

# CONFIDENTIALITY AND PRIVACY:

42 CFR Part 2,  
HIPAA, and  
Goals of  
Interoperability

EQR MEDICAID QUALITY FORUM  
October 28, 2015

# PANEL MEMBERS

- **Julián Gonzales, Certification Supervisor, Behavioral Health and Service Integration Administration, Department of Social and Health Services**
- **Kathryn Ruckle, Privacy Officer, Department of Social & Health Services**
- **Karen Jensen, Healthier Washington Data Privacy & Security Manager, Health Care Authority**

# AUDIENCE

- **Regional Support Networks (RSNs)**
- **Managed Care Organizations (MCOs)**
- **State Agencies covered by HIPAA (DSHS & HCA)**
- **Health Care providers and others involved in behavioral health care**

# OVERVIEW

- **Federal laws governing confidentiality/privacy of health records, including alcohol/drug patient records**
  - **42 CFR Part 2**
  - **HIPAA**
- **Reconciling confidentiality laws in new models of care**

## 42 CFR PART 2

**Disclosure of information that identifies patient (directly or indirectly) as having a current or past drug or alcohol problem (or participating in a drug/alcohol program) is generally prohibited, unless:**

- **Patient consents in writing or**
- **Another exception applies**

## 42 CFR PART 2

This is true even if the person seeking the information—

- Already has it
- Has other ways to get it
- Has some kind of official status
- Has obtained a subpoena or warrant
- Is authorized by State law

# 42 CFR PART 2

## Who is covered?

Drug/alcohol treatment and prevention programs that are Federally assisted must follow 42 C.F.R. Part 2

Three definitions of “Program”

First definition:

Individual or entity other than general medical facility that holds itself out as providing, and does provide, drug/alcohol diagnosis, treatment, or referral for treatment

# 42 CFR PART 2

## **Second definition:**

**An identified unit within a general medical facility that holds itself out as providing, and does provide, drug/alcohol diagnosis, treatment, or referral for treatment**

## **Third Definition:**

**Medical personnel or other staff in a general medical care facility whose primary function is the provision of drug/alcohol diagnosis, treatment, or referral for treatment, and who are identified as such**



# 42 CFR PART 2

The law does not define “general medical facility,” but SAMHSA FAQs give some examples:

- Hospitals
- Trauma Centers
- Federally Qualified Health Centers

Key point when dealing with a general medical facility:

It is the **unit or medical personnel** that is the “**program**” NOT the whole general medical facility

# 42 CFR PART 2

**What does “holds itself out” mean?**

**Law does not define this but SAMHSA FAQs give examples:**

**State licensing procedures, advertising, or posting notices in office, certifications in addiction medicine, listings in registries, internet statements, consultation activities for non-“programs,” information given to patients and families, any activity that would reasonably lead one to conclude those services are provided.**

# 42 CFR PART 2

Examples of a “program” –

First definition:

- Freestanding drug/alcohol treatment program
- Student assistance program in a school
- Primary care providers who provide drug/alcohol services as their principal practice

# 42 CFR PART 2

## Second definition:

- Detox unit
- Inpatient or outpatient drug/alcohol program within a general medical facility

## Third definition:

- Addiction specialist working in a primary care practice

# 42 CFR PART 2

## When is a program “federally assisted”?

- Receives Federal funds in any form (even if not used for drug/alcohol services), or
- Is authorized, licensed, certified, registered by the Federal government, such as—
  - Assisted by IRS by grant of tax-exempt status
  - Has DEA registration to dispense controlled substances to treat drug/alcohol abuse
  - Is authorized to provide methadone treatment
  - Is certified to receive Medicaid or Medicare reimbursement

# 42 CFR PART 2

## What is a “disclosure”?

- **Communication (oral or written) of information that identifies someone as having a past or current drug/alcohol problem or being a past or current patient in a drug/alcohol program**
- **Disclosure includes communications to people who already know the information**

# 42 CFR PART 2

Four exceptions to the general rule prohibiting disclosure that are most relevant to co-located and integrated services:

**Exception 1: Written consent**

**Exception 2: Internal communications**

**Exception 3: Medical emergency**

**Exception 4: Qualified service organization agreement (QSOA)**

# 42 CFR PART 2

## **Exception 1: Written Consent**

Proper Format for Consent to Release Information  
must be in writing!

- 1.Name/general designation of program making disclosure
- 2.Name of individual/entity receiving disclosure
- 3.Name of patient who is subject of disclosure
- 4.Purpose/need for disclosure
- 5.Description of how much and type of information will be disclosed
- 6.Patient's right to revoke consent and any exceptions
- 7.Date/event/condition on which consent expires
- 8.Patient's signature
- 9.Date signed
- 10.HIPAA: program's ability to condition treatment, payment, enrollment, or eligibility on the consent



# 42 CFR PART 2

## **Exception 1: Written Consent** **Written Prohibition on Redisclosure**

Language dictated by regulations:

“This information has been disclosed to you from records protected by Federal confidentiality rules (42 CFR part 2). The Federal rules prohibit you from making any further disclosure of this information unless further disclosure is expressly permitted by the written consent of the person to whom it pertains or as otherwise permitted by 42 CFR part 2. A general authorization for the release of medical or other information is NOT sufficient for this purpose. The Federal rules restrict any use of the information to criminally investigate

# 42 CFR PART 2

## Exception 2: Internal Communications

OK to disclose information to:

- Other program staff
- Entity that has administrative control over the program (e.g., records or billing department of a general hospital program is part of)
- Only to the extent the recipient needs information in connection with provision of drug/alcohol services (purpose and amount)

(\*HIPAA: “minimum necessary”)

# 42 CFR PART 2

## Exception 3: Medical Emergencies

OK to disclose:

- To Medical personnel
- To the extent necessary
- To meet a bona fide medical emergency of the patient or any other individual

What is a **medical emergency**?

- Immediate threat to health of individual AND
- Requires immediate medical attention

# 42 CFR PART 2

## Exception 4: QSO/BA AGREEMENTS

- OK to disclose without patient consent to certain outside organizations that provide services to the program or its patients
- 42 C.F.R. Part 2 calls these organizations Qualified Service Organizations (“QSOs”)
- HIPAA calls these organizations Business Associates (“BAs”)

### Examples of services provided by QSOs

- Medical services, data processing, dosage prep, lab analyses, vocational counseling, patient transport, legal or accounting

# 42 CFR PART 2

## Exception 4: QSO Agreements

### Requirements of a QSO Agreement

- Program must enter into written agreement with the QSO, agreeing:
- QSO is fully bound by 42 C.F.R. Part 2
- QSO will resist an effort to obtain access to patient information except as permitted by 42 C.F.R. Part 2
- The written agreement must contain certain elements required by 42 C.F.R. Part 2
- If organization serving as QSO is also covered by HIPAA, must also meet requirements of a BA agreement

# HIPAA APPLICATION

- HIPAA sets the *minimum* standards for confidentiality of PHI.
- State laws may be more restrictive than HIPAA - (In WA these include laws that apply to mental health, HIV/AIDS and STD test results, diagnosis or treatment, medical information for minors, and reproductive health.)
- 42 CFR Part 2 is a federal law that is more restrictive than HIPAA in use and disclosure of past or current substance abuse treatment or being a past or current patient in a substance abuse program.

# HIPAA & 42 CFR PART 2 APPLICATION

## HIPAA

- Applies if:
- Health Care Provider, Health Plan, or Health Care Clearing house;  
**AND**
- Transmit PHI electronically via covered transactions

## 42 CFR Part 2

- Applies if:
- Substance abuse treatment and prevention **program**;  
**AND**
- **Federally assisted** - (i.e. receives federal \$ even if not used specifically for SUD services.)

# HIPAA & CFR PART 2 APPLICATION

- **Most Substance Use Disorder (SUD) treatment programs are covered by both laws.**
- **Do you have to comply with both? YES!**
- **Certain programs within DSHS must follow both laws. This impacts internal sharing of information.**



# HIPAA OVERVIEW

- **Privacy Rule – Keep PHI private!**
- **Security Rule – Keep PHI secure!**
- **Breach Notification Rule – If you don't keep PHI private and secure you have to notify!**

# HIPAA: PRIVACY RULE

- **Regulates the circumstances under which covered entities may use and disclose PHI and requires covered entities to have safeguards in place to protect the privacy of the information.**
- **Examples of protected health information (PHI) include:**
  - **Demographic (name, address, DOB, SSN, Driver's Lic #)**
  - **Financial (credit card/bank acct #, claims info)**
  - **Eligibility (client status; receiving public assistance)**
  - **PHI (includes the above & clinical info – diagnosis, medications, lab results)**

# HIPAA: SECURITY RULE

- **Requires covered entities to implement certain administrative, physical, and technical safeguards to protect electronic information.**
- **Examples –**
  - **Administrative Safeguard – Training**
  - **Physical Safeguard –key card access**
  - **Technical Safeguard - encryption**

# HIPAA: BREACH NOTIFICATION RULE

- Requires covered entities and Business Associates (contractors) to provide notification following discovery of a breach of unsecured protected health information.
- Notification required to go to individual whose information was compromised and to the Secretary of U.S. Dept. of Health and Human Services.

“Unsecured PHI” is PHI that has not been made unusable, unreadable, or indecipherable to unauthorized individuals through the use of technology such as encryption.

# BREACH NOTIFICATION AT DSHS

## ■ DSHS Staff:

If a breach or potential breach of Confidential Information is discovered, staff at a minimum must notify within one (1) business day of discovery:

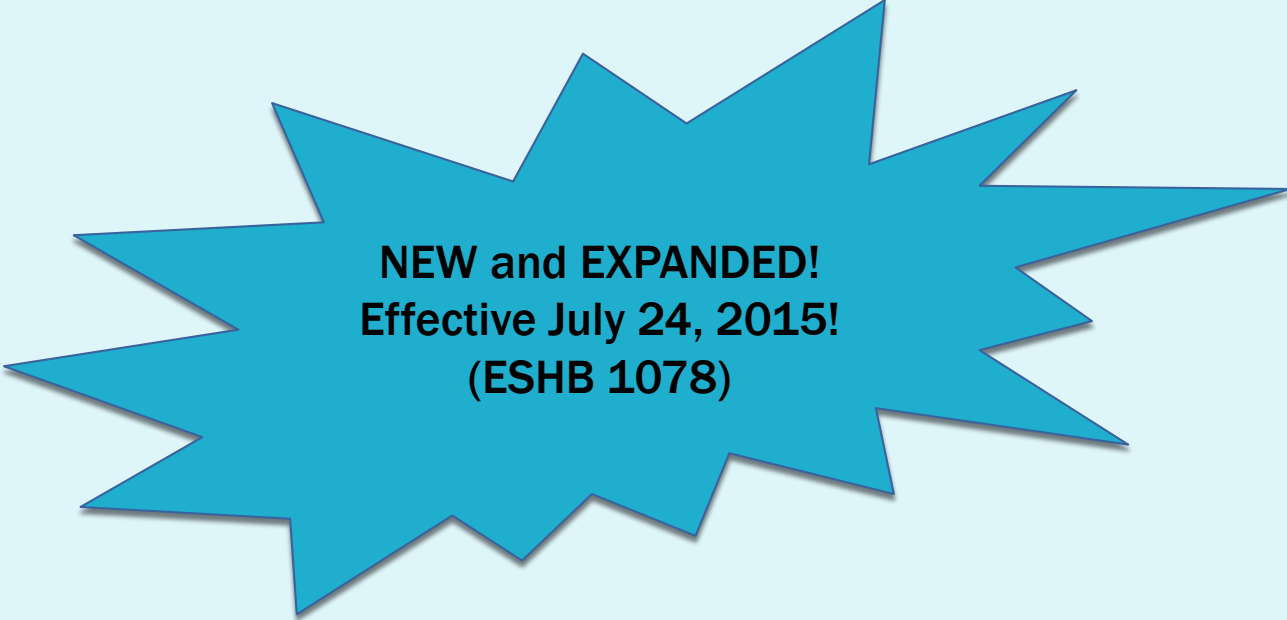
- The ISSD Service Desk at [ISSDservicedesk@dshs.wa.gov](mailto:ISSDservicedesk@dshs.wa.gov); and
  - The administration's or division's Privacy Coordinator.
  - For breaches involving over 500 individuals staff must also notify the DSHS Privacy Officer at [DSHSprivacyofficer@dshs.wa.gov](mailto:DSHSprivacyofficer@dshs.wa.gov).
- 
- ## ■ DSHS Contractors – Standard DSHS Contract language:
- Business Associate will notify the DSHS Contact shown on the cover page of this Contract within one (1) business day by telephone or e-mail of any potential Breach of security or privacy of PHI by the Business Associate or its Subcontractors or agents.

# BREACH NOTIFICATION

- Under HIPAA –
  - If over 500 must notify and report to Secretary within 60 days
  - If over 500 must also notify media
  - If under 500 must notify individual within 60 days, but you can report to Secretary anytime but not later than 60 days after the end of the calendar year

# OTHER BREACH NOTIFICATION STATUTES

- RCW 70.02.290 – Applies to state or local agencies obtaining patient health care information that are not health care facilities or providers.
- RCW 42.56.590 & 19.255 RCW – Notice of security breaches



**NEW and EXPANDED!**  
**Effective July 24, 2015!**  
**(ESHB 1078)**

# PERMITTED DISCLOSURES (HIPAA & 42 CFR PART 2)

- Information De-identified (to HIPAA standards)
- **Written patient consent/authorization** (must comply w/ laws)
- **Medical emergencies**
- Qualifying research activities
- Audit/evaluation activities
- Appropriately tailored Court Order (“QPO”)
- **Communications within a Program**
- **Qualified service organization agreement and/or BAA**
- To report child abuse or neglect
- Crime on program premises/against program personnel



# INTEROPERABILITY

- **The vision and expectations for electronic health records:**
  - Integration across facilities and providers
  - Improved patient care
- **The reality:**
  - Point-to-point EHR sharing is impractical
  - Regional and organizational EHRs are still silos without full interoperability within and across systems

# FEDERAL LANDSCAPE

- **2009 - Federal legislation**
  - **American Recovery and Reinvestment Act (ARRA)- \$20 billion for health information technology infrastructure**
  - **HITECH Act – Health Information Technology for Economic and Clinical Health -**
  - **Office of the National Coordinator for Health Information Technology (ONC)**

# WASHINGTON IMPLEMENTATION

- **Washington State Implementation**
  - **Health Care Authority – lead agency to coordinate funding from ARRA and the HITECH Act**
  - **Substitute Senate Bill 5501 (2009) – designated the Health Care Authority as lead agency for implementation of Health Information Technology Programs**

# WASHINGTON INITIATIVES

- **Washington Health IT Initiatives**
  - **Medicaid Electronic Health Record Incentive Program**
  - **Washington Health State Health Information Exchange**
  - **State Medicaid HIT Plan**

# HEALTH CARE AUTHORITY

- **CLINICAL DATA REPOSITORY (CDR)**
  - Health Care Authority response to interoperability challenges
  - Connection between disparate EH platforms
  - Aggregates clinical information in on e accessible location

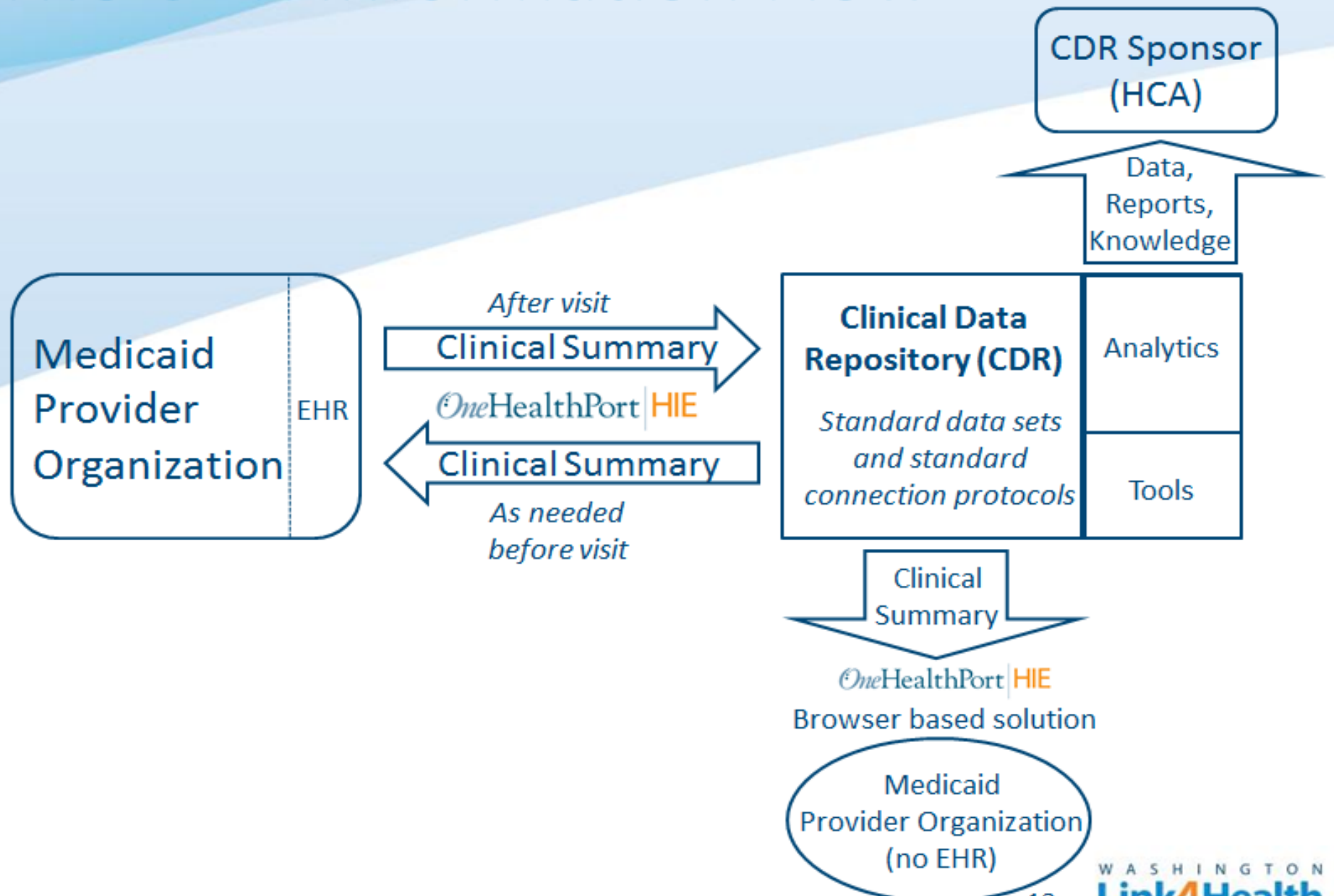
# CARE COORDINATION

- **“LINK4HEALTH” Initiative**
  - **Multi-year initiative to advance the statewide electronic exchange of clinical records**
  - **Goal: improve coordination of care and patient outcomes**
  - **Near-real time medical, dental, behavioral health and social service support data**

# CDR IMPLEMENTATION

- **Link4Health Clinical Data Repository - Staged Implementation**
  - **Working with state Health Information Exchange**
  - **First lives – Apple Health Enrollees in Managed Care**

# The CDR Information Flow





# OPPORTUNITIES AND CHALLENGES

- **CONNECTION TO PRIVACY AND SECURITY ISSUES**
  - The same laws and rules apply with respect to confidentiality and privacy
  - Technology solutions:
    - Data segmentation
    - Access controls
    - Consent management



**Questions  
and  
Discussion**

**Thank you!**