

**Why do I have to Worry About  
42 C.F.R. Part 2 ?**

Boston HCCA Regional Compliance Conference  
September 7, 2018

**Confidentiality of Substance Use Disorder Patient  
Records**

<p>Lisa Adragna <i>Clinical Integration Program Director Partners Healthcare</i></p> <p>Christine Griffin, JD, HIM <i>Director and Privacy Officer Massachusetts General Hospital</i></p>	<p>Hannah Baldwin, JD, CHC, CHPC <i>Compliance &amp; Privacy Manager Elliot Health System</i></p> <p>Travis Smith, JD, MPH <i>Head of Policy &amp; General Counsel Collective Medical Technologies</i></p>
---	--

---

---

---


---

---

---

---

---



**Agenda**

- Regulatory Requirements and Updates
- Program Applicability
- Sharing Health Information
  - Provider's Perspective
  - Statewide Care Collaboration Network Perspective

---

---

---


---

---

---

---

---



**Elliot and 42 C.F.R. Part 2**

**Our Story**

- New Hampshire has the 2<sup>nd</sup> highest opioid-related overdose deaths in the country.
- New Hampshire is one of the states that spends the least amount of funds on treatment per patient.
- Manchester, NH:
  - Estimated population for 2018 is 111,196 individuals
  - 2009 the first year substance use appeared in the Manchester Community Needs Assessment
  - Since 2015 Elliot has seen a 118% increase in Substance Use Disorder (SUD) visits to the emergency department.

---

---

---

---

---

---

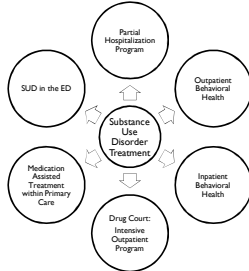
---

---

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

### Our Goals

- Unhindered access to care and medications.
- Increased collaboration and support.
- Compliance with applicable privacy rules.



---

---

---

---

---

---

---

---

## What is 42 C.F.R. Part 2

### Regulatory Basis

- 42 U.S.C. 290dd-2; 42 C.F.R. Part 2
- Stricter protections for privacy
  - Protect patients from additional vulnerability due to availability of medical record and stigma.
- Separate from HIPAA and HITECH
- **What Information is Protected?**
  - Any information identifies a patient as having or had a SUD and is information obtained or maintained by a Part 2 Program.
- **Who has to protect this Information?**
  - Part 2 Programs
  - Lawful Holders
  - Third Party Payers
  - Entities with direct administrative control over a Part 2 Program

---

---

---

---

---

---

---

---

## What is 42 C.F.R. Part 2

### • **What is a Part 2 Program?**

- There are two elements:
  - 1. Federally assisted program and
  - 2. a "Program"

### • **Federally Assisted Program:**

- A program contracted or directly controlled by a federal department or agency.
- Requires a federal license, certification, registration or authorization.
- Supported by federal funds, even if the funds do not directly pay for SUD treatment, diagnosis, or referral
- A program that is granted tax exempt status or allowed tax deductions for contributions by the IRS.

---

---

---

---

---

---

---

---

**What is 42 C.F.R. Part 2**

**What is a “Program”**

1. Individual/Entity (not a general medical facility) **holds self out** as providing AND provides SUD diagnosis, treatment or referral for treatment services.
2. An identified unit within a general medical facility that **holds self out** as providing AND provides SUD diagnosis, treatment or referral for treatment services.
3. Medical personnel or other staff in a general medical facility that has the primary function of providing SUD diagnosis, treatment or referral for treatment services.

---

---

---

---

---

---

---

---

**What is 42 C.F.R. Part 2**

**When do Restrictions Not Apply?**

- This is different from “exceptions” to the consent requirements.
- There are specific times when the restrictions on use and disclosure do not apply:
  - Communications between or among personnel of a Part 2 Program.
  - Communications between a Part 2 Program and entity with direct administrative control.
  - Qualified Service Organizations (QSO).
  - Crimes committed on premises.
  - Reports of suspected child abuse and neglect.

---

---

---

---

---

---

---

---

**What is 42 C.F.R. Part 2**

**Consent**

- **General Rule:** A written consent is required unless an exception applies.
- **Consent Requirements:**
  - Patient name
  - Purpose of disclosure
  - Patient’s right to revoke
  - Condition for expiration of consent
  - Patient’s signature and date
  - **Amount and Kind**
    - Requires specificity
  - **Specific name or general designation of program or person permitted to make the disclosure**
  - **Name or title of the individual or name of the organization that disclosure is being made to**
    - “To Whom”

---

---

---


---

---

---

---

---



**What is 42 C.F.R. Part 2**

**Exceptions to Consent Requirement**  
(i.e. disclosures w/o consent):

- Medical Emergencies
  - May disclose to the extent necessary to meet a bona fide medical emergency for which patient consent cannot be obtained.
  - Must document disclosure in the patient's record.
- Research
- Audit and Evaluation
  - Records not copied or removed
  - Copying and/or removal of records

---

---

---

---

---


---

---

---

---

---



**42 C.F.R. Part 2 – The Future**

**Proposed Bills**

- Federal Government has two proposed bills:
  - 1 from the House: H.R. 6082 passed the house June 20<sup>th</sup> 357-57
  - 1 from the Senate: S/ 1850
- H.R. 6082 Overdose Prevention & Patient Safety Act
  - Received in Senate June 21, 2018
  - Senate referred bill to the Committee on Health, Education, Labor, and Pensions
  - Content:
    - Permitted disclosure includes: treatment, payment, and healthcare operations. i.e. more aligned with HIPAA disclosure rules.
    - Breach notification aligned with HIPAA and HITECH
- S. 1850 Protecting Jessica Grubb's Legacy Act
  - Read by the Senate and referred to the Committee on Health, Education, Labor, and Pensions September 25, 2017
  - Content:
    - Permitted disclosure includes: treatment, payment, and healthcare operations. i.e. more aligned with HIPAA disclosure rules.

**State Law**

- Is it equal or more restrictive than federal law?
- New Hampshire RSA 330-C

---

---

---

---

---


---

---

---

---

---



**Patient Confidentiality Governance**

---

---

---

---

---

---

---

---

---

---

## Partners Healthcare Governance Structure

**Enterprise workgroup was created with representation from:**

- Office of the General Council
- Compliance
- Information Security
- Medical Records and Health Information Management
- PCPs, Mental Health Clinicians, Emergency Services
- Key EHR Subject Matter Experts

**Workgroup Goals and Objectives**

- To design enterprise standards to support the Epic build and where applicable, support streamlined workflows and provide appropriate privacy and security protocols
- To understand the Epic functionality and determine the best implementation method to achieve compliance with state and federal laws
- Understand dependencies on the clinical content decisions and build, and the impact to provider and staff workflows
- Workgroup recommendations will be presented to Partners eCare Clinical Council and Clinical Steering Committee for approval and to various eCare Governance councils (i.e. HIS, Patient Access) as needed

**42 CFR Decision Approach**

- Review of State and Federal requirements
- Current state review by site to understand what sites were doing to accommodate regulation
- Reviewed future state options

13

---

---

---

---

---

---

---

---

---

---

## Patient Confidentiality Levels

---

---

---

---

---

---

---

---

---

---

## Epic Confidentiality Levels

Level	Data Types	Epic Tool
Patient Level Information (Demographic and Clinical)	<ul style="list-style-type: none"> <li>• Name</li> <li>• DOB</li> <li>• Address</li> <li>• Allergies</li> <li>• Medications</li> <li>• Problems</li> <li>• Histories</li> <li>• Immunizations</li> <li>• Imaging</li> </ul>	<ul style="list-style-type: none"> <li>• Confidential Patient</li> <li>• Confidential Address</li> <li>• Patient Safety Flag (Partial)</li> <li>• Employee</li> <li>• VIP/V-VIP FYI flags for patients identified by entity leadership</li> <li>• 42 CFR Encounter</li> </ul>
Encounter Level Information	<ul style="list-style-type: none"> <li>• Encounter</li> <li>• Notes</li> </ul>	<ul style="list-style-type: none"> <li>• Private Encounter</li> <li>• Confidential Guarantor</li> <li>• Patient Safety Flag (Partial)</li> <li>• Break the Glass- Appropriate (Soft Stop Warning)</li> <li>• Break the Glass- Inappropriate (Removes encounter)</li> <li>• Sensitive Notes</li> </ul>
Order Level Information	<ul style="list-style-type: none"> <li>• Lab Orders</li> <li>• Lab Results</li> </ul>	<ul style="list-style-type: none"> <li>• Sensitive Orders</li> </ul>

15

---

---

---

---

---

---

---

---

---

---

## Clinical Chart Restrictions

---

---

---

---

---

---

---

---

## Overview of 42CFR Protections

- 42CFR encounters will only be viewable by 42CFR staff, other mental health providers, and ED clinicians
- All 42CFR departments will be removed from the login/change context department list, only users with their site's 42CFR sub-template will be able to log into that site's 42CFR departments
- Cadence schedules will be restricted so that users outside of the 42CFR department do not have access
- All users, except those with a 42CFR sub-template, will receive patient level break the glass on patients that have a 42CFR encounter. HIM and billing are also exempt

---

---

---

---

---

---

---

---

### Current State - 42 CFR Encounter Access

User	McLean 42 CFR Departments	MGH 42 CFR Departments	BWF 42 CFR Departments	NWH 42 CFR Departments
McLean 42 CFR Users (logged into a McLean 42 CFR dept.)	Full Access	Restricted	Restricted	Restricted
McLean Users (logged into any McLean dept.)	Soft Stop Break the Glass	Restricted	Restricted	Restricted
MGH 42 CFR Users (logged into an MGH 42 CFR dept.)	Restricted	Full Access	Restricted	Restricted
BWF 42 CFR Users (logged into a BWF 42 CFR dept.)	Restricted	Restricted	Full Access	Restricted
NWH 42 CFR Users (logged into an NWH 42 CFR dept.)	Restricted	Restricted	Restricted	Full Access
Mental Health Clinicians (with mental health security templates)	Soft Stop Break the Glass	Soft Stop Break the Glass	Soft Stop Break the Glass	Soft Stop Break the Glass
ED Clinicians (with ED security templates)	Soft Stop Break the Glass	Soft Stop Break the Glass	Soft Stop Break the Glass	Soft Stop Break the Glass
PCPs and other clinicians	Restricted	Restricted	Restricted	Restricted

NOTE: 42 CFR users must have the sites 42 CFR sub-template to log in

---

---

---

---

---

---

---

---

## 42 CFR Final Rule – Announced on 1/13/17

### In Summary.....

Now allows for the disclosure of patient information with a consent from a Part 2 program to an intermediary such as an HIE, which may then disclose to its participants that have a treating provider relationship with the patient.

- Treating provider name no longer needs to be specified
- However, the HIE must track and provide listing of disclosures to Patient upon request (disclosures for past 2 years)

### Other Highlights:

- To Whom (past/present/future treating providers w/o spec identifying them)
- From Whom – allows also for a general designation on consent
- Re-disclosure Prohibition – data that directly or indirectly identifies the pt.
- Medical Emergencies – clarified language to allow for disclosure
- Research – aligns much of the requirements with HIPAA and Common Rule
- Patient Identifying Information – will need to assess the data in context of the Part 2 program
- Qualified Service Organization – CM requires consent; expanded uses to include PHM
- Other Consent Provisions – may extend for a period of time or until the expiration of an event. (Patient death)
- What was Not Included – does not align permitted disclosures with HIPAA

19

---

---

---

---

---

---

---

---

---

---

## 42 CFR - Pilot based on Final Rule

### What's changing?

- Currently, Epic users, who work outside of 42 CFR Practices cannot see these encounters, except mental health and emergency department clinicians
- Starting 4/20/2018, users will see patient encounters at these practices for any patient who consents

### Who does this change impact and what do I need to know?

- PCPs and Non-ED/Non-Mental Health Clinicians

### What you will see:

- 42 CFR encounters. You will need to break the glass for access

### What you won't see:

- You will not see encounters from before the patient consented.

### What you need to know:

- Disclosure of 42 CFR Part 2 information is prohibited unless required by law or a patient care emergency
- Never copy and paste the information into your notes, letters or documentation
- Never release or share (verbally, paper or otherwise) unless you have proper patient written authorization. Contact Privacy Office with questions.
- If you don't need the information in paper form, don't print it.

### For ED and Mental Health Clinicians:

- No change. All 42 CFR encounters will remain available to you as it is currently. You will continue to need to break the glass for access

20

---

---

---

---

---

---

---

---

---

---

## Future 42 CFR-Encounter Access with Consent

User	MGH Unprotected 42 CFR Departments (Patient Consent)	42 CFR Departments Protected (No Patient Consent)
PCPs, Specialists and other clinicians	Soft Stop Break the Glass	No Access
All Users	Soft Stop Break the Glass	No Access
McLean 42 CFR Users	Soft Stop Break the Glass	No Access
BWF 42 CFR Users	Soft Stop Break the Glass	No Access
NWH 42 CFR Users	Soft Stop Break the Glass	No Access
Mental Health Clinicians (with mental health security templates)	Soft Stop Break the Glass	Soft Stop Break the Glass
ED Clinicians (with ED security templates)	Soft Stop Break the Glass	Soft Stop Break the Glass

---

---

---

---

---

---

---

---

---

---

# Making Sensitive Information Compliance Work in a Statewide Care Collaboration Network

---

---

---

---

---

---

---

---

## About the Collective Network

**National Technology Platform & Governance Framework**

- Applications**  
(e.g., Features, Standard/Configurable Functionality, EMR Integrations)
- Policies & Procedures**  
(e.g., Data Use, Network Access, Sensitive Information, Patient Consent & Opt-Out)
- Governance & Compliance Administration**  
(e.g., Process, Personnel, Tools, Terms of Use, Subscriber Contracts)
- Technology Infrastructure & Controls**  
(e.g., MPI, Interfaces, Data Filters, User Permissions, Audit Trail)

---

---

---

---

---

---

---

---

## Tools for Cross-Continuum Care Collaboration

**Real-Time Notifications ("Supercharged ENS")**

**Shared Care Planning**

**Dashboards & Reporting**

---

---

---

---

---

---

---

---





## Data Flow Drill-Down for Sensitive Information Compliance

1. How is information shared with (i.e., **sent to**) the Collective Platform?
  - Automated data integrations (Example: EMR ADT feed)
  - Patient Eligibility Files (Example: csv file with patient demographics, care management info)
  - Manual inputs via PreManage or ED ie web portal (e.g., care plans, security events)
2. How is information accessed through (i.e., **received from**) the Collective Platform?
  - Enables provider to share SI throughout CMT Network
  - Pursuant to CMT NH Sensitive Information Policy
3. What controls can we use in both the information sending + receiving process to meet compliance requirements?
  - **Administrative controls** (contractual requirements, policies + documentation, limit number of users access, role-based permission for users, user training)
  - **Technical controls** (narrow data inputs, data feed filtering, data processing + mapping patient + data tagging to apply SI rules in application [e.g., redisclosure notice], masking providers as data sources)

**Bottom line: focus on specific use cases enables drill-down to identify specific ways to implement controls (administrative or technical) to address compliance needs.**

---

---

---

---

---

---

---

---

---

---

---

---

## NEW: Support for Sensitive Information Consent w/ CMT Special Consent Form\*

- CMT is responsible for:
  - Providing Special Consent Form
    - SI/D information (Part 2)
      - Mental health information (inpatient, outpatient, voluntary, involuntary)
      - HIV/AIDS and STD information
  - Providing Special Consent Policy + Implementation Instructions + Training Materials
  - Managing technical controls:
    - redisclosure notice
    - tracing provider relationship
    - track audit trail
    - provide electronic summary of Special Consent Form
  - 3rd Party Legal Analysis approving Special Consent Form and Policy
- Provider is responsible for:
  - Managing workflow to obtain patient consent using Special Consent Form
  - Indicating patient consent status in Eligibility File

**SI/D SPECIAL CONSENT POLICY**  
Approved 10/20/15  
 Collective Medical Technologies, Inc.

**Objective**  
 This policy describes the terms and requirements for CMT Subscribers who wish to use the Special Consent Form to share Sensitive Information (SI/D) with the CMT Network.

**Policy**

**1. General**

**1.1. Purpose**  
 The purpose of this policy is to define the requirements for CMT Subscribers who wish to use the Special Consent Form to share Sensitive Information (SI/D) with the CMT Network.

**1.2. Scope**  
 This policy applies to all CMT Subscribers who wish to use the Special Consent Form to share Sensitive Information (SI/D) with the CMT Network.

**1.3. Definitions**  
 Sensitive Information (SI/D): Information that is protected by state or federal laws, regulations, or contracts, and is not intended for public release. This includes, but is not limited to, mental health information, HIV/AIDS information, and STD information.

**1.4. Objectives**  
 The objectives of this policy are to ensure that CMT Subscribers who wish to use the Special Consent Form to share Sensitive Information (SI/D) with the CMT Network are provided with the necessary information and resources to do so.

**1.5. Responsibilities**  
 CMT: Provide the Special Consent Form and Policy to CMT Subscribers who wish to use the Special Consent Form to share Sensitive Information (SI/D) with the CMT Network.  
 CMT Subscribers: Provide the necessary information and resources to use the Special Consent Form to share Sensitive Information (SI/D) with the CMT Network.

**1.6. Compliance**  
 CMT Subscribers who wish to use the Special Consent Form to share Sensitive Information (SI/D) with the CMT Network must comply with the terms and conditions of the Special Consent Form and Policy.

**1.7. Enforcement**  
 CMT reserves the right to enforce the terms and conditions of the Special Consent Form and Policy.

**1.8. Revision**  
 This policy may be revised from time to time without notice.

**1.9. Contact**  
 For more information, please contact the CMT Compliance Department.

**1.10. Approval**  
 Approved by the CMT Board of Directors on 10/20/15.

\*Also supporting limited "DIY" consent process in New Hampshire

---

---

---

---

---

---

---

---

---

---

---

---

## Compliance Result from Sender & Receiver Perspectives

1. As a **sender** of information, you have comfort because:
  - You are only sending information to the minimum extent necessary for the use case
  - You can filter out Sensitive Information (i.e., that can't be shared without patient consent)
  - If you make an mistake and send SI in a data integration, much lower risk that it is processed/mapped and shared
  - You have a limited number of users with ability to manually share information
  - You have a few, simple rules users can remember when they manually share information to void SI mistakes
  - If you want, you can enable expanded sharing of information through a carefully focused SI patient consent
2. As a **receiver** of information, you have comfort because:
  - You know that most Sensitive Information will be excluded from the Collective Platform (because of the SI controls on sharing information) or is only available to you because a patient has signed a valid SI consent
  - You know that you will only have access to information that is appropriate / permissible for you see
  - If you do see Sensitive Information subject to a redisclosure prohibition, you receive a redisclosure notice so that you know what not to do

---

---

---

---

---

---

---

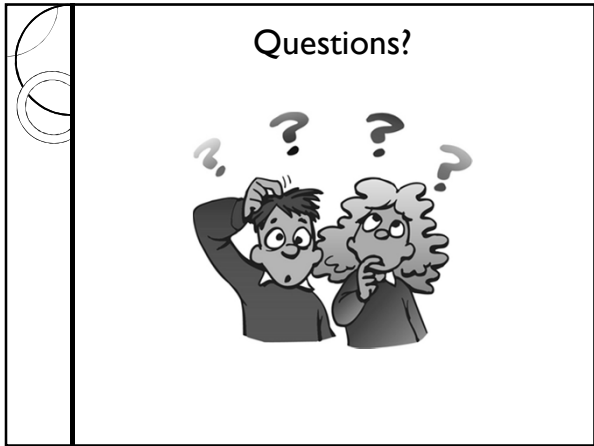
---

---

---

---

---



---

---

---

---

---

---

---

---