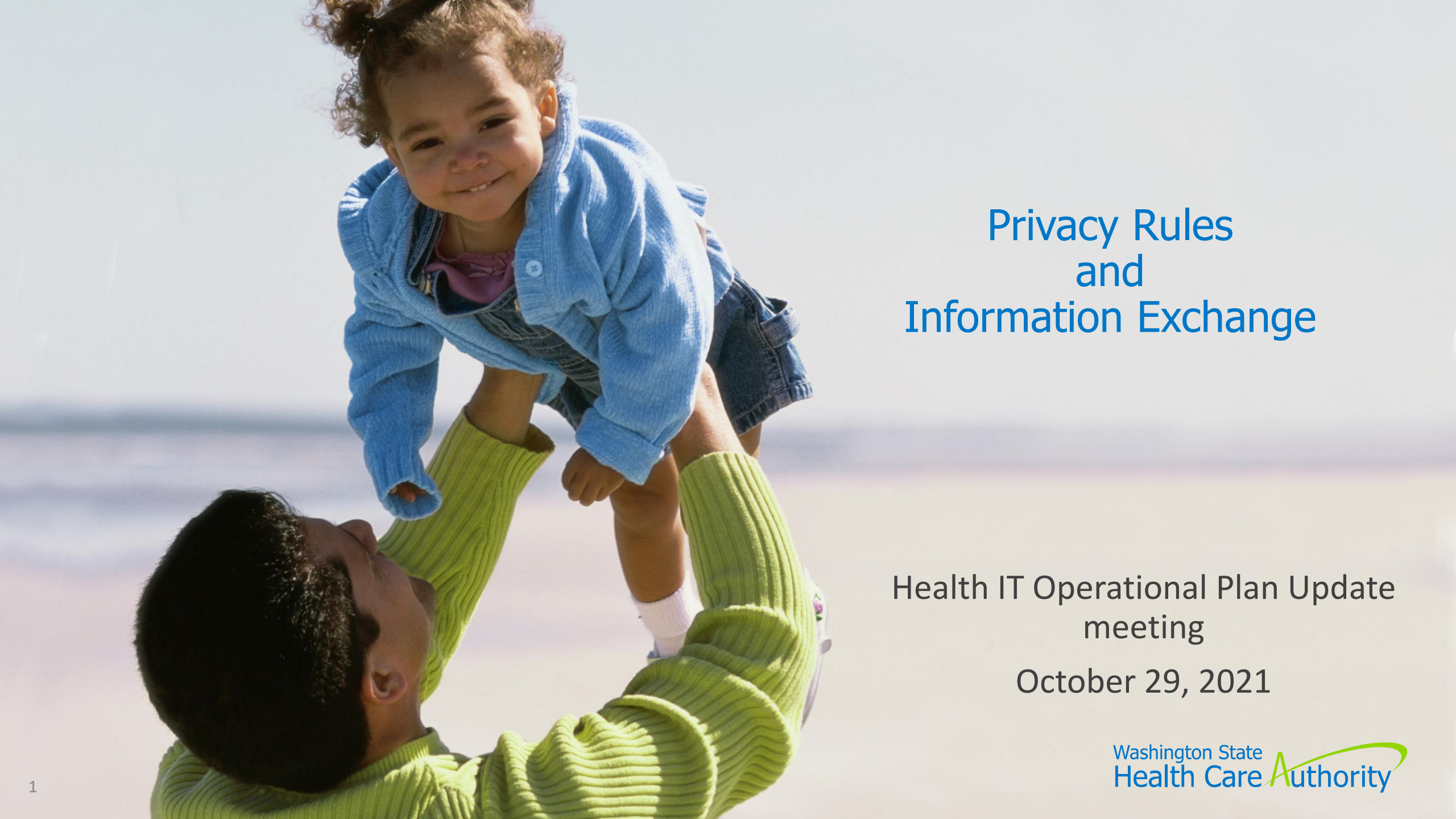

Privacy Rules and Information Exchange

Health IT Operational Plan Update meeting

October 29, 2021

Washington State Health Care Authority

Agenda

- Privacy Requirements for Health Information Exchange
  - 42 CFR Part 2
  - HIPAA
  - Washington State Privacy Requirements
- Presenter: Sam Mendez, HCA Privacy Officer
- Scenarios: Applicability of privacy rules to information access and exchange on behalf of a person with co-occurring mental health and substance use disorders

42 CFR Part 2

An Introduction

Sam Mendez
Privacy Officer
Washington State Health Care Authority

Topics

1. Part 2 & HIPAA
2. Part 2: What Does It Cover?
3. Who Must Follow Part 2?
4. Proper Consent
5. Disclosures Not Requiring Consent

Part 2 & HIPAA

Summarized & Compared

Part 2 & HIPAA

Health Insurance Portability and Accountability Act (HIPAA)

- Federal law that applies to Covered Entities (health plans, health care clearinghouses, and most health care providers) and their Business Associates
- Requires Covered Entities and their Business Associates to protect and not disclose the Protected Health Information (PHI) of individuals.
- Security requirements
- Privacy requirements – Cannot disclose PHI outside of certain circumstances
- Dates to 1996, updated significantly by HITECH Act, effective 2013

Part 2 & HIPAA

42 CFR Part 2

- Federal law that applies to Part 2 Programs, their Qualified Service Organizations (QSOs), and holders of Part 2 data
- Requires entities to protect and not disclose records arising from Part 2 Programs.

- Entities still subject to HIPAA
- Far fewer exceptions allowing disclosure
- Dates to 1972, effective 1975

Part 2 & HIPAA

When Multiple Laws Apply…
The most protective law must be followed.

Often Part 2 will be the more protective law.

Part 2 & HIPAA

When multiple laws apply,
the most protective law must be followed.

Often Part 2 will be the more protective law.

- e.g. Disclosing a record for treatment purposes.
  - HIPAA permits disclosures for treatment purposes without patient consent.
  - Part 2 requires patient consent.
- Part 2 is more protective, so written patient consent must be obtained.

Part 2: What Does it Cover?

Entities & Information

Part 2: What Does it Cover?

- What is a Part 2 Program?
  - A federally assisted entity that "holds itself out as providing, and provides, substance use disorder diagnosis, treatment, or referral for treatment."

Part 2: What Does it Cover?

- What is a Part 2 Program?
  - A federally assisted entity that "holds itself out as providing, and provides, substance use disorder diagnosis, treatment, or referral for treatment."
- Could be:
  - An entity or individual on its own (like a rehabilitation facility)
  - An identified unit within a general medical facility
  - Medical personnel or other staff in a general medical facility whose primary function is the provision of SUD treatment

Part 2: What Does it Cover?

- What is a Part 2 Program?
  - A federally assisted entity that "holds itself out as providing, and provides, substance use disorder diagnosis, treatment, or referral for treatment."
- "Federally assisted" is interpreted very broadly, and most entities out there are federally assisted. Includes:
  - Receiving any federal funding
  - Having any license, registration, certification from the federal government (e.g. DEA license to prescribe)
  - Medicare/Medicaid provider
  - Non-profit status

Part 2: What Does it Cover?

- What is a Part 2 Program?
  - A federally assisted entity that "holds itself out as providing, and provides, substance use disorder diagnosis, treatment, or referral for treatment."
- An emergency room in a general hospital where 95% of its work is SUD-related services (say due to a drug epidemic) is still not a Part 2 Program unless it is identified as a SUD provider and "holds itself out" to the public as providing SUD services.

Part 2: What Does it Cover?

- What is a Part 2 Program?
  - A federally assisted entity that "holds itself out as providing, and provides, substance use disorder diagnosis, treatment, or referral for treatment."
- BUT a doctor in that same general hospital who is identified as a SUD provider and whose work is 95% SUD-related services (say due to a drug epidemic) is a Part 2 Program.
  - The difference: the doctor is identified as a SUD provider and her primary function is SUD services, regardless of what she "holds herself out" to the public.

Part 2: What Does it Cover?

- Information: Part 2 protects information that identifies someone as seeking or receiving substance use disorder (SUD) services from a Part 2 program.
  - E.g. name, address, date of birth, social security number, fingerprints, status in the program, diagnosis, treatment, medication
- Includes information in any form – written, verbal, electronic

Part 2: What Does it Cover?

- All Part 2 information relates to SUDs
- But not all SUD information is subject to Part 2

Part 2: What Does it Cover?

- All Part 2 information relates to SUDs
- But not all SUD information is subject to Part 2
- For Part 2 to be applicable, the information must have arisen from a Part 2 Program and must relate to a SUD.

Part 2: What Does it Cover?

- Examples where Part 2 doesn't apply
- All Part 2 information relates to SUDs, but not all SUD information is subject to Part 2
  - Example 1: ABC Rehab holds itself out as providing treatment services for alcohol, drug, and gambling addiction. John enters the program for his gambling problem.
    - John's information is ***not*** subject to Part 2 (not relating to a SUD)

Part 2: What Does it Cover?

- Examples where Part 2 doesn't apply
- All Part 2 information relates to SUDs, but not all SUD information is subject to Part 2
  - Example 2: Acme Hospital is a general hospital with an emergency unit. Jane suffers a heroin overdose and is taken to the emergency unit, where she is treated with naloxone.
    - Jane's information is ***not*** subject to Part 2 (relates to a SUD, but it wasn't at a Part 2 Program)

Part 2: What Does it Cover?

- All Part 2 information relates to SUDs
- But not all SUD information is subject to Part 2
- For Part 2 to be applicable, the information must have arisen from a Part 2 Program and must relate to a SUD.
- Questions?

Who Must Follow Part 2?

Part 2 Programs & Lawful Holders

Who Must Follow Part 2?

- Part 2 Programs - (A federally assisted entity that "holds itself out as providing, and provides, substance use disorder diagnosis, treatment, or referral for treatment.")
  - Standalone entities
  - Identified units within a general facility
  - Identified staff within a general facility

Who Must Follow Part 2?

- Lawful Holders: anyone who receives protected records from a Part 2 Program
  - Primary care providers
  - Social workers
  - Contractors
  - Lawyers

- Lawful holders will often (but not always) will get Part 2 information either via
  - written patient consent, or
  - Qualified Service Organization Agreement

Proper Consent

Proper Consent

- In most cases, Part 2 information cannot be shared without written patient consent
  - Some exceptions
- Part 2 follows the information even to non-Part 2 Programs

Proper Consent

- 9 required elements to a valid written consent
  1. Patient name
  2. Who is making the disclosure
  3. Who is receiving the information
  4. How much and what type of information being disclosed
  5. Purpose of the disclosure
  6. Patient notice of right to revoke consent
  7. Expiration date/event/condition
  8. Patient signature
  9. Date signed

Proper Consent

- Consent forms may now authorize disclosure to an individual or entity (changed in 2020)
  - Previously, could only name individuals, which could make disclosure difficult
  - Also it is no longer required for an entity to have a treating provider relationship with patient

Proper Consent

- Consent forms must be accompanied with a written notice prohibiting re-disclosure
  - (1) This record which has been disclosed to you is protected by federal confidentiality rules (42 CFR part 2). The federal rules prohibit you from making any further disclosure of this record unless further disclosure is expressly permitted by the written consent of the individual whose information is being disclosed in this record or, is otherwise permitted by 42 CFR part 2. A general authorization for the release of medical or other information is NOT sufficient for this purpose (see §2.31). The federal rules restrict any use of the information to investigate or prosecute with regard to a crime any patient with a substance use disorder, except as provided at §§2.12(c)(5) and 2.65; or
  - (2) 42 CFR part 2 prohibits unauthorized disclosure of these records.

Proper Consent

- Consent & Health Information Exchanges (HIEs)
  - Part 2 information may be shared through an HIE with written patient consent
  - The consent form must specify the name of the HIE and the recipients
  - Can name specific HIE participants or a general designation (e.g. “all my current and future treating providers”)

Disclosures Not Requiring Consent

Disclosures Not Requiring Consent

- Part 2 requires patient's written consent to make a disclosure unless an exception applies
  - Just like HIPAA
  - Far fewer allowable disclosures than HIPAA
- In sum:
  - Medical emergencies
  - Research
  - Audit and evaluation
  - De-identified information
  - Internal communications
  - QSOs
  - Reporting certain crimes
  - Reporting suspected child abuse
  - Court order

Disclosures Not Requiring Consent

- In sum:
  - Medical emergencies
  - Research
  - Audit and evaluation
  - QSOs
  - Reporting suspected child abuse
  - Court order
  - De-identified information
  - Internal communications
  - Reporting certain crimes

Disclosures Not Requiring Consent

- Medical emergencies
  - Part 2 programs may share Part 2 information with medical personnel to meet a bona fide medical emergency
  - Only when prior consent cannot be obtained
  - Program must document the disclosure
  - Information loses its Part 2 protections once shared

Disclosures Not Requiring Consent

- Research
  - Very similar to HIPAA exception
  - Records may be disclosed for research
  - Generally must be IRB approved
  - Generally must be requested from a HIPAA covered entity, business associate, or FDA-regulated entity

Disclosures Not Requiring Consent

- Audit and evaluation
  - Part 2 Programs & lawful holders may share records with certain entities that are conducting audits and evaluations
  - Entity conducting the audit/evaluation must first agree in writing to follow Part 2 requirements
  - Records may only be used for the audit/evaluation

Disclosures Not Requiring Consent

- Audit and evaluation
  - Includes governments, entities with direct administrative control, and contractors where required by law
  - Records can only be disclosed if audit/evaluation cannot be carried out with de-identified information

Disclosures Not Requiring Consent

- Audit and evaluation
  - Illustrative list of what are considered audits and evaluations
    - E.g. government agency may review Part 2 records to identify necessary changes in policies or procedures to improve care and outcomes for patients with SUDs

Disclosures Not Requiring Consent

- QSOs & QSOAs
  - QSOA: Written agreement in place between Part 2 Program and QSO
  - QSO must agree to resist outside attempts to obtain Part 2 records
- Examples:
  - Data processing
  - Bill collecting
  - Legal services
  - Medical staffing services

Disclosures Not Requiring Consent

- QSOs & QSOAs
  - QSOAs are similar to HIPAA's business associate agreements, but not identical
  - Can be the same agreement incorporating both laws

Disclosures Not Requiring Consent

- Reporting suspected child abuse
- Part 2 does not apply to these disclosures IF
  - Being reported pursuant to state law
  - To appropriate state/local authorities
  - Suspected child abuse and neglect

- The original SUD information held by the Part 2 program is still subject to Part 2

Disclosures Not Requiring Consent

- Court Orders
- Person holding Part 2 information must disclose only with a valid court order and a subpoena
- They're aren't obligated with only one

- Doesn't apply to researchers, auditors, or evaluators (under those proper Part 2 sections)

Disclosures Not Requiring Consent

- Court Orders
- Court orders are only valid IF:
  - Necessary to prevent serious bodily injury or threat to life (includes child abuse)
  - Necessary in connection with investigation or procescution of extremely serious crime, OR
  - In connection with litigation or administrative proceeding where patient has offered testimony on the Part 2 information

Remember

When multiple laws apply, the most protective law must be followed.

All Part 2 information relates to SUDs, but not all SUD information is subject to Part 2

Thank You

Questions?

Sam Mendez
Privacy Officer
privacyofficer@hca.wa.gov

Scenario:
Information Access and Exchange on Behalf "Mary"

- Applicability of privacy rules to information exchange and access on behalf of a person with co-occurring mental health and substance use disorders (SUD)*

- Scenario: Hypothetical patient "Mary":
  - experiences a crisis,
  - transported to the Emergency Department (ED) at the nearby acute care hospital,
  - admitted to the in-patient psychiatric unit of the hospital,
  - transferred to and discharged from an SUD Intensive Out-patient Program (IOP)

- Along the way health information is accessed, created, and exchanged.

- Questions: Which privacy requirements apply and when?

Please Note: This is not legal advice. Please consult with your own legal counsel.

Technology Used in the Scenario

Technology Used	Definitions[1]
Electronic Health Record (EHR)	A digital version of a patient's paper chart, used to make information available instantly and securely to authorized users.
Care Everywhere	A free HIE platform that facilitates interoperable information exchange among providers and healthcare organizations regardless of EHR system or network that the user belongs to. Care Everywhere is an implementer of the Care*e*quality Framework.
Care*e*quality Framework	A public-private collaborative (including several HIT vendors) that facilitates agreement among diverse stakeholders to develop and maintain a common interoperability framework enabling exchange. Care*e*quality implementation guide (IG) outlines policy, technical, and process requirements for Implementers of the Care*e*quality Query-Based Document Exchange Use Case. The IG outlines requirements related to release of information and patient consent/authorization to share (as defined by HIPAA and 42 CFR Part 2).
Collective Medical (CM)	An HIT vendor that helps care teams across care settings collaborate to support their most vulnerable patients. CM provides real-time data for providers about: Where their patient is, Why they are being seen, Who else is treating them, What are avoidable risks.

1. See more complete technology/exchange definitions and details at end of slide deck.

Scenario 1:
Crisis Response and ED Admission and Discharge

- An emergency call comes in to 911.
- The caller notes that Mary will not wake up and suspects that Mary has overdosed. The caller notes that Mary has a history of using heroin and serious mental illness (major depression).
- EMS (ambulance) responds to the emergency.
- EMS arrives on the scene and finds Mary to be unresponsive and having difficulty breathing.

Questions: Crisis Response and Privacy

Accessing Information	Questions
EMS responders log into the portal of a nearby hospital to search for Mary's medical history, medications, allergies, and emergency contacts	Q1: Do EMS providers need Mary's consent to search for Mary's health information? Do any of the following privacy rules apply? • HIPAA • 42 CFR Part 2 • WA State MH Privacy Laws

Crisis Response and ED Admission and Discharge (cont'd)

- EMS administers Narcan and transports Mary to the ED at the nearby hospital.
- Mary is regaining consciousness when she arrives at the ED.

Questions: ED Admission and Privacy

Accessing Information	Questions

To understand Mary's history and condition, clinicians in the ED gather information from:
• **The EHR system used in the ED/acute care hospital** to see if Mary has an electronic health record and whether she has had any health care encounters.
• **Care Everywhere**, a module in their EHR system, to search and receive Mary's clinical history from health and behavioral health care providers that previously provided services to Mary. (Note: These providers may or may not use the same EHR as used at the ED).
• **Collective Medical** using the EDIE (Emergency Department Information Exchange) to:
  ○ search whether Mary has had other ED or acute care hospital visits (or SNF stays)
  ○ see if Mary has had opioid prescriptions from other providers (as noted in the PDMP); and
  ○ See notifications regarding whether Mary has had a safety and security event, has a Care plan, and if there are any current care team members who may have additional insights about Mary.
	Do clinicians in the ED need Mary's consent to search for Mary's clinical history using:
	• The Mary's EHR in hospital?
	• The Care Everywhere module (included in the EHRs used by many physical health and behavioral health providers)?
	• Collective Medical tools used in nearly all acute care hospitals and EDs, and by some Behavioral health providers in Washington State?
	
	Do any of the following privacy rules apply?
	• HIPAA
	• 42 CFR Part 2
	• WA State MH privacy laws

ED Discharge

- Based on a review of clinical information gathered from these electronic sources and information provided by Mary, ED clinicians enter the following clinical summary into Mary's EHR:

  - Mary reports that she is very depressed, the overdose was not accidental and she intended to kill herself.
  - Mary was recently discharged from an in-patient SUD treatment facility for treatment for polysubstance abuse (heroin and methamphetamine).
  - Mary was prescribed Buprenorphine for her Opioid Use Disorder (OUD).
  - The ED recommends that Mary be admitted to the Psychiatric Unit in the acute care hospital.

Questions: ED Discharge and Privacy

Creating and Sending Information	Questions
ED Clinicians: • Enter into **Mary's EHR in the ED/acute care hospital**: the clinical summary and information about Mary's admission and discharge from the ED. (Note: The ED and the hospital share the same EHR.) • Use **Collective Medical**/ EDIE to automatically and instantaneously send the ED admission/discharge information to Mary's care team members on the Collective network, so that Mary's care team members can have real-time visibility into this hospital/ED event and coordinate care in a timely manner. Mary's team members include primary care practitioner, MOUD prescriber, mental health counselor.	Do clinicians in the ED need Mary's consent to: (i) enter this information into Mary's EHR? (ii) use Collective Medical tools to share information about Mary's ED visit with her care team? Do any of the following privacy rules apply? • HIPAA • 42 CFR Part 2 • WA State MH privacy laws

Scenario 2:
In-patient Psychiatric Unit Admission and Discharge

- Mary is admitted to the In-patient Psychiatric Unit of the acute care hospital where the ED is also located.

- Upon admission to In-patient Psychiatric Unit, information from different data sources is gathered and Mary is assessed.

Questions: In-patient Psych Unit Admission and Privacy

Accessing Information	Questions

Upon admission, clinicians in the In-patient Psychiatric Unit use the following information sources:
• The **hospital's EHR system** to search for an electronic health record for Mary and understand Mary's history and conditions
• The **Care Everywhere** module in their EHR to search and receive Mary's clinical history across health and behavioral health providers (that use EHRs that include the Care Everywhere module).
• Assuming the IP Psych unit is on the Collective network, clinicians use the **Collective Medical** portal to:
  ○ search for whether Mary has had other ED or Inpatient stays at acute care hospitals (and prior SNF stays);
  ○ search for potential Safety and Security events, Care plans, and whether there are current care team members working with Mary (e.g., primary care, both MH and SUD, or others) and notify these community-based team members of Mary's admission to the In-patient Psychiatric Unit
	Does Mary need to provide consent for clinicians in the In-patient Psychiatric Unit to access Mary's clinical history using:
	• The Mary's hospital's EHR?
	• The Care Everywhere module?
	• Collective Medical Tools?
	
	Do any of the following privacy rules apply?
	• HIPAA
	• 42 CFR Part 2
	• WA State MH privacy laws See note above.

In-Patient Psychiatric Unit Admission, Treatment and Discharge

- Clinicians in the In-patient Psychiatric Unit compile information and develop a care plan for Mary. The care plan addresses her mental health (MH) and substance use disorder (SUD) treatment needs.
- Interventions for Mary while at the In-patient Psychiatric Unit include: individual and group counseling for both her MH condition and SUD, and medication management for her depression.
- After a two week stay in the Psychiatric Unit, Mary is discharged to an SUD Intensive Out-patient Program (IOP) that specializes in addictions and mental health conditions, including depression.
- The In-patient Psychiatric Unit creates and enters into Mary's EHR clinical summary of her admission, treatment, and discharge from the Unit.

Questions: In-Patient Psych Unit Discharge and Privacy

Creating and Sending Information	Questions

The In-patient Psychiatric Unit Clinicians use the following tools:
 	
• The **In-patient Psych Unit's EHR** to document in Mary's electronic health record information about Mary's admission to, treatment provided, and discharge from the In-patient Psychiatric Unit, including the clinical summary.
• Assuming the IP Psych unit is on the Collective network, clinicians in the IP Psyc unit, use **Collective Medical** tools:
  ○ automatically and instantaneously send the Inpatient Psychiatric unit admission/discharge/transfer (ADT) information to Mary's community-based care team members on the Collective network
  ○ share with Mary's community-based care team members information about her stay and treatment in the in-patient psych unit (e.g., a Care Insight noting Clinical, diagnostic observations and medication recommendations from Psychiatry, Safety and Security event information, and summary of essential elements of the discharge plan)
	Do clinicians in the In-patient Psychiatric Unit need Mary's consent to:
	• Enter this information into Mary's EHR in the In-Patient Psych Unit?
	• Use Collective Medical tools to share:
	  a. ADT information to community-based care team members?
	  b. Clinical information (care insights) to community-based care team members?
	
	Do any of the following privacy rules apply?
	• HIPAA
	• 42 CFR Part 2
	• WA State MH privacy laws

Scenario 3: Admission and Discharge to an SUD IOP

- Mary is discharged from the in-Patient Psychiatric Unit and admitted to an SUD Intensive Out-patient Program (IOP) that specializes in addictions and mental health conditions, including depression.

- Upon admission, to help clinicians understand Mary's clinical status and history, the IOP gathers information from different data sources.

Questions: SUD IOP Admission and Privacy

Accessing and Sending Information	Questions

Upon admission, clinicians in the SUD IOP use the following information sources:
 	
• The **SUD IOP's EHR system** is searched for an electronic health record for Mary about any prior treatment
• The **Care Everywhere module in their EHR** is used (using the Care*e*quality platform) to search and retrieve information about Mary from health and behavioral health providers that have this module in their EHRs. They retrieve the clinical summary created by the ED and the In-patient Psyc Unit regarding Mary's recent admissions.
• **Collective Medical** tools are used to:
  ○ search for whether Mary has had recent ED or acute care hospital (or SNF) visits;
  ○ identify and notify BH (both MH and SUD) providers, primary care and other care team members of Mary's admission to the IOP
  ○ Review information on Mary's patient page (on the Collective Portal) for any risk of violence (in the safety and Security event section), presence of Care Plans, and additional clinical insights.
	Does Mary need to provide consent for clinicians in the SUD IOP to access Mary's clinical history using:
	• Mary's EHR in the IOP?
	• The Care Everywhere module ?
	• Collective Medical Tools?
	
	Do any of the following privacy rules apply?
	• HIPAA
	• 42 CFR Part 2
	• WA State MH privacy laws

SUD IOP Admission, Discharge, and Treatment

- Clinicians in the IOP compile information and develop a care plan for Mary that requires:
  - MOUD for her SUD
  - individual and group counseling for her SUD
  - individual and group counseling for her SMI/depression
  - Peer Support Services for both her SUD and MH conditions

- After 90 days Mary is discharged from the SUD IOP and referred to community-based licensed MH counselors, SUD Professionals, and an MOUD prescriber.

Questions: SUD IOP Discharge and Privacy

Creating and Sending Information	Questions

• The SUD IOP Clinicians use the following tools:
  ○ **Mary's EHR at the SUD IOP** to:
  ○ document information about Mary's admission to, treatment in, and discharge from the IOP regarding her (i) SUD treatment and (ii) MH treatment; and
  ○ Create and send a discharge summary that is shared with the licensed MH counselors, SUD Professionals, and an MOUD prescriber to which Mary is being referred.
  ○ **Collective Medical** Tools to:
  ▪ automatically populate Mary's portal with the IOP care team information.
  ▪ Any additional content that the IOP enters into the Collective portal (e.g., Care plan information).
Note: All of Mary's information on the Collective Medical portal's is hidden from the rest of the care team unless/until the SUD clinic obtains consent from Mary.
	Do clinicians in the SUD IOP need Mary's consent to:
	• enter this information into Mary's EHR at the SUD IOP?
	• Send a discharge summary regarding her (i) MH treatment information and (ii) SUD treatment information to the community-based prescriber, MH and SUD professionals?
	• use Collective Medical tools to share information regarding her (i) SUD and (ii) MH treatment?
	
	Do any of the following privacy rules apply?
	• HIPAA
	• 42 CFR Part 2
	• WA State MH privacy laws

Questions?

- Slides from the bi-monthly HIT Operational Plan Update Meeting are be posted on HCA Transformation website.

https://www.hca.wa.gov/about-hca/health-information-technology/washington-state-medicaid-hit-plan

- Privacy Questions -- Contact:

  Sam Mendez
  Privacy Officer
  privacyofficer@hca.wa.gov

Bi-Monthly HIT Operational Plan Meetings

- 4th Tues. of every other month.
- Next meeting: January 25, 2022

Technology Referenced in Presentation

- **Electronic Health Record** a digital version of a patient's paper chart. EHRs are real-time, patient-centered records that make information available instantly and securely to authorized users. While an EHR does contain the medical and treatment histories of patients, an EHR system is built to go beyond standard clinical data collected in a provider's office and can be inclusive of a broader view of a patient's care. EHRs are a vital part of health IT and can:
  - Contain a patient's medical history, diagnoses, medications, treatment plans, immunization dates, allergies, radiology images, and laboratory and test results
  - Allow access to evidence-based tools that providers can use to make decisions about a patient's care
  - Automate and streamline provider workflow
- [Source: https://www.healthit.gov/faq/what-electronic-health-record-ehr]

Technology Referenced in Presentation (cont'd)

- **Care Everywhere** an HIE platform that facilitates interoperable information exchange among providers and healthcare organizations regardless of EHR system or network that user belongs to. Standards used include: industry standard transport protocols, integration profiles developed by Integrating the Healthcare Enterprise (IHE), and HL7's Clinical Document Architecture (CDA) standards. Care Everywhere is free to use for treatment and care coordination, regardless of the exchange partners technology platform. Care Everywhere is an implementer of the Carequality Framework. [Source: https://www.himss.org/resource-environmental-scan/care-everywhere]

Technology Referenced in Presentation (cont'd)

- **Car*e*quality Framework** a public-private collaborative that facilitates agreement among diverse stakeholders to develop and maintain a common interoperability framework enabling exchange between and among data sharing networks. Car*e*quality brings together a diverse group of representatives from the private sector and government to come to collective agreement on how to enable data to flow seamlessly between and among networks and providers, much like the telecommunications industry did for linking cell phone networks. It is… chartered to advance implementation of secure, interoperable nationwide health data sharing. For more information, visit www.carequality.org. [Source: https://www.healthit.gov/faq/what-carequality]

Technology Referenced in Presentation (cont'd)

- **Car*e*quality Framework** (cont'd): Car*e*quality implementation guide outlines policy, technical, and process requirements for Implementers of the Car*e*quality Query-Based Document Exchange Use Case. https://carequality.org/wp-content/uploads/2021/07/Query-Based-Document-Exchange-Implementation-Guide-v2.0-Published-07122021-1.pdf The Car*e*quality implementation guide outlines requirements related to release of information and patient consent/authorization to share. Car*e*quality Interoperability Framework Adopters include several HIT vendors. Generally, Car*e*quality Implementation Guide specifies patient permission is required as defined by HIPAA. In addition, entities requesting information from facilities covered under 42 CFR part 2 must prevent the unauthorized disclosure of any such information and must also be able to parse and interpret information contained in document metadata.

Technology Referenced in Presentation (cont'd)

- **Collective Medical** is a HIT vendor that helps care teams collaborate to support their most vulnerable patients — those whose needs cannot be met in any single care setting. Collective unifies a patient's entire care team — including hospitals, primary and specialty care, post-acute care, behavioral health providers, community service organizations, and health plans — offering real-time patient insights that power better decision-making for improved patient outcomes. Collective empowers caregivers to impact care outside their walls, by providing real-time data that tells them: Where their patient is, Why they are being seen, Who else is treating them, What are the avoidable risks. [Source: https://collectivemedical.com/purpose/]