HHIAG Special Presentation

Data Transfer and Use:

Navigating Federal and State Laws and Regulations

The Office of the National Coordinator for Health Information Technology

HIPAA Privacy Framework

HIV Health Improvement Affinity Group
Data Transfer and Use: Navigating Federal and State Laws and Regulations
March 28, 2017

Peyton Isaac, BSN, JD, Senior Privacy Analyst

Agenda

- Health Insurance Portability and Accountability Act (HIPAA) Permitted and Required Uses and Disclosures of Protected Health Information (PHI)
- HIPAA De-mystified
- The Role of State Law
- Data Aggregation
  - » Public Health Reporting
  - » Health Oversight
- Resources

The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule

- **Applies** to "Covered Entities (CE)"
  - » Health plans including employer and self-insured plans, and Medicaid agencies
  - » Health care clearinghouses
  - » Health care providers conducting covered electronic transactions
  - » Business associates of the above

The HIPAA Privacy Rule Framework cont. . .

- **Permits** exchange of protected health information without patient authorization
  - » "Permitted Uses and Disclosures" includes Treatment , Payment, Health Care Operations (HCO)
  - » Permissive disclosures are at the discretion of the covered entity
  - » Business Associates (e.g., HIEs) may undertake the disclosure function on behalf of covered entities when delegated by the CE in the Business Associate Agreement (BAA)

The HIPAA Privacy Rule Framework cont. . .

- **Supports** exchange when required by federal, state or local law
  - » Public health activities (e.g., infectious disease reporting)
  - » Health oversight agencies or other purposes

HIPAA De-Mystified

- HIPAA does not preempt state laws that are more privacy protective than HIPAA
- HIPAA does not prohibit use and disclosure of mental and behavioral health data, including HIV or other specific clinical categories
  - » Psychotherapy notes and correctional medical records are the exception
  - » Disclosable data includes labs, prescriptions, appointments, and procedures
  - » There is a restriction in federal law for sharing Veteran HIV PHI

HIPAA De-Mystified cont . . .

- The "Minimum Necessary" standard applies to sharing health care operations (HCO) data
- Minimum Necessary rule does not apply to treatment data under HIPAA
- HIPAA requires that patients or their representatives be allowed to access their own data
  - » Includes transmitting a copy to a third party, including an app

The Role of State Law

- State Laws (and/or organizational policies) may impose additional rules for health information disclosure
  - » May restrict disclosure of certain sensitive categories of information with patient consent, e.g., HIV
  - » May restrict the types of information held by state/local governments
  - » May enable broad collection (state registry) , but not dissemination, of health information

The Role of State Law cont . . .

- State laws may apply when HIPAA does not apply
  - » E.g., when non-covered entities (e.g., housing authorities) are using or disclosing PHI health information
- State laws may require the use and/or disclosure of PHI for certain purposes
  - » Public health surveillance or reporting
  - » Health oversight
  - » Law enforcement under certain conditions

Data Aggregation Definition

- 45 CFR 164.501 – *Data aggregation* means, with respect to ***protected health information created or received by a business associate in its capacity as the business associate of a covered entity***, the combining of such protected health information by the business associate with the protected health information received by the business associate in its capacity as a business associate of another covered entity, ***to permit data analyses that relate to the health care operations*** of the respective covered entities.

Key Health Care Operations

Health Care Operations (HCO) (1, 2, 4)
45 CFR 164.501 Excerpt of HCO

*care planning

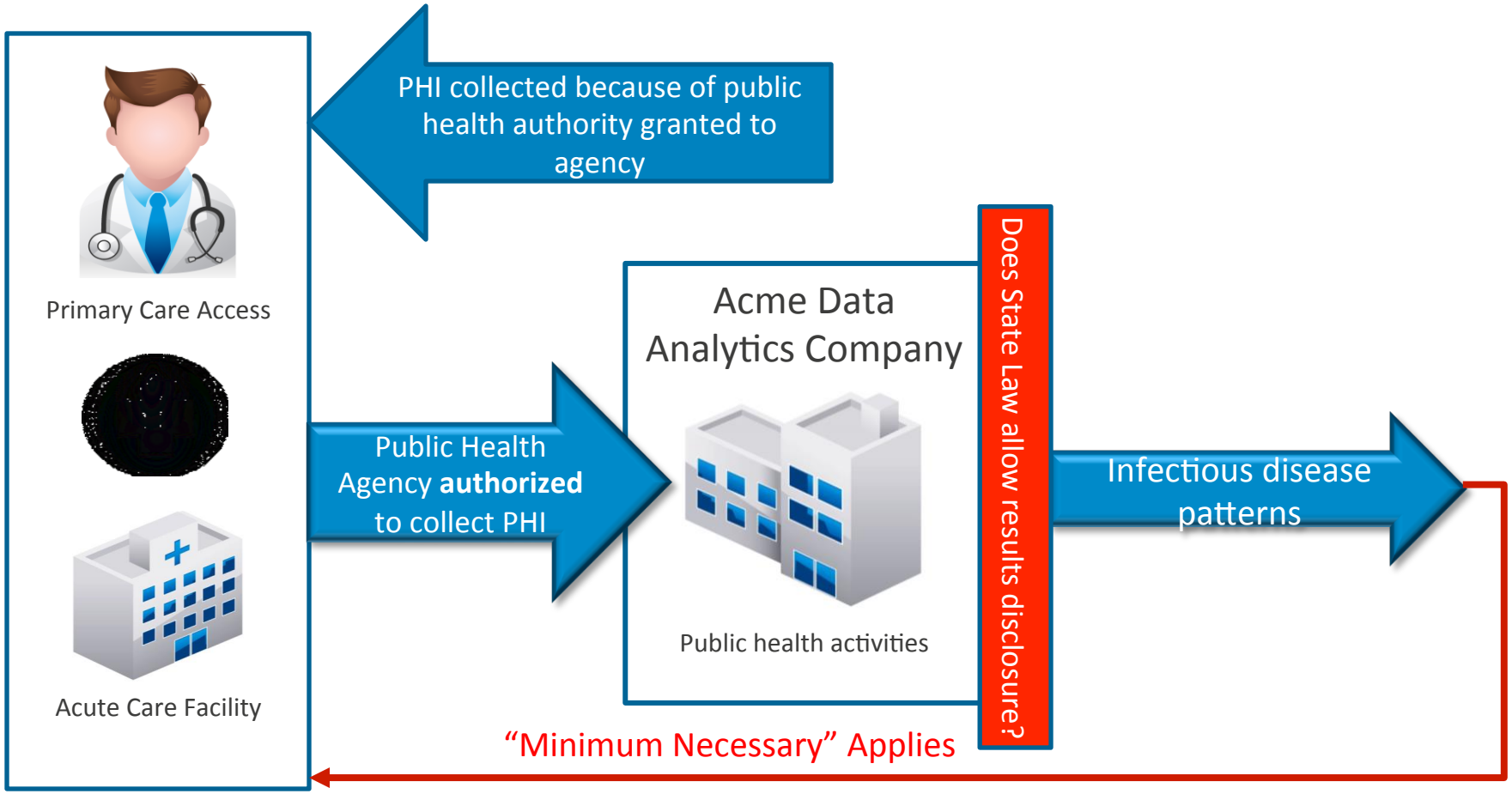
Health care operations means any of the following activities of the covered entity to the extent that the activities are related to covered functions:

(1) **Conducting quality assessment and improvement activities**, including outcomes evaluation and development of **clinical guidelines**, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; patient safety activities (as defined in42 CFR 3.20); **population-based activities** relating to improving health or reducing health care costs, **protocol development, case management and care coordination**, contacting of health care providers and patients with information about **treatment alternatives**; and related functions that do not include treatment;

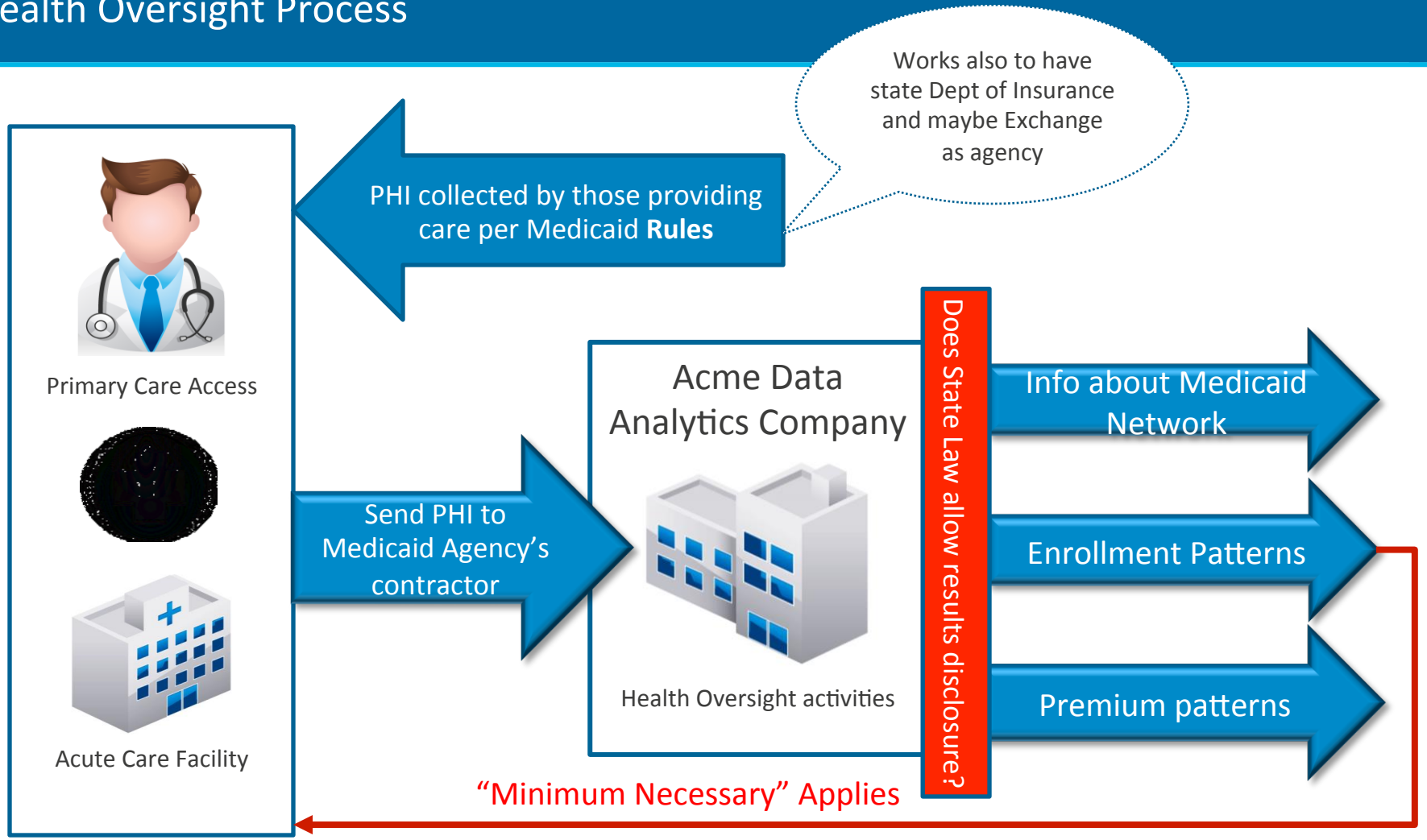
(2) Reviewing the competence or **qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance,** conducting **training** programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or **credentialing activities**;

(4) Conducting or arranging for medical review, legal services, and auditing functions, including **fraud and abuse detection and compliance programs;**

Public Health Activity Process



Health Oversight Process

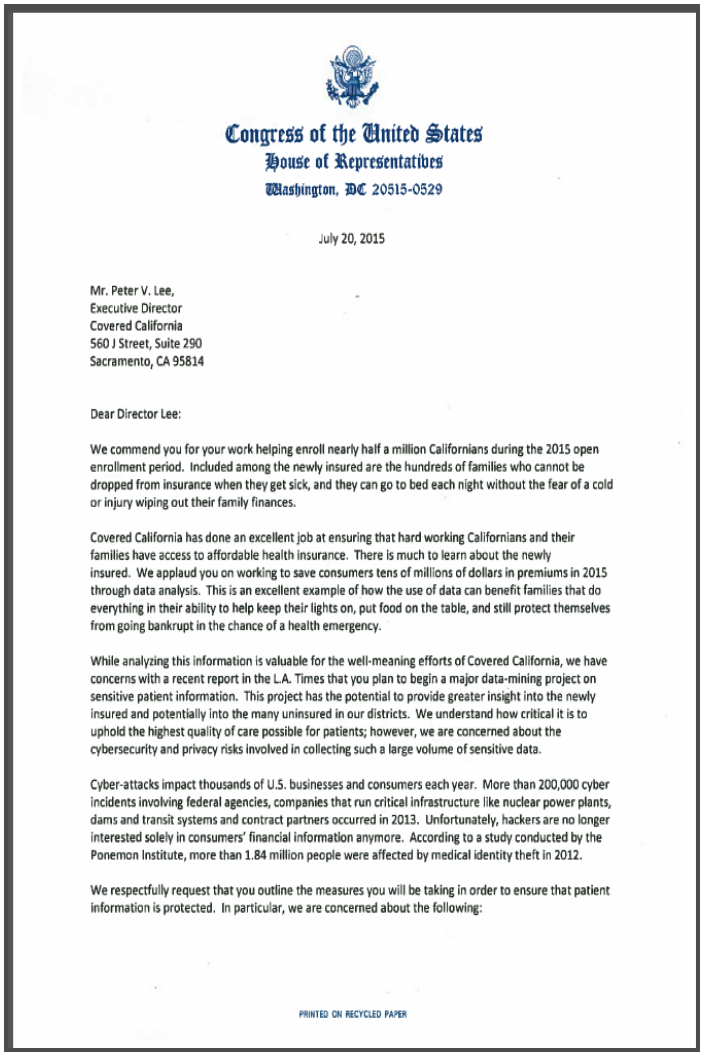


Lawful Methods of Aggregating

Method	Sharing is	Summary	Aggregated results or combined PHI can be disclosed
Voluntary Covered Entity Data Aggregation	Permitted	2 or more CEs hire a single BA, combine their PHI with the BA for a health care operation involving data of patients the CEs have in common	Authorized by a BAA and specified by participation contracts and HIPAA rules
Health Oversight	Permitted	A Health Oversight agency collects data from CEs, and, using an analytics process the Health Oversight agency manages, uses the data for the agency's purposes	Specified by law that applies to data held by health oversight agency
Public Health Activities	Permitted	Id. Except the activities are for Public Health as defined by state law	Specified by law that applies to data held by public health agency

Using Data Aggregation for Quality Measurement

Congressional Letter to Covered California CEO



Congress of the United States
House of Representatives
Washington, DC 20515-0529

July 20, 2015

Mr. Peter V. Lee,
Executive Director
Covered California
560 J Street, Suite 290
Sacramento, CA 95814

Dear Director Lee:

We commend you for your work helping enroll nearly half a million Californians during the 2015 open enrollment period. Included among the newly insured are the hundreds of families who cannot be dropped from insurance when they get sick, and they can go to bed each night without the fear of a cold or injury wiping out their family finances.

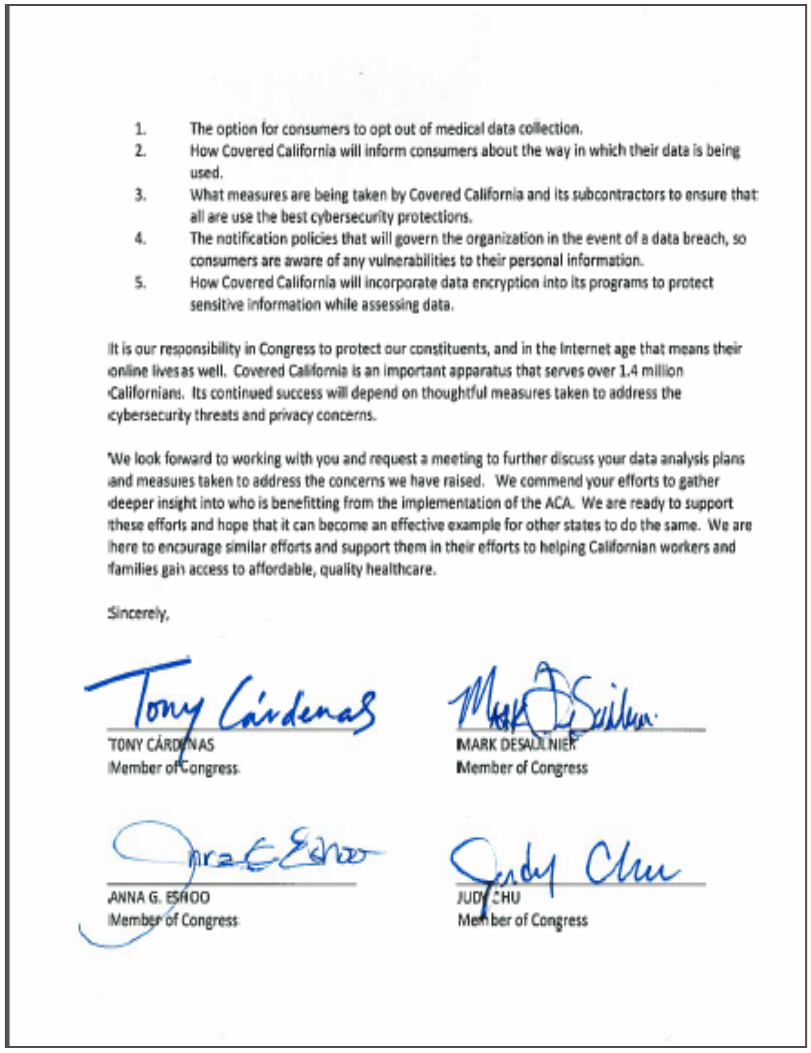
Covered California has done an excellent job at ensuring that hard working Californians and their families have access to affordable health insurance. There is much to learn about the newly insured. We applaud you on working to save consumers tens of millions of dollars in premiums in 2015 through data analysis. This is an excellent example of how the use of data can benefit families that do everything in their ability to help keep their lights on, put food on the table, and still protect themselves from going bankrupt in the chance of a health emergency.

While analyzing this information is valuable for the well-meaning efforts of Covered California, we have concerns with a recent report in the L.A. Times that you plan to begin a major data-mining project on sensitive patient information. This project has the potential to provide greater insight into the newly insured and potentially into the many uninsured in our districts. We understand how critical it is to uphold the highest quality of care possible for patients; however, we are concerned about the cybersecurity and privacy risks involved in collecting such a large volume of sensitive data.

Cyber-attacks impact thousands of U.S. businesses and consumers each year. More than 200,000 cyber incidents involving federal agencies, companies that run critical infrastructure like nuclear power plants, dams and transit systems and contract partners occurred in 2013. Unfortunately, hackers are no longer interested solely in consumers' financial information anymore. According to a study conducted by the Ponemon Institute, more than 1.84 million people were affected by medical identity theft in 2012.

We respectfully request that you outline the measures you will be taking in order to ensure that patient information is protected. In particular, we are concerned about the following:

PRINTED ON RECYCLED PAPER



1. The option for consumers to opt out of medical data collection.
2. How Covered California will inform consumers about the way in which their data is being used.
3. What measures are being taken by Covered California and its subcontractors to ensure that all are use the best cybersecurity protections.
4. The notification policies that will govern the organization in the event of a data breach, so consumers are aware of any vulnerabilities to their personal information.
5. How Covered California will incorporate data encryption into its programs to protect sensitive information while assessing data.

It is our responsibility in Congress to protect our constituents, and in the Internet age that means their online lives as well. Covered California is an important apparatus that serves over 1.4 million Californians. Its continued success will depend on thoughtful measures taken to address the cybersecurity threats and privacy concerns.

We look forward to working with you and request a meeting to further discuss your data analysis plans and measures taken to address the concerns we have raised. We commend your efforts to gather deeper insight into who is benefitting from the implementation of the ACA. We are ready to support these efforts and hope that it can become an effective example for other states to do the same. We are here to encourage similar efforts and support them in their efforts to helping Californian workers and families gain access to affordable, quality healthcare.

Sincerely,

Tony Cárdenas
TONY CÁRDENAS
Member of Congress

MARK DESAULNIER
Member of Congress

ANNA G. ESHOO
Member of Congress

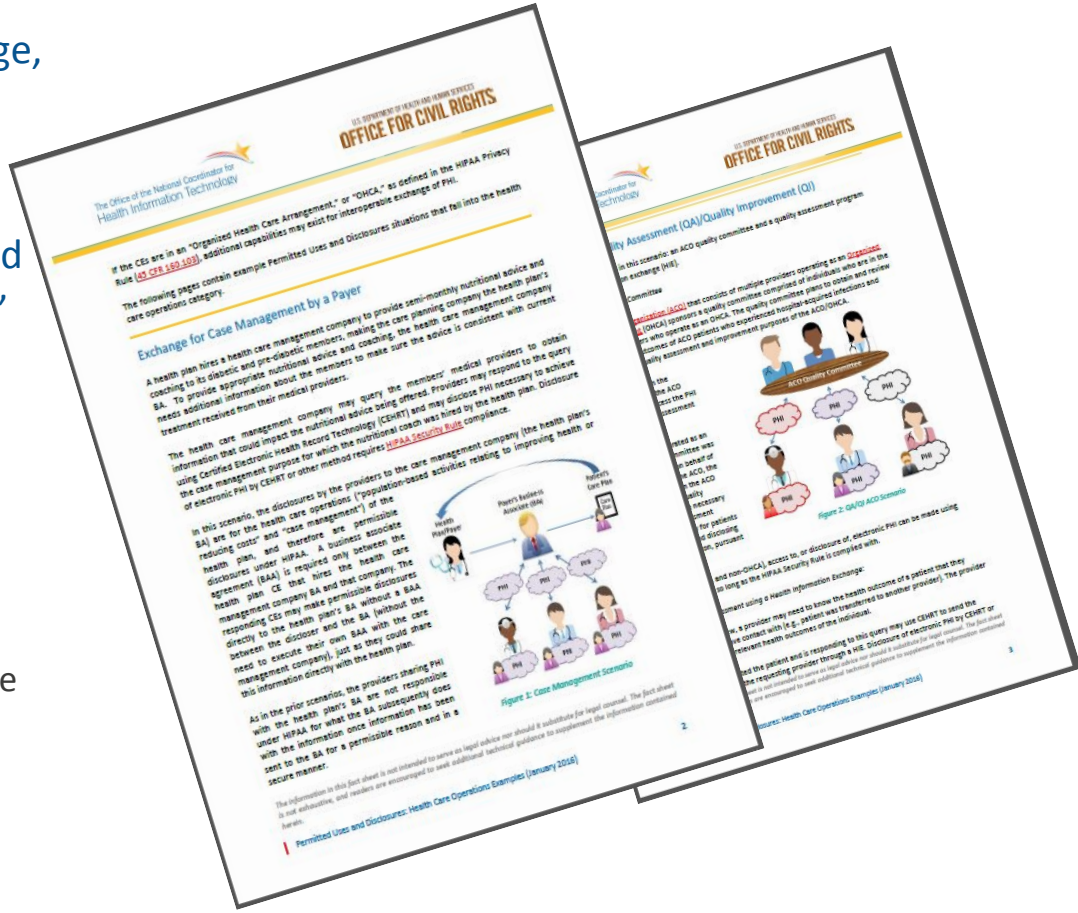
JUDY CHU
Member of Congress

NOT Examples of Data Aggregation

- Combining data that is de-identified to a HIPAA standard
- Conducting research using either:
  - » A limited data set as defined by HIPAA; or
  - » Protected Health Information (PHI) because patients have consented or an Institutional Review Board (IRB) has waived consent

The Real HIPAA Supports Interoperability| HealthIT.Gov Fact Sheets and Blog Series

- OCPO/OCR co-branded educational fact sheets that provide practical, plain language, examples with illustrations to supplement the blog series.
- OCPO launched a 4-part blog series entitled the "Real HIPAA Supports Interoperability" on February 4
  - » Blog 1: The Real HIPAA Supports Interoperability
  - » Blog 2: Background on HIPAA's PU&D
  - » Blog 3: Examples of Care Coordination, Care Planning, Case Management
  - » Blog 4: Examples of Quality Assurance and Population-Based Activities



- **Hot off the press:** Public Health Activities and Health Oversight Fact Sheets

https://www.healthit.gov/sites/default/files/12072016_hipaa_and_public_health_fact_sheet.pdf

https://www.healthit.gov/sites/default/files/phi_permitted_uses_and_disclosures_fact_sheet_012017.pdf

QUESTIONS

Peyton S. Isaac, BSN, JD

Senior Policy Analyst

Peyton.isaac@hhs.gov

202.690.3910

Public Health Data Use and Release: HIV Health Improvement Affinity Group webinar

Matthew Penn, JD, MLIS

Rachel Hulkower

Maggie Power

Public Health Law Program

Office for State, Tribal, Local and Territorial Support

March 28, 2017

Disclaimer

The contents of this presentation do not represent official CDC determinations or policies.

The findings and conclusions in this report are those of the authors and do not necessarily represent the official position of CDC.

The contents are for educational purposes only and are not intended as a substitute for professional legal advice.

Always seek the advice of an attorney or other qualified professional with any questions you may have regarding a legal matter.

Use and Release of PII

- "~~Sharing~~"
- "Use" and "Release"
  - States laws govern "use" and "release" (aka "disclosure" in some laws) of PII held by the health department
    - Not "sharing" – the term is too vague.
      - Sharing within the agency or outside the agency?

"Use" of PII

- General use
  - Health departments use PII for a range of public health purposes without patient consent AND
  - The PII does not leave the agency that holds the information.
- Disease-specific use
  - Health departments use PII pertaining to a specific disease or group of diseases (e.g., STDs) for a range of public health purposes without patient consent
- A 'use provision' of a law may indicate if and how the health department can use PII

Example “General Use” Provision

“When the Director has knowledge, or is informed of the existence of a suspected case or outbreak of a communicable disease:

A. The Director shall take whatever steps necessary for the investigation and control of the disease.

B. If the Director finds that the nature of the disease and the circumstances of the case or outbreak warrant such action, the Director shall make, or cause to be made, an examination of the patient in order to verify the diagnosis, make an investigation to determine the source of the infection, and take appropriate steps to prevent or control spread of the disease.”

ARK. ADMIN. CODE 007.15.2–VII.

Example "Specific Use" Provision

"Protocol for management of infectious forms of tuberculosis.

A. When a physician or other person knows that a person has an infectious form of tuberculosis, the physician or other person shall promptly notify the department.

B. Upon receiving notification that a person has an infectious form of tuberculosis, the department shall prescribe the person a treatment plan meeting the department's therapeutic specifications for the infectious form of tuberculosis…."

N.M. STAT. ANN. § 24-1-15.1 (West 2009).

“Release” PII

- General release
  - For purposes health departments may release PII, without patient consent, to entities outside of the department that holds the PII
- Disease-specific release
  - For specific purposes health departments may release PII pertaining to a specific disease or group of diseases (e.g., STDs), without patient consent, to entities outside of the department that holds the PII
- A ‘release provision’ of a law may indicate when and to what entity and for what purpose a health department can release PII

Example "General Release" Provision

"Health care information in the possession of the department, a local board, a local health officer, or the entity's authorized representatives may not be released except: …

(5) to another state or local public health agency, including those in other states, whenever necessary to continue health services to the named person or to undertake public health efforts to prevent or interrupt the transmission of a communicable disease or to alleviate and prevent injury caused by the release of biological, chemical, or radiological agents capable of causing imminent disability, death, or infection…."

MONT. CODE ANN. § 50-16-603.

Example "Specific Release" Provision

"Confidentiality and disclosure.

No person who obtains confidential HIV related information in the course of providing any health or social service … may disclose or be compelled to disclose such information, except to the following: …

A health care provider or health facility when knowledge of the HIV related information is necessary to provide appropriate care or treatment to the protected individual, a child of the individual, a contact of the protected individual or a person authorized to consent to health care for such a contact; …"

N.Y. PUB. HEALTH LAW § 2782.

Decision Making Framework

Data Collection

- **Who is collecting the data?**
  - Public health agency employees or representatives?
  - Employees or representatives of non-public health agency entities?
- **What is the role of the entity collecting the data?**
  - Health care provider?
  - Public health authority?
  - Employer?
  - Other?
- **What data are being collected?**
- **In what form are the data being collected?**
- **From whom are the data being collected?**
- **What is the purpose of collecting the data?**

Data Use

- What are the data to be used for?

Data Disclosure

- Who is requesting the data?
- If different from the requestor, to whom will the data be disclosed?
- What is the role of the entity or individual requesting the data?
- What specific information is being requested?
- For what purpose are they requesting the data

Decision Making Framework

Data Protection

- **Storage**
  - Who stores the data?
  - In what form are the data stored?
  - How are the data protected?
  - How long are the data being retained?
- **Transmission**
  - In what form are the data transmitted?
  - How are the data protected?
- **Disposal**
  - How are the data destroyed?
  - When are the data destroyed?
  - Who destroys the data?

Matthew Penn
mpenn@cdc.gov
(404) 498-0452

For more information, contact CDC
1-800-CDC-INFO (232-4636)
TTY: 1-888-232-6348 www.cdc.gov

The findings and conclusions in this report are those of the authors and do not necessarily represent the official position of the Centers for Disease Control and Prevention.

Substance Abuse and Mental Health Services Administration

SAMHSA

www.samhsa.gov • 1-877-SAMHSA-7 (1-877-726-4727)

Behavioral Health is Essential To Health

Prevention Works

Treatment is Effective

People Recover

Substance Abuse and Mental Health Services Administration
SAMHSA
www.samhsa.gov • 1-877-SAMHSA-7 (1-877-726-4727)

Confidentiality of Substance Use Disorder Patient Records Final Rule (42 CFR Part 2)

Kimberly Johnson, PhD
Director, Center for Substance Abuse Treatment
Substance Abuse and Mental Health Services Administration
U.S. Department of Health & Human Services

DEPARTMENT OF HEALTH & HUMAN SERVICES · USA

MODERNIZING 42 CFR PART 2

OVERVIEW OF PRESENTATION

- Background
- Notice of Proposed Rulemaking (NPRM)
- Final Rule
- Supplemental Notice of Proposed Rulemaking (SNPRM)

RIGHTS AND RESPONSIBILITIES

➔Modern version of the Hippocratic Oath:

"I will respect the privacy of my patients, for their problems are not disclosed to me that the world may know."

http://guides.library.jhu.edu/c.php?g=202502&p=1335759

ACCESS & QUALITY HINGE ON TRUST…

The Washington Post

PowerPost

Federal Insider

Cyberattacks on personal health records growing 'exponentially'

By Joe Davidson | Columnist September 28 at 7:00 AM

United States Government Accountability Office

GAO

Report to the Committee on Health, Education, Labor, and Pensions, U.S. Senate

August 2016

ELECTRONIC HEALTH INFORMATION

HHS Needs to Strengthen Security and Privacy Guidance and Oversight

HEALTH PRIVACY LEGISLATION

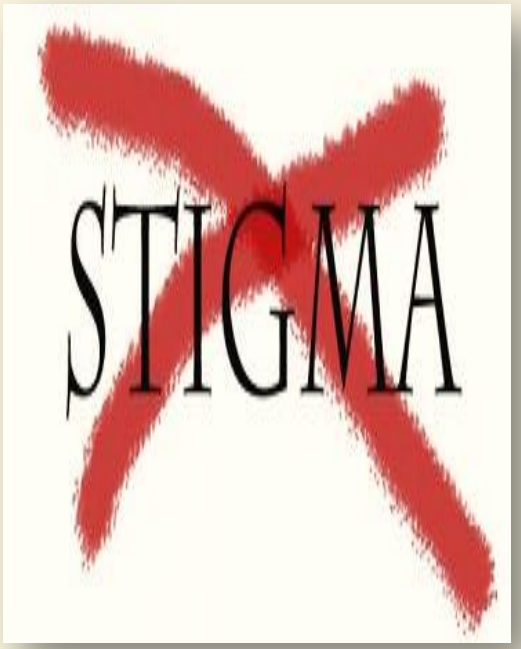
- Congress recognized that the stigma associated with substance use disorders and fear of prosecution deterred people from entering treatment, and enacted the statute authorizing **42 CFR part 2** to ensure an individual's right to privacy and confidentiality.
- For decades 42 CFR part 2 has been in the vanguard of personal privacy protections and the cornerstone of treatment programs across the country.

BASICS: 42 CFR Part 2

- Implements federal drug and alcohol confidentiality law (42 U.S.C. §290dd-2).
  - Protects confidentiality of the identity, diagnosis, prognosis, or treatment of any patient records maintained in connection with the performance of any federally assisted program or activity relating to substance abuse education, prevention, training, treatment, rehabilitation or research.

CONTEXT: 42 CFR Part 2

- The law and regulations were written during a time of great concern about the potential use of substance use disorder information against an individual.



- The purpose of 42 CFR part 2 is to ensure that a patient receiving treatment for a substance use disorder in a part 2 program is not made more vulnerable than an individual with a substance use disorder who does not seek treatment.

WHY REVISE 42 CFR PART 2?

- Regulations first promulgated in 1975 and last substantively updated in 1987.
- Significant changes have impacted health care delivery since then:
  - New models of integrated care that rely on information sharing to support coordination of patient care.
  - Electronic infrastructure for information exchange.
  - New focus on performance measurement.

CONSIDERATIONS IN REVISING 42 CFR PART 2

- Breach of privacy of information protected by part 2 can still lead to civil and criminal consequences for patients, including:
  - Loss of employment, housing, child custody.
  - Discrimination by medical professionals and insurers.
  - Arrest, prosecution and incarceration.

PREVENTING UNINTENDED CONSEQUENCES

- Importantly, the consequences of fewer and laxer privacy controls and regulations can disproportionally penalize minority, underserved, and otherwise marginalized populations.
  - In this context, loosening privacy controls could *increase* rather than reduce health disparities, and *impede* rather than promote access.

LISTENING TO THE PUBLIC

- SAMHSA held a Public Listening Session in 2014 to solicit feedback on 42 CFR part 2.
  - Approximately 1,800 individuals participated in the session (in person or by phone).
  - SAMHSA received 112 oral comments and 635 written comments.

THE PROCESS: 42 CFR PART 2 NPRM

- In addition to considering the wealth of public input received from the Listening Session, SAMHSA collaborated with its federal partner experts in developing the NPRM.
- NPRM published in the Federal Register on February 9, 2016 (81 FR 6988).
- Comment Period was 60 days and closed on April 11, 2016.
- 376 comments were received.

42 CFR PART 2 FINAL RULE

- Final rule published in the Federal Register on January 18, 2017 (82 FR 6052).
- Federal Register effective date initially scheduled for February 17, 2017.
- *Review by the administration resulted in a revised effective date of 3/21/2017.*

6052 Federal Register / Vol. 82, No. 11 / Wednesday, January 18, 2017 / Rules and Regulations

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Office of the Secretary

42 CFR Part 2

[SAMHSA–4162–20]

RIN 0930–AA21

Confidentiality of Substance Use Disorder Patient Records

AGENCY: Substance Abuse and Mental Health Services Administration, HHS.

ACTION: Final rule.

SUMMARY: The Department of Health and Human Services (HHS) is issuing this final rule to update and modernize the Confidentiality of Alcohol and Drug Abuse Patient Records regulations and facilitate information exchange within new health care models while addressing the legitimate privacy concerns of patients seeking treatment for a substance use disorder. These modifications also help clarify the regulations and reduce unnecessary burden.

e. Withdrawal Management
2. Existing Definitions
a. Central Registry
b. Disclose or Disclosure
c. Maintenance Treatment
d. Member Program
e. Patient
f. Patient Identifying Information
g. Person
h. Program
i. Qualified Service Organization
j. Records
k. Treatment
3. Terminology Changes
4. Other Comments on Definitions
E. Applicability (§ 2.12)
F. Confidentiality Restrictions and Safeguards (§ 2.13)
1. Delayed Implementation of List of Disclosures Provision
2. Responsibilities Under the List of Disclosures Process
3. Technological Challenges and Burden of the List of Disclosures Provision
4. Recommendations to Further Protect Patient Privacy
5. Other Comments and Recommendations on the List of Disclosures Provision
G. Security for Records (§ 2.16)
H. Disposition of Records by Discontinued Programs (§ 2.19)
I. Notice to Patients of Federal Confidentiality Requirements (§ 2.22)
3. Documentation of Medical Emergency
4. Other Comments on Medical Emergency
N. Research (§ 2.52)
1. General
2. Suggestions for Improvement of the Research Provisions
3. HIPAA and HHS Common Rule Requirements
4. Data Linkages
5. Multi-Payer Claims Database
O. Audit and Evaluation (§ 2.53)
P. Other Public Comments on the Proposed Rule
1. Requests to Extend the Public Comment Period
2. Rulemaking Process
3. Implementation Timeline and Other Barriers to Implementation
4. Educational Opportunities
5. Increased Enforcement
6. Other Miscellaneous Comments on the Proposed Rule
VI. Rulemaking Analyses
A. Paperwork Reduction Act
B. Regulatory Impact Analysis
C. Regulatory Flexibility Act
D. Unfunded Mandates Reform Act
E. Federalism (Executive Order 13132)

Acronyms

ACO Accountable Care Organization
ABAM American Board of Addiction

https://www.federalregister.gov/documents/2017/01/18/2017-00719/confidentiality-of-substance-use-disorder-patient-records

Snapshot of Final Rule Major Provisions

PROTECTION AND FACILITATION

- Final rule is intended to modernize the part 2 rules by facilitating the electronic exchange of substance use disorder information for treatment and other legitimate health care purposes while ensuring appropriate confidentiality protections for records that might identify an individual, directly or indirectly, as having a substance use disorder.

LANGUAGE MATTERS

- In the final rule, SAMHSA made terminology changes throughout for clarity, consistency, and to modernize the regulations (e.g., from “alcohol and drug abuse” to “substance use disorder”).
  - SAMHSA changed the name of the regulations to**: Confidentiality of Substance Use Disorder Patient Records**.

CONSENT REQUIREMENTS (§2.31)

➔The final rule:

- Allows, in certain circumstances, a patient to include a *general designation* in the "To Whom" section of the consent form.
  - Distinction between those with and without a treating provider relationship with the patient.
- Requires an explicit description of the "Amount and Kind" of substance use disorder treatment information.

CONSENT REQUIREMENTS (§2.31) (cont.)

- The final rule retains the "From Whom" provision of the 1987 regulations (as amended) with minor updates to terminology.
  - The final "From Whom" provision of the consent requirements *specifies that a written consent to a disclosure of patient identifying information must* include the specific name(s) or general designation(s) of the part 2 program(s), entity(ies), or individual(s) permitted to make the disclosure.

CONSENT REQUIREMENTS (§2.31) (cont.)

- The final rule requires the consent form to include a statement that the patient understands:
  - When using a general designation in the "To Whom" section, their right to obtain, upon request, a list of entities to whom their information has been disclosed, pursuant to the general designation (see §2.13).
- The final rule permits electronic signatures (to the extent that they are not prohibited by any applicable law).

CONFIDENTIALITY RESTRICTIONS & SAFEGUARDS (§2.13)

- The final rule requires that, upon request, patients who have included a general designation in the "To Whom" section of the consent form must be provided a list of entities to whom their information has been disclosed pursuant to a general designation (List of Disclosures).
  - However, in the final rule, SAMHSA clarified that the entity that serves as an intermediary, ***NOT the part 2 program***, is responsible for complying with the List of Disclosures requirement.

CONFIDENTIALITY RESTRICTIONS & SAFEGUARDS (§2.13) (cont.)

- The final rule clarifies that the general designation on the consent form may not be used until entities required to comply with the List of Disclosures provision have the ability to do so.
- SAMHSA may issue subregulatory guidance on this provision.

PROHIBITION ON RE-DISCLOSURE (§2.32)

- The final rule clarifies that the prohibition on re-disclosure only applies to information that would identify, directly or indirectly, an individual as having been diagnosed, treated, or referred for treatment for a substance use disorder, such as indicated through standard medical codes, descriptive language, or both, and allows other health-related information shared by the part 2 program to be re-disclosed, if permissible under other applicable laws.

PROHIBITION ON RE-DISCLOSURE (§2.32) (cont.)

- SAMHSA made some additional minor clarifying revisions to §2.32 relative to:
  - The use of general authorizations.
  - The restrictions on using information to criminally investigate or prosecute a patient with a substance use disorder.

APPLICABILITY(§2.12)

- Applicability is based on the definition of *Program,* which did not change except for updating terminology.
- Consistent with SAMHSA's previous FAQ guidance, a practice comprised of primary care providers could be considered a "general medical facility" and be subject to 42 CFR part 2 if the practice is both "federally assisted" and meets the definition of a program under § 2.11.

SECURITY FOR RECORDS (§2.16)

➔The final rule:

- Addresses both paper and electronic records.
- Clarifies that both part 2 programs and other lawful holders of patient identifying information must have in place formal policies and procedures for the security of records, including sanitizing media associated with both paper and electronic records.

SECURITY FOR RECORDS (§2.16) (cont.)

- Must reasonably protect against unauthorized uses and disclosures of patient identifying information and protect against reasonably anticipated threats or hazards to the security of patient identifying information.

- Replaces relevant language in other sections with reference to the policies and procedures requirement in §2.16.

➔ SAMHSA may provide subregulatory guidance on this provision.

MEDICAL EMERGENCIES (§2.51)

- The final rule revises the medical emergency exception to make it consistent with the statutory language and to give providers more discretion to determine when a "bona fide medical emergency" exists.
- SAMHSA is considering issuing subregulatory guidance addressing this provision.

RESEARCH (§2.52)

- The final rule allows a part 2 program or other lawful holder of patient identifying information to disclose part 2 data to qualified personnel for purposes of conducting scientific research if the researcher provides documentation of meeting certain requirements for existing protections for human research (HIPAA and/or HHS Common Rule).

RESEARCH (§2.52): DISCLOSURE MODIFICATIONS

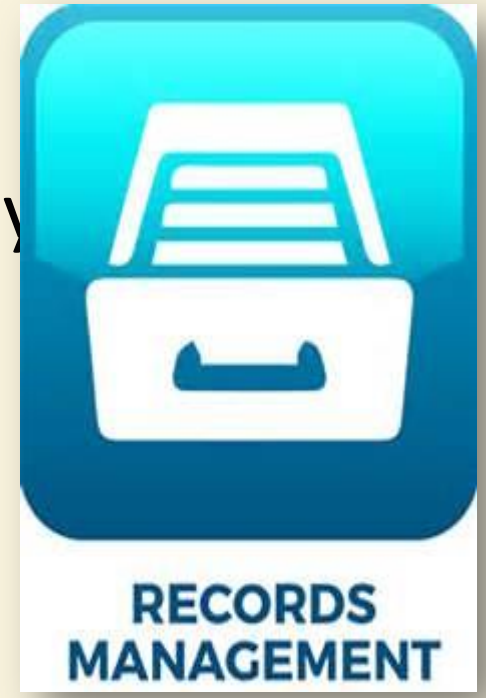
- In the final rule:
  - § 2.52(a) clarifies that lawful holders may re-disclose part 2 data for research purposes, subject to the other conditions imposed in § 2.52.
  - § 2.52(a)(2) clarifies that disclosure of part 2 data also is permitted for research that qualifies for exemption under the Common Rule due to the lower risk to subjects in circumstances where exemptions apply.

RESEARCH (§2.52): **DATA LINKAGES**

- The final rule enables researchers holding part 2 data to link to data sets from federal and non-federal data repositories provided certain conditions are met.
  - Supports more advanced research, including studies of longitudinal effects of patient treatments.

RESEARCH (§2.52): **RECORDS MANAGEMENT**

- The final rule addresses the retention and disposal of part 2 data used in research by referencing §2.16, Security for Records.
- SAMSHA may issue additional subregulatory guidance on the Research provision.



AUDIT AND EVALUATION (§2.53)

➔ The final rule:

- Includes provisions for both paper and electronic patient records.
- Permits the part 2 program, not just the part 2 program director, to determine who is qualified to conduct an audit or evaluation.
- Updates the Medicare and Medicaid audit or evaluation section to include the Children's Health Insurance Program (CHIP).

AUDIT AND EVALUATION (§2.53) (cont.)

- Permits an audit or evaluation necessary to meet the requirements (under certain conditions) of Centers for Medicare & Medicaid (CMS)-regulated accountable care organizations or similar CMS-regulated organizations (including CMS-regulated Qualified Entities).
- Revises the requirements for destroying records by referencing §2.16, Security for Records.

REPORTS OF VIOLATIONS (§2.4)

- The final rule revises the requirement for reporting violations of part 2 by opioid treatment programs to the Food and Drug Administration (FDA) because authority over these programs was transferred from the FDA to SAMHSA in 2001.

NOTICE TO PATIENTS OF FEDERAL CONFIDENTIALITY REQUIREMENTS (§2.22)

➔The final rule:

- Clarifies that the written summary of federal law and regulations may be provided to patients in either paper or electronic format.
- Requires the statement regarding the reporting of violations to include contact information for the appropriate authorities.

DISPOSITION OF RECORDS BY DISCONTINUED PROGRAMS (§2.19)

➔The final rule:

- Includes provisions for both paper and electronic patient records.
- Adds requirements for sanitizing paper records and electronic media, which is distinctly different from deleting electronic media.

DISPOSITION OF RECORDS BY DISCONTINUED PROGRAMS (§2.19) (cont.)

- Requires the process of sanitizing paper media (including printer and FAX ribbons, drums, etc.) or electronic media to be permanent and irreversible, so that there is no risk that the information may be recovered.
- Makes a distinction between electronic devices (something that has computing capability, such as a laptop, tablet, etc.) and electronic media (something that can be read on an electronic device, such as a CD/DVD, flash drive, etc.).

DISPOSITION OF RECORDS BY DISCONTINUED PROGRAMS (§2.19) (cont.)

- Allows one year to complete the process of sanitizing electronic media that are subject to longer retention periods required by law.
  - This change should allow for select patient records to be removed from both the specific site and any operational sources without disrupting other patient records.

DEFINITIONS (§2.11)

➔The final rule revises the previous regulations by:

- Consolidating all but one definition in a single section (§2.11).
  - "Federally assisted" remains in the Applicability provision at §2.12 for the purpose of clarity.
- Modernizing terminology and ensuring consistency of use across regulations.

EXISTING DEFINITIONS (§2.11)

➔Updated terminology, only:

- *Central registry.*
- *Diagnosis.*
- *Disclose (formerly Disclose or disclosure).*
- *Maintenance treatment*.
- *Program*.

➔*Member program:* updated terminology and replaced a reference to a specific geographic distance.

EXISTING DEFINITIONS (§2.11) (cont.)

➔ *Patient identifying information:* ". . . or similar information by which the identity of a patient, as defined in this section, can be determined with reasonable accuracy ~~and speed~~ either directly or by reference to other ~~publicly~~ available information."

- Clarified the meaning of the term *similar information* in the preamble discussion.

EXISTING DEFINITIONS (§2.11) (cont.)

- *Patient:* updated terminology and added that the definition includes both current and former patients.
- *Person:* added "Also referred to as 'individual or entity'".
- *Qualified Service Organization:* updated terminology, and revised the list of examples to add *population health management*, and to clarify that the term *medical services* is limited to *medical staffing services.*

EXISTING DEFINITIONS (§2.11) (cont.)

- *Records:* updated terminology, added examples of a record, and "any information, whether recorded or not, created by, ~~relating to a patient~~ received or acquired by a part 2 program relating to a patient…"
- *Treatment:* updated terminology and deleted the term *management* because it has a broader meaning than when the regulations were last revised.

NEW DEFINITIONS (§2.11)

- *Part 2 program:* which is separate and distinct from the definition of *Program.*
- *Part 2 program director:* which replaced *Program director*.
- *Withdrawal management: which replaced Detoxification treatment.*

NEW DEFINITIONS (§2.11) (cont.)

- *Substance Use Disorder:* which replaced *Alcohol abuse* and *Drug abuse*.
- *Treating provider relationship:* added because the final rule revises the consent requirements to permit, in certain circumstances, a general designation of individuals or entities to which a disclosure can be made, but only if they have a *treating provider relationship* with the patient whose information is being disclosed.

2017 SUPPLEMENTAL NOTICE OF PROPOSED RULEMAKING (SNPRM)

- In addition to the final rule, SAMHSA issued a SNPRM on January 18, 2017 (82 FR 5485).
  - Sought to obtain additional comments and information on some additional proposed clarifications to 42 CFR part 2.

CLARIFICATIONS

https://www.regulations.gov/document?D=HHS-OS-2016-0005-0378

42 CFR PART 2 SNPRM PUBLIC COMMENT PERIOD

- Comment Period was 30 days and closed on February 17, 2017.

https://www.regulations.gov/document?D=HHS-OS-2016-0005-0378

SNPRM OVERVIEW: PERMISSIBLE DISCLOSURES

- SAMHSA issued this SNPRM in response to public comments received on the NPRM that addressed specific changes not proposed in the NPRM.
- These comments led SAMHSA to propose additional clarifications and modifications to the part 2 rules to clarify the scope of permissible disclosures.

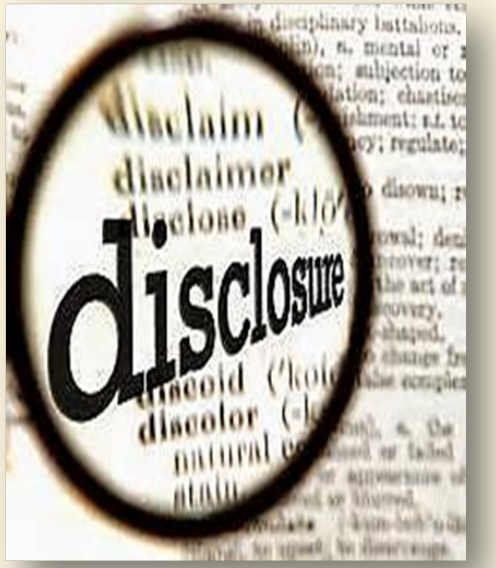
STAKEHOLDER CONCERNS: USE & DISCLOSURE

- NPRM comments highlighted varying interpretations of the rule's restrictions on lawful holders and their contractors' and subcontractors' use and disclosure of patient identifying information for purposes of carrying out payment, health care operations, and other health care related activities.
  - Third-party payers, other lawful holders, and their contractors and subcontractors and legal representatives play a critical role in the provision of health care services.

42 CFR PART 2 SNPRM: SNAPSHOT OF MAJOR PROVISIONS

PROPOSED PROVISIONS § 2.32 & § 2.33

- Specifically, SAMHSA sought comments on the following proposed provisions:
  - § 2.32 (Prohibition on Re-disclosure) – to consider whether an abbreviated notice would be appropriate and in which circumstances.
  - § 2.33 (Disclosures Permitted with Written Consent) – to define and limit the circumstances in which certain disclosures for the purposes of payment and health care operations can be made.



PROPOSED PROVISION: § 2.53

- § 2.53 (Audit and Evaluation) - to expressly address **further disclosures** to contractors, subcontractors, and legal representatives for purposes of carrying out a Medicaid, Medicare, or CHIP audit or evaluation.

PROHIBITION ON RE-DISCLOSURE (§2.32): ADDED NOTIFICATION?

- SAMHSA did not propose to substantively modify the existing notice at 2.32, *but sought comment on whether it should add an abbreviated notice to accompany re-disclosure for use in certain circumstances where a shorter notice may be warranted.*
  - For example, "Data is subject to 42 CFR part 2. Use/disclose in conformance with part 2."

Disclosures Permitted With Written Consent (§2.33): **Patient Identifying Information (PII)**

- SAMHSA proposed to explicitly list and limit under § 2.33(b), specific types of activities for which any lawful holder of patient identifying information would be allowed to further disclose the minimal information necessary for specific payment and health care operations activities.
  - *Lawful holders may disclose patient identifying information to contractors, subcontractors, and legal representatives for the purposes described in the list of activities.*

Disclosures Permitted With Written Consent (§2.33): **PII & Required Consent**

- List of activities is similar to HIPAA Privacy Rule's definitions of "payment" and "health care operations," but excludes those related to diagnosis, treatment, or referral for treatment (e.g., care coordination or case management).
  - *Consent is required*, and *contractors, subcontractors, and legal representatives must perform a function that is consistent with the stated purpose of the consent and only use the information to perform that function*.

Disclosures Permitted With Written Consent (§2.33): PII and Contractors & Subcontractors

- SAMHSA proposed new regulatory text under § 2.33(c) *requiring that lawful holders that engage contractors and subcontractors* to carry out payment and health care operations that will entail using or disclosing patient identifying information include specific contract and subcontract provisions *requiring contractors and subcontractors to comply with the provisions of part 2*.
  - Appropriate comparable instrument will suffice in cases involving a legal representative.

Disclosures Permitted With Written Consent (§2.33): **Adequate Privacy Protections?**

- SAMHSA solicited comment on whether the proposed listing of explicitly permitted activities is adequate and appropriate to ensure the health care industry's ability to conduct necessary payment and the described health care operational functions, while still affording adequate privacy protections.

Disclosures Permitted With Written Consent (§2.33): Clarity On Scope of Consent

- SAMHSA sought comments on the proper mechanisms to convey the scope of the consent to lawful holders, contractors, subcontractors, and legal representatives, including those who are downstream recipients of patient identifying information given current electronic data exchange technical designs.

AUDIT AND EVALUATION (§2.53)

- SAMHSA proposed to revise the Audit and Evaluation provision to address the following issues raised by commenters:
  - Contractors, subcontractors, and legal representatives may be tasked with conducting audit and evaluation activities.
  - Such entities may not be CMS-regulated, and audits may be conducted for private payers as well as Medicare and Medicaid programs.

AUDIT AND EVALUATION (§2.53) (cont.)

- Audits and evaluations may include quality improvement activities, as well as efforts related to reimbursement and financing.

RESPONSIVENESS TO PUBLIC COMMENTS?

- The new proposals and clarifications discussed in this SNPRM are intended to provide the desired solutions and understanding sought by commenters to the NPRM, while also offering patient protections appropriate to the current health care environment.
- The payment, health care operations, and audit and evaluation functions discussed in the SNPRM may be subject to other applicable laws and regulations, in addition to 42 CFR part 2. (e.g., the HIPAA Privacy and Security Rule).

PATIENT PRIVACY & DUE DILIGENCE

- The fact that lawful holders and part 2 programs are permitted to disclose data in no way obviates:
  - The purpose of part 2: to protect patient identifying information for patients seeking diagnosis, treatment, or referral for treatment for substance use disorders.
  - The responsibility lawful holders and part 2 programs have: to exercise due diligence with respect to their contractors, subcontractors, or legal representatives to whom they disclose or with whom they exchange patient identifying information.

FINAL RULE AND SNPRM NEXT STEPS

➔SAMHSA will:

- Review SNPRM comments received by the deadline and determine how to move forward.
- Consider developing subregulatory guidance.
- Consider the need for additional webinars, other presentations, and outreach materials.
- Consistent with the 21st Century Cures Act, "convene relevant stakeholders" to discuss its effect on "patient care, health outcomes, and patient privacy."

CLOSING THOUGHTS: PRIVACY & BEST CARE

- 42 CFR Part 2 and other regulations provide ground rules, but how these rules are applied to ensure privacy *and* the best care requires careful analysis and monitoring.
  - Who needs what information when?
  - Who determines who needs what information when?
  - What are the consequences & outcomes?
  - And more…

QUESTIONS OR COMMENTS?

THANK YOU,

Kimberly.Johnson@samhsa.hhs.gov