning the Laws – FERPA law; FERPA Scenarios***

# Questions?

**Kat Foo**

HIPAA Privacy and Security Officer

Colorado Department of Human Services

[Kathleen.Foo@state.co.us](mailto:Kathleen.Foo@state.co.us)

303.866.5871

# ***Process Change and Implementation of Authorization/Consent Form – Jefferson County Juvenile Assessment Center***

***Jeff McDonald, Executive Director, 1<sup>st</sup> Judicial Youth Services  
Program, Director, Jefferson County Juvenile Assessment Center***

***Stephanie Rondenell, Executive Director – National Juvenile  
Information Sharing Initiative***

# Consent Process Background



- CCYIS Privacy Committee (2011) was created to:
  - Identify privacy and confidentiality issues related to information sharing across agencies
  - Identify gaps in policy and practices
  - Develop standardized procedures
- Developed a consent / privacy matrix to assist in determining when consent was needed and what laws applied



# Consent and Privacy Matrix Online Tool



COLORADO  
CHILDREN & YOUTH  
INFORMATION SHARING COLLABORATIVE



[HOME](#) | [NJISI SITES](#) | [ABOUT US](#) | [NEWS](#) | [TOOLS](#) | [TRAINING](#) | [RESOURCES](#) | [PUBLICATIONS](#) | [DISCUSSIONS](#)

In Cooperation With



Office of Juvenile Justice and  
Delinquency Prevention



Office of Justice Programs

## NJISI SITES



Click on your state to see  
promising sites in your area

## QUICK LINKS

Substance Abuse and Mental  
Health Services  
Administration

NASCIO – National  
Association of State Chief  
Technology Officers

National Council of Juvenile  
and Family Court Judges

GOVERNANCE  
GUIDELINES  
FOR JUVENILE  
INFORMATION SHARING

TRAINING AND  
TECHNICAL ASSISTANCE  
REQUEST FORM

NJISI ADVISORY GROUP

FREQUENTLY  
ASKED QUESTIONS

## NATIONAL CONSENT AND PRIVACY MATRIX

Bitatur, officat iberior poreprem quunt accat. Ectiontsequi dolorecus sequi doluptatibus quis quatem dolessi tatiis seque sitatur sus ma dolumet que ati dolupta tatem. Et hiligenest as ent, od esti beatatius doluptate volorup tasperi onecea volestio coresequia pla sed quiatemquam, seque voluptatquam quaeepud aeriorumquas doluptatem con nem fugit labor.

Select a State to perform a Search

Colorado ▾

Incident or Event Requiring Data Exchange

Comply with Judicial Issued subpoena ▾

Primary Agency Needing Information

School ▾

Participating Agencies which May Provide  
Records

School ▾

Data Exchange Element Types

Supervision Data ▾

Time/Urgency

As Soon as Possible ▾

**SUBMIT**

[HOME](#) | [NJISI SITES](#) | [ABOUT US](#) | [NEWS](#) | [TOOLS](#) | [TRAINING](#) | [RESOURCES](#) | [PUBLICATIONS](#) | [MEMBER LOG-IN](#)

©2009, 2011, 2012 by Center for Network Development/National Juvenile Information Sharing Initiative. All rights reserved. No part of any document may be reproduced or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of CND/NJISI.

This website was prepared by the Center for Network Development, and supported by grant numbers 2007-JF-FX-K053/2009-MU-FX-K101 from the Office of Juvenile Justice and Delinquency Prevention, Office of Justice Programs, U.S. Department of Justice.

Points of view or opinions expressed in this website are those of the authors and do not necessarily represent the official positions or policies of OJJDP or the U.S. Department of Justice.

# Conducted Consent Form Analysis



- Collected over 45 consent forms from the CCYIS membership
- Agencies brought in multiple forms used by divisions and departments
- Privacy and Security SME and NJISI project team conducted a review and analysis:
  - Data collected
  - Purpose for the form (mental health, substance abuse, common informed consent)
  - Documented age of form and disclosures provided to recipient
  - Signatures required – disclaimers provided by agencies/organizations

# Standardize Consent Form



- Includes all agency contact information
- Includes youth information and identifiers for youth
- Has a section for 'consenter' – person authorized to provide legal consent for information sharing
- Provides list of agencies and service providers
- Allows form to be filled out online or manually
- Gives a clear understanding of the purpose of the information sharing that will occur
- Provides a list of disclaimers by record types
- Allows requester to review record types or categories with families in the process

# Consent Form Demonstration

# Authorization/Consent Use Case Activity

*MacKenzie Use Case*

# Authorization/Consent Form Implementation

*Jeff McDonald, Executive Director, 1<sup>st</sup> Judicial  
Youth Services Program, Director, Jefferson  
County Juvenile Assessment Center*

# Process Changes

- Understanding the existing process
- Examination of forms and consent
- Assisted in development of form
  - walked through multiple agency process at the JCJAC
- Discussed differences between comprehensive versus universal forms

# Implementation of Form and Process Changes

- Presented new form to leadership
- Met with partners and JCJAC agencies
- Implemented form with 'JAC staff' only
- Reviewed outcomes with NJISI team
  - Changes and improvements identified
  - Redeployment of form
- Implemented with SB94 staff
  - Changes and improvements identified
  - Reviewed training needs and tools
- Final changes deployed – training in development



# Lessons Learned

## Staff Positives

- Ease of use
- Form structure
- More 'legal' than previous form
- Easy to visualize process/Easy to Understand

## Staff Negatives

- It takes longer to fill-out
- Problems if 'authorized consentor' doesn't come with youth to JAC
- Explaining the disclosures is 'overwhelming'
- Need more training
- Process changes
- Have to type it up!

## Improvements

- More space in 'other' fields
- Need a 'script' on what to say to families – how to explain the disclosures
- Need multiple ways to document how the information will be shared
- Would like dates to auto-populate

# Lesson Learned

## Parent Responses

- Had all the necessary information,
- Did not think it was 'too much',
- Easy to see all that was being collected,
- Appropriate print size – it had all of the proper citations and lists all necessary information,
- Felt informed about rights – what she had the right to do and not do –
- Too many acronyms - thought that all the acronyms were appropriately explained and highlighted on the form,
- Staff did a great job explaining the form.

# Use Case #1

## *Juvenile Probation Officer and Outpatient Mental Health Counselor*

# Use Case #2

## *Multi-agency Meeting to Develop Re-Entry / Transition Plan*

# Closing Remarks

**Meg Williams**

**Manager, Office of Adult and Juvenile Justice  
Assistance**

**Division of Criminal Justice**

**Colorado Department of Public Safety**

# Q & A Session