2018

ADDRESSING THE OPIOID EPIDEMIC:

INFORMATION SHARING

In the context of

State and Federal Privacy Laws

METROPOLITAN MAYORS COALITION

a local initiative facilitated by METROPOLITAN AREA PLANNING COUNCIL

ACKNOWLEDGEMENTS

Harvard Cyberlaw Clinic:
Austin Bohn
Mason Kortz
Michael Roig

CONTENTS

INTRODUCTION

A major challenge in providing care and ongoing support for people with opioid use disorders is effectively and legally sharing information. Individuals with a substance use disorder (SUD) interact with a range of organizations and individuals, from hospitals to police officers, recovery coaches, or family members. Helping people with SUDs recover often requires that those parties work together and understand the circumstances of those in recovery in as close to real time as possible. There are of course operational barriers to effective information sharing, but of equal importance is an understanding of the legal parameters that delineate what medical and addiction treatment information can be shared – and shared by whom, and with whom; with whose consent; in what formats; and when.

BACKGROUND

The content of this document was developed by the Harvard Law School CyberLaw Clinic. The Clinic conducted this work in support of a project the Metropolitan Area Planning Council (MAPC) is leading on behalf of the 15 cities and towns in Greater Boston's inner core that make up the Metropolitan Mayor's Coalition (MMC). A forum held in May 2017 and subsequent engagement with municipal public health and safety personnel from MMC communities identified information sharing as a key challenge in addressing the opioid epidemic for local governments. This project intends to help municipal officials improve information sharing approaches and this document is intended to inform their options.

SUMMARY

The document is designed to address some basic questions for organizations and municipal officials about the laws that govern medical and addiction treatment related information. To achieve that goal, the document summarizes federal and state data sharing laws and their application; presents the role of consent regimes that enable information sharing; provides some scenario-based examples to inform practice; and describes data sharing models that currently exist. **By no means is the document comprehensive and the statements herein do not constitute formal legal advice.** The rules governing data sharing can be highly case-specific and different circumstances may result in different applications. **Talking to appropriate legal counsel is therefore recommended before implementing any data sharing plans.**

OVERVIEW OF FEDERAL AND STATE PRIVACY LAWS

Inventory of Federal and State Laws
HIPAA's Privacy Act[1]
HIPAA's Part 2
FERPA
MGL c.94c, § 18B, Voluntary Non-Opioid Directive Form
MGL c.94c, § 24A, Electronic Monitoring of Prescription Drugs
MGL c.111, § 70F, HIV Testing (MGL c.111, § 70G)
MGL c.112, § 12A, Reporting of Opiate Overdose
MGL, c. 112, § 135A, Confidentiality & Social Workers
MGL c.112, § 172, Confidentiality & Mental Health Providers
- (MGL c.112, § 121A)

FEDERAL LAWS REGULATING DATA SHARING

The primary, federal bodies of law that apply are **HIPAA's Privacy Act[1], HIPAA's Part 2[2]**, and **FERPA[3].**

The Standards for Privacy of Individually Identifiable Health Information ("Privacy Rule") is the implementation of the **Health Insurance Portability and Accountability Act**[4] ("HIPAA") to protect certain healthcare data. The Confidentiality of Substance Use Disorder Patient Records ("Part 2") imposes additional restrictions on the disclosure and use of substance use disorder patient records. Depending on the person or organization holding the data, and the nature of the information involved, healthcare data may fall under the Privacy Rule, Part 2, or both.

HIPAA Privacy Rule

> **Under 45 CFR Parts 160 and 164, the Privacy Rule applies to all covered entities and business associates.**
>
> Covered entities include health plans, health care clearinghouses, and health care providers who transmit any health information in electronic form in connection with a transaction covered by the Privacy Rule. Government agencies may be covered entities. For example, Medicare and Medicaid are health plans, and public health agencies that process data or facilitate health information exchanges may qualify as health care clearinghouses.
>
> Business associates are organizations that handle **Protected Health Information (PHI)** on behalf of covered entities, usually as contractors. Common business associates include data storage providers, benefits managers, patient portal providers, and legal, business, or accounting firms.[5]

+ What data does the Privacy Rule apply to?

The Privacy Rule prohibits a covered entity or business associate from using or disclosing PHI, except as otherwise permitted.

PHI means individually identifiable health information, which is:

1. Created or received by a health care provider, health plan, employer, or health care clearinghouse; and
2. Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and
3. Identifies the individual or could be reasonably believed as providing the ability to identify the individual.

The Privacy Rule does not restrict information that has been de-identified. De-identified protected health information is health information that does not identify, nor could be reasonably used to identify, an individual. The Privacy Rule defines 17 specific pieces of information that must be removed for PHI to be de-identified, as well as a catch-all for any unique number, characteristic, or code that is associated with an individual.

However, de-identified data can include a code used internally by the covered entity to identify an individual, as long as that code is not made available outside the covered entity.[6]

+ What exceptions from the Privacy Rule are available?

With proper HIPAA authorization, most data can be disclosed. Additionally, some information may be shared with some parties based on a simple, unwritten agreement by the patient (see the "Consent" section below). There are also some situations in which a covered entity (or business associate) may disclose PHI without authorization or consent.

These exceptions enable, but do not require, a covered entity to use and disclose PHI without an individual's authorization for the following purposes:

1. To the individual;
2. To a health care provider for treatment purposes;
3. To a covered entity for payment or health care operations (so long as both entities have or had a relationship with the individual and the PHI pertains to the relationship);
4. To a family member or other person involved in the individual's care, when the individual is incapacitated or unavailable and in the covered entity's professional judgment disclosure is in the best interests of the individual;
5. To police, courts, or other government agencies for specific, official functions;
6. To public health authorities for particular activities, such as controlling the spread of disease, conducting public health investigations and interventions, and reporting child abuse and neglect;
7. To prevent serious and imminent danger to the individual or another person;
8. As a limited data set, without certain identifiers, provided for research, health care operations, or a public health purpose; or
9. Incidental use and disclosure so long as reasonable safeguards are in place (described in further detail by the Privacy Rule).

The limits of these exceptions are not always clear. For example, there is no definition for what constitutes being "involved with" a patient's care. Guidance from the Department of Health and Human Services (HHS) describe it as including close friends, caregivers, and home health aides[7], but does not expressly limit it to those circumstances. Similarly, the "public health" exception has been the subject of much debate and even some litigation. The few judicial opinions available suggest that the exception applies to tracking or preventing disease and injury on a large scale[8] but not to individual interventions or treatment[9]. However, exactly where the line should be drawn is still an open question.

HIPAA Part 2

> Part 2 applies to any substance abuse information obtained by a federally assisted substance abuse program, which means any program that (1) directly or indirectly receives federal funds, is federally licensed, or is tax-exempt under federal law and (2) primarily provides substance abuse treatment. Such programs may include an individual, entity, or identified unit within a general medical facility holding itself out as providing, and provides, substance use disorder diagnosis, treatment, or referral for treatment. Such programs also include medical personnel or other staff in a general medical facility whose primary function is the provision of substance use disorder diagnosis, treatment, or referral for treatment, and who are identified as such providers.[10]

+ What data does Part 2 apply to?

Part 2 restricts disclosure of information that could reasonably be used to identify an individual as having or had a substance use disorder either directly, by reference to publicly available information, or through verification of such identification by another person.[11]

Part 2 does not restrict information that has been de-identified. De-identified PHI is health information that does not identify, nor could be reasonably used to identify, an individual. The Privacy Rule defines specific requirements for data to be considered de-identified in 45 CFR § 164.514.

+ What exceptions from Part 2 are available?

HIPAA Part 2 has a much stronger prohibition against use and disclosure than the Privacy Rule. Part 2 allows for communications within a substance abuse program, or between a substance abuse program and an entity that has direct administrative control over it, such as a hospital that contains a substance abuse clinic. However, even these disclosures are on a "need to know" basis—they are limited to those persons who need the information in connection with the provision of diagnosis, treatment, or referral for treatment of patients with substance use disorders.[12] Records can also be disclosed in a medical emergency; the substance abuse program must document any disclosure made under this rule.[13] Any other disclosure requires authorization compliant with Part 2 requirements.

Family Educational Rights and Privacy (FERPA)

> FERPA applies to educational agencies and institutions that receive funds under any program administered by the U.S. Department of Education. This law exists because these educational agencies generally would not be covered entities under HIPAA.[14]
>
> An educational agency subject to FERPA may not have a policy or practice of disclosing the education records of students, or personally identifiable information from education records, without a parent or eligible student's written consent. An "eligible student" is a student who is at least 18 years of age or one who attends a postsecondary institution at any age.
>
> Education records are records that directly relate to a student and are maintained by the educational agency or by a party acting for the agency or institution. At the elementary or secondary level, a student's health records, including immunization records and records by a school nurse, maintained by an educational agency subject to FERPA are considered education records. As education records, the information is protected under FERPA and not HIPAA. Education records also include transcripts, disciplinary records, and attendance information.

De-identified education records may be shared without consent under FERPA.

FERPA protects personally identifiable records and information. Personally identifiable information includes but is not limited to:

- The student's name or address, or that of their family;
- Any personal identifier, such as a social security number, student number, or biometric record;
- Indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name;
- Other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; or
- Any other information, if the educational agency or institution reasonably believes that the requester knows the identity of the student involved.

+ What exceptions are available from FERPA?

There are two exceptions that allow disclosure of education records without consent.[15] In either circumstance, the disclosure may only occur on the condition that the receiving party will not disclose the information to any other party without the consent of the parent or eligible student.

These exceptions are:

1. Disclosure to other school officials within the agency whom the agency has determined to have legitimate educational interests (School officials include parties to whom a school has outsourced institutional services or functions, provided that the outside party: performs an institutional service/function for which the agency would otherwise use employees; is under the direct control of the agency with respect to the use and maintenance of education records; and is subject to the redisclosure requirements of education records); and

2. Disclosure to officials of another school where the student seeks or intends to enroll, or where the student is already enrolled so long as the disclosure is for purposes related to the student's enrollment or transfer.

MASSACHUSETTS STATE LAWS REGULATING DATA SHARING

Massachusetts privacy law is not as comprehensive as HIPAA or HIPAA Part 2. Under **Massachusetts General Law, MGL** c.111, s.70E, the "Patients' Rights Law," patients are conferred a broad right to "confidentiality of all records and communications to the extent provided by law" and are granted the right to "informed consent to the extent provided by law." However, despite its sweeping language, the Patients' Rights Law has been interpreted to permit the sharing of private health information insofar as it is done in compliance with HIPAA and Part 2.[16]

Other discrete laws and regulations impose piecemeal restrictions that, by and large, are consistent with or slight variations on the federal confidentiality regime:

MGL c.94c, § 18B, Voluntary Non-Opioid Directive Form

> This law directs the health departments to create forms, which would be voluntarily signed by patients, directing hospitals not to administer opioids to them.

MGL c.94c, § 24A, Electronic Monitoring of Prescription Drugs

> MA requires that an electronic system be used to monitor the prescription of drugs. Importantly, upon review of such information, "if there is reasonable cause to believe a violation of law or breach of professional standards may have occurred, the department shall notify the appropriate law enforcement . . . [and] provide prescription information required for an investigation."

MGL c.111, § 70F, HIV Testing

MA law forbids the disclosure of the results of HIV tests, as well as the identity of individuals undergoing HIV tests, without written informed consent. Written authorization for the purposes of disclosing results or identities associated with HIV testing must be "distinguished from written consent for the release of any other medical information." In other words, a standard HIPAA authorization form would not suffice to disclose such information under MA law. Written informed consent is defined as specifying each individual release the medical provider intends. MGL c.111, § 70G similarly protects genetic information.

MGL c.112, § 12A, Reporting of Opiate Overdose

Consistent with HIPAA and Part 2, MA requires that hospitals that treat individuals for injuries related to opiates also file a report containing information about that treatment with the commissioner of public health. Additionally, "the department of public health may promulgate regulations to enforce this section."

MGL, c. 112, § 135A, Confidentiality & Social Workers

All communication between a social worker and their client is deemed confidential. This information can be disclosed in two ways: 1.) where the need to disclose the information is necessary for the safety of the client or others; 2.) "upon express, written consent of [the] client." If the client is unable to consent, the client's guardian (designated by the client him or herself) may consent to the disclosure. 258 CMR 22.04, a state regulation, instructs that social workers can share information about the client without written consent to an employee of the social worker, an administrative or clinical supervisor, or a licensed professional colleague. However, the client must be given an "opportunity to object" to the disclosure, and such disclosures must be limited to what is reasonably necessary. The regulation also stipulates that recipients of such disclosures must keep the information confidential.

MGL c.112, § 172, Confidentiality & Mental Health Providers

> Information pertaining to the client of a mental health provider is deemed confidential. Confidentiality with respect to this information can be waived (i.e., relinquished) in limited circumstances. If the client communicates a plan or the commission of a crime, he or she has waived confidentiality. Alternatively, a client can waive confidentiality through consent. State regulation 262 CMR 8.02 allows a mental health professional to disclose certain information about the client to another professional, but only for the purpose of informing the provider's own treatment of the individual. Best efforts must be made to protect the client's privacy, and the client's identity cannot be shared. MGL c.112, § 121A, which covers psychologists, is substantially similar to the mental health provider statute.

+ Other Massachusetts State Laws that Regulate Data Sharing

For the purposes of this project, 104 CMR 27.17 (which governs mental health facilities), largely align with HIPAA in terms of what private health information may be disclosed. Written authorizations are required for the disclosure of private mental health information, barring exigent circumstances. On the subject of mental health, the report "Sharing Behavioral Health Information in Massachusetts" is quite useful.[17] Similarly, 105 CMR 165.084 (the regulation governing substance abuse programs) limits disclosures except where consistent with "42 CFR Part 2, and 45 CFR Parts 160 and 164 (HIPAA Privacy and Security Rules)."

On the subject of school record privacy, 603 CMR 23.00 regulates the use and disclosure of such documents. Disclosure of school records to third parties is only possible with the informed written consent of an eligible student or that student's parents. An eligible student is one who is 14 years old or has entered the 9th grade. The student or parent is able to designate which parts of the record can be disclosed. Copies of the record must be offered to the student or parent. Personally identifiable information may only be disclosed to a third party "on the condition that he/she will not permit any other third party to have access" to that information without the written consent of the student or parent.

THE ROLE OF CONSENT UNDER THE LAW

The type of consent required for the sharing of private information is contingent on two main factors: the kind of data sought to be shared, and the stakeholders involved in the sharing. Of course, an individual is free to personally share information about him or herself with anyone of their choosing. The legal limits on information sharing come into play when a health provider who controls someone's private information seeks to make a disclosure to a third party. Often, consent is the vehicle that enables third party disclosures.

When health providers seek to share information, their disclosures are governed by HIPAA and Part 2. Such disclosures generally require one of two types of consent: an opportunity to object (which can be oral or written) or authorization (which must be written and often has additional requirements). However, as discussed above, HIPAA does provide some narrow exceptions where Private Health Information (PHI) may be disclosed without a patient's prior approval. Barring those exceptions, all PHI disclosures require consent.

HIPAA PRIVACY RULE

The vast majority of healthcare disclosures require HIPAA authorization.[18] An authorization is a special type of consent given by the patient that enables healthcare providers to share PHI.

Authorizations are written; a patient cannot give authorization orally. The form must be signed by the patient, and must also include a disclaimer articulating the patient's rights with respect to the authorization (e.g., the patient's right to revoke authorization). HIPAA authorizations are subject to the "minimum determination rule" which provides that **disclosures should only contain the amount of information necessary to achieve their purpose.**

In sum, an authorization form must include:

1. The patient's name
2. The identity of the party disclosing the information
3. The identity of the third party recipients of the information
    - For HIPAA, a "class" of individuals may identified, as opposed to specific individual's names. The class can be as broad as "medical professionals."
4. A specific description of the information meant to be disclosed
5. The purpose of the disclosure
6. An expiration date, or expiration event
    - The expiration date must relate in some way to the purpose of the disclosure.

Consent may also be conferred under HIPAA by providing the patient the opportunity to agree or to object.[19] This kind of consent only applies in very narrow circumstances. Under two specific scenarios, a healthcare provider may disclose PHI to the patient's family member, relative, close personal friend, or any other person identified by the individual.

First, when the patient is present, PHI disclosures can be made to the aforementioned individuals if:

1. The patient agrees,
2. The healthcare provider offer the patient an opportunity to object and the patient does not object, or
3. The provider reasonably infers from the situation that the individual would not object.

Second, when the patient is absent or incapacitated, the provider may disclose the information to the aforementioned parties if he or she believes it to be in the best interests of the patient. This kind of disclosure must be limited to what is minimally necessary.

Part 2 allows for disclosure on the basis of one kind of consent, though it provides instances where information can be divulged without consent, for example, during medical emergencies. Even if a disclosure could be made with just an opportunity to object or without consent at all under the Privacy Rule, if the disclosure also falls under Part 2 then Part 2 consent is required.

Part 2 Consent Forms are similar to HIPAA authorizations, but contain some notable differences (bolded below).

In addition to a disclaimer of the patient's rights, such authorizations must include:

1. The patient's name
2. **A "general designation" of the party disclosing the information.** This is perhaps somewhat narrower than "class," but still need not include the name of the individuals making the disclosure.
3. **The name and title of the individuals receiving the information.**
4. A description of the amount and kind of information to be disclosed.
5. The purpose of the disclosure
6. An expiration date
7. Patient signature and date of signature.

Importantly, any disclosure of information through Part 2 requires the inclusion of specific language directed at the third party receiving the data. This language explicitly forbids any further disclosure of the information conveyed.

Each Part 2 authorization must include one of the following disclaimers:

> This information has been disclosed to you from records protected by federal confidentiality rules (42 CFR part 2). The federal rules prohibit you from making any further disclosure of information in this record that identifies a patient as having or having had a substance use disorder either directly, by reference to publicly available information, or through verification of such identification by another person unless further disclosure is expressly permitted by the written consent of the individual whose information is being disclosed or as otherwise permitted by 42 CFR part 2. A general authorization for the release of medical or other information is NOT sufficient for this purpose (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

42 CFR part 2 prohibits unauthorized disclosure of these records.

FERPA

Finally, **valid, written consent under FERPA is required for most disclosures of education records**, which includes PHI and other health care data held by the educational agency.

Valid, written consent requires:

1. Signature of a parent
   - A student can sign if he or she is
     a) 18 years or older, or
     b) enrolled in a postsecondary institution
2. A description of the specific records to be disclosed
3. A description of the purpose of the disclosure
4. The provision of a copy of the records to the parents and the student (if so desired)

Valid consent must be written and signed by the parent or eligible student and include certain information: specific records that may be disclosed; the purpose of the disclosure; and the party or class of parties to whom the disclosure may be made.

INFORMATION SHARING IN THE MUNICIPAL CONTEXT

Camden Arise
Chelsea Hub
Data-Driven Justice Initiatives
Example Scenarios

EXAMPLES OF CITIES THAT HAVE IMPLEMENTED DATA SHARING SYSTEMS

There are no restrictions on the use or disclosure of de-identified health information. De-identified health information neither identifies nor provides a reasonable basis to identify an individual.

There are two ways to de-identify information under the Privacy Rule, either:

1. a formal determination by a qualified statistician; or
2. the removal of specified identifiers of the individual and of the individual's relatives, household members, and employers is required, and is adequate only if the covered entity has no actual knowledge that the remaining information could be used to identify the individual.

However, the difficulty arises when PHI is involved. A healthcare organization covered by Part 2 or the Privacy Rule must either have authorization from the individual or fall under a specified exemption in order to use or disclose any PHI. Even organizations that are not governed by HIPAA, such as law enforcement departments, are sometimes prohibited from sharing substance abuse information obtained from a Part 2 program. Some states have similar "re-disclosure rules" that apply to non-substance abuse PHI as well.

There are also a number of exceptions to HIPAA that apply to law enforcement.[20] The Privacy Rule allows law enforcement to obtain an individual's PHI without his or her written authorization in certain circumstances.

CAMDEN ARISE

Camden Arise is a data-sharing plan information from public data systems, including criminal justice, healthcare, and housing, to create a multi-dimensional picture of citywide challenges. It is a program of the Camden Coalition—a coalition of healthcare providers, community partners, and advocates—working to address complex medical and social challenges. In their first project integrating data, they have created two separate agreements. One is a data sharing agreement between the Camden City School District and the Camden Coalition of Healthcare Providers in which the School District to provides data to the Coalition, particularly regarding absenteeism. The other is a memorandum of understanding between The County of Camden (Department of Police Services) and the Camden Coalition of Healthcare Providers authorizing the police to provide information to the Coalition. (https://www.camdenhealth.org/arise-camden/)

CHELSEA HUB

Chelsea Hub is a collection of community organizations, organized by the Police Department, that meets weekly to share information about individuals or families at risk and strategize ways to intervene. The data sharing that occurs goes through a four-stage process: identification of individuals at risk (through the identification of risk factors); introduction of de-identified data to gain intervention consensus; identification of the appropriate parties through revealing limited information; and a detailed conversation among the parties who deliver relevant services about the individual. (http://chelseapolice.com/chelsea-hub/)

DATA-DRIVEN JUSTICE INITIATIVE

The **Data-Driven Justice Initiative** is a data-sharing program that initially started in the Obama White House, and is now coordinated by the Laura and John Arnold Foundation. One of its most successful projects is a collaboration between Johnson County, Kansas, and the University of Chicago's Center for Data Science and Public Policy. The program tracks individuals across multiple public systems, including jails, emergency rooms, mental-health facilities, and social services, and attempts to identify the most effective ways to get people the care they need. The University of Chicago has entered multiple data-sharing agreements with private and public data providers so that it can integrate and analyze the data in a secure and confidential environment. (http://www.naco.org/resources/data-driven-justice-playbook; http://dsapp.uchicago.edu/projects/criminal-justice/data-driven-justice-initiative/)

A medical provider may disclose information to law enforcement in the following situations:

1. In compliance with a court order, warrant or subpoena;
2. In response to an administrative request;
    - Administrative requests are made without the involvement of a judge. They can be made by law enforcement or certain other administrative agencies. Such a request must include a description of the limited information desired, as well as the purpose of that information.
3. In response to a request for information that serves the purpose of identifying a suspect, fugitive, witness, or missing person;
4. In response to a request for information about the victim of a crime;
    - The victim must him or herself agree to this disclosure.
5. In order to report abuse, neglect, or domestic violence (these disclosures may also be made to other authorized agencies, such as public health agencies, social services, or protective services);
6. In order to report to law enforcement when required by state law;
7. In order to report the death of an individual;
8. When necessary to alert police to an on-site criminal activity, or off-site criminal activity to which medical providers responded;
9. Where, in the medical provider's professional judgment, disclosure is necessary to prevent domestic violence or any other serious, imminent threat to an individual or the public;
10. In the course of investigation concerning national security;
11. In response to a request concerning an individual in a correctional facility or in police custody.

SCENARIO 1:

A POLICE OFFICER ASKS A HOSPITAL'S REPRESENTATIVE (NOT A SUBSTANCE ABUSE, PART 2, ORGANIZATION) IF A PARTICULAR INDIVIDUAL HAS BEEN TO THE HOSPITAL, AND IF SO, HOW OFTEN AND FOR WHAT PURPOSE. HOW SHOULD THE REPRESENTATIVE RESPOND?

First, the representative may share the information if the hospital has a valid HIPAA authorization from the individual, the authorization lists the hospital as a party who can make the disclosure and lists the police as a party to whom the disclosure can be made, and the authorization has not expired or has been revoked.

If there is no authorization, the representative may indicate the individual's presence in a facility if the individual has had the opportunity to object to this type of disclosure, but it is limited to location and general condition, as discussed above. Additionally, they may disclose information about a patient who is suspected to be a victim of a crime if either the individual agrees to the disclosure or the individual is unable to agree because of incapacity or emergency circumstances and the representative reasonably believes it is in the best interest of the individual.

If there is no authorization and no opportunity to object to certain disclosures, then the representative may disclose if it falls under one of the exceptions. Particularly applicable are the exceptions for requests by law enforcement. Among others, the representative may disclose limited information for purposes of identification and location of a suspect, fugitive, material witness, or missing person. They may also disclose information about a patient who is reasonably believed to be a victim of abuse, neglect, or domestic violence as required by law.

+ What processes could help enable communication?

Obtaining valid HIPAA authorization upon admittance to the hospital to share this type of information with law enforcement would most easily enable this disclosure.

+ What if the records are held by a "federally assisted program" to which HIPAA Part 2 applies?

The representative may not disclose any PHI in this circumstance unless the individual has granted valid Part 2 authorization. If there is no authorization, the representative cannot answer. Note, most hospital's departments that provide substance use disorder treatment are "federally assisted programs" for the purposes of Part 2. However, departments such as emergency rooms that may incidentally treat drug-related issues, such as overdoses are not.

SCENARIO 2:

A POLICE OFFICER IS SITTING AMONG VARIOUS SOCIAL SERVICE ORIENTED ORGANIZATIONS, INCLUDING HOSPITALS, AND ASKS IF AN INDIVIDUAL HAS BEEN HOSPITALIZED RECENTLY OR REGULARLY. HOW SHOULD THE REPRESENTATIVES RESPOND?

First, the representatives may disclose the relevant PHI (e.g. name, admitted date, etc.) if the individual has granted valid HIPAA authorization to do so. In this case, each participating organization could receive information from the representative. However, each participating organization would need to obtain separate authorization to disclose information separately (although only if the organization is covered by HIPAA).

Without authorization, it is unlikely that one of the exceptions would apply because of the many stakeholders present (thus, the law enforcement exceptions do not apply), and the representative is unable to respond. This is the same for organizations that are covered entities under the HIPAA Privacy Rule, regardless of whether Part 2 applies (although they have different requirements for valid authorization).

Other organizations who are not subject to HIPAA may be able to share this information if they are able. However, they must be compliant with any applicable re-disclosure limitations, which may apply if the information was originally disclosed from an organization subject to HIPAA.

SCENARIO 3:

A HEALTH CARE REPRESENTATIVE ASKS A POLICE OFFICER IF AN INDIVIDUAL HAS BEEN ARRESTED OR PREVIOUSLY IMPRISONED, AND IF SO, HOW OFTEN AND FOR WHAT REASON. HOW SHOULD THE OFFICER RESPOND?

Arrest and conviction records are public record, so the officer should be able to respond accordingly, subject to Massachusetts state law.

SCENARIO 4:

A HOSPITAL RECEIVES A NEW PATIENT AND KNOWS THAT THEY HAVE A RECOVERY COACH. THE HOSPITAL IS UNSURE IF THE RECOVERY COACH IS AWARE OF THE HOSPITALIZATION. WHAT CAN THE HOSPITAL DO?

If the hospital has either obtained the individual's agreement, provided an opportunity for the individual to object to the disclosure and they did not object, or reasonably inferred that the individual does not object, then the hospital may notify a family member, personal representative of the individual, or another person responsible for the care of the individual. The notification may include the individual's location and general condition. If the recovery coach is considered "responsible for the care of the individual," then it is likely the recovery coach may be notified.

If the individual is not present or the opportunity to practicably object to the disclosure due to incapacity or anemergency circumstance is not present, then the hospital may exercise its professional judgment to determine if the disclosure is in the individual's best interest. However, the recovery coach must still be considered responsible for the care of the individual to allow notification.

+ What if the hospital is unaware of whether the patient has a recovery coach?

There is some debate over whether recovery coaches are "health care providers" under HIPAA. If they are, a hospital could freely share PHI with a recovery coach for treatment purposes under 45 CFR § 164.508. Even assuming the recovery coach is not a health care provider, there are circumstances in which the hospital could disclose the individual's PHI.

If a recovery coach inquires to the hospital about the individual's presence, the hospital may disclose the name and location so long as either the individual had the opportunity to object or was unable to do so due to incapacity or emergency circumstance and the hospital, in its professional judgment, thought it in the individual's best interest to disclose.

If the hospital believed the individual did not have a recovery coach and wanted to connect the individual with one, it would need to wait until it could obtain the patient's consent, as there is neither a pre-existing relationship nor an imminent threat that would permit the disclosure.

REFERENCES & RESOURCES

ENDNOTES

1. https://www.hhs.gov/hipaa/for-professionals/privacy/index.html
2. http://www.integration.samhsa.gov/operations-administration/the_confidentiality_of_alcohol_and_drug_abuse.pdf
3. https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html.
4. Department of Health and Human Services ("HHS") provides a summary here: https://www.hhs.gov/sites/default/files/privacysummary.pdf
5. https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html. See 45 CFR § 160.103 for further definition of business associates.
6. 45 CFR § 164.514
7. https://www.hhs.gov/sites/default/files/provider_ffg.pdf; https://www.hhs.gov/sites/default/files/hipaa-opioid-crisis.pdf.
8. Big Ridge, Inc. v. Fed. Mine Safety & Health Review Comm'n, 715 F.3d 631 (7th Cir. 2013).
9. Miguel M. v. Barron, 17 N.Y.3d 37, 950 N.E.2d 107 (2011).
10. 42 CFR § 2.11
11. https://www.samhsa.gov/sites/default/files/part2-hipaa-comparison2004.pdf
12. 42 CFR § 2.12(c)(3).

13. 42 CFR § 2.51.
14. See joint guidance on FERPA and HIPAA here: https://www2.ed.gov/policy/gen/guid/fpco/doc/ferpa-hipaa-guidance.pdf
15. https://www.law.cornell.edu/cfr/text/34/99.31; https://www2.ed.gov/policy/gen/guid/fpco/doc/ferpa-hipaa-guidance.pdf
16. http://www.mass.gov/eohhs/docs/eohhs/masshiway/20151207hitcouncil-presentation.pdf
17. https://mehi.masstech.org/sites/mehi/files/documents/Behavioral_Health_Data_Sharing_FINAL.pdf
18. https://www.hhs.gov/hipaa/for-professionals/faq/264/what-is-the-difference-between-consent-and-authorization/index.html
19. https://www.law.cornell.edu/cfr/text/45/164.510
20. https://www.hhs.gov/hipaa/for-professionals/faq/505/what-does-the-privacy-rule-allow-covered-entities-to-disclose-to-law-enforcement-officials/index.html

HOW TO STAY UPDATED

CHRISTINE HOWE
Grants Management and Procurement Specialist,
CHowe@mapc.org
617-933-0732

SHARON RON
Public Health Research Analyst
SRon@mapc.org
617-933-0788