Sharing Information with Law Enforcement—What Are the Restrictions on Crisis Teams?

Two important federal laws limit crisis teams' ability to share information with law enforcement, particularly when the purpose is investigating crimes. These two laws are:

- **The Health Insurance Portability and Accountability Act (HIPAA), including a HIPAA Privacy Rule**
- **Confidentiality of Substance Use Disorder Patient Records (42 CFR Part 2)**

DHCS

BEHAVIORAL HEALTH Continuum Infrastructure Program

CRISIS CARE MOBILE UNITS PROGRAM

HIPAA PRIVACY RULE

Of the two laws, HIPAA is more generally applicable but includes fewer restrictions. HIPAA restricts "covered entities"—providers of health care, including assessment of a person's physical or mental condition or functional status who share information electronically—from disclosing protected health information (PHI). Included in the definition of PHI are not only diagnoses, test results, and treatment history, but also verifying that a person has received services. A crisis care mobile unit (CCMU) that keeps or shares medical information electronically would almost certainly be considered a covered entity. Unless crisis teams have gotten a legal opinion that they are not covered by HIPAA, they should assume they are covered.

The most straightforward ways to share PHI in compliance with HIPAA is to have individuals sign consent forms. In that case, the CCMU team is aware of what the individual is willing to allow the team to share. Consent forms may be particularly useful in police-mental health collaborations, as noted in a helpful Council of State Governments Justice Center brief. However, obtaining consent during crisis interactions may be difficult and may be more practicable during follow-up encounters.

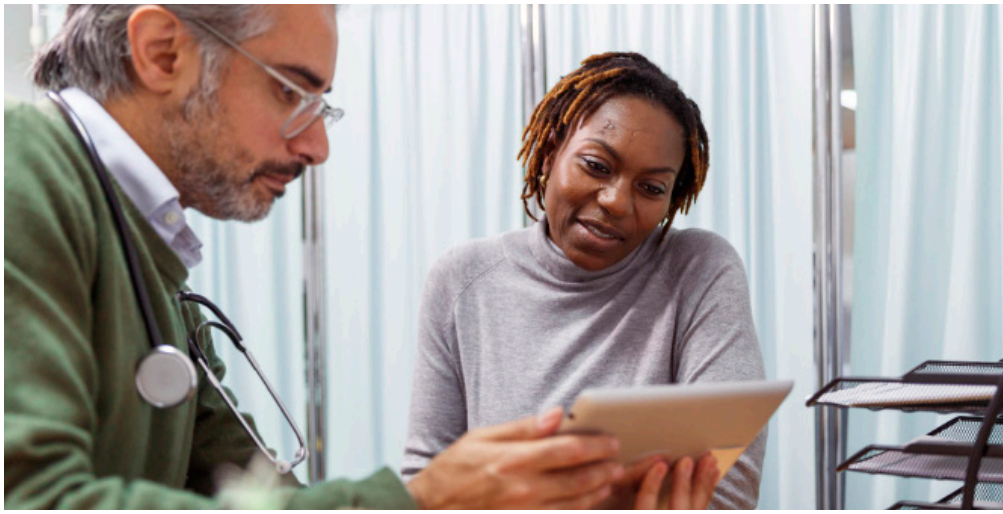
HIPAA does not prohibit all sharing of information without the individual's consent. The specific situations in which covered entities can share PHI, such as to report abuse or neglect, are covered by the HIPAA Privacy Rule. The HHS Office of Civil Rights has also put together a brief explaining that covered entities may share information about a person's identity to help connect people to family or friends who help care for the person.

The HIPAA Privacy Rule includes provisions that are specific to sharing PHI with law enforcement. The Departments of Justice and Health and Human Services (HHS) have produced a basic overview of these provisions, which include allowing a covered entity to share PHI or other information with law enforcement when:

- Needed to prevent a serious and imminent threat to the public or a specific individual;
- A crime has been committed at the covered entity or against its staff;
- A court orders the disclosure;
- State law requires reporting PHI (e.g., gunshot wounds or child abuse); or
- Needed to help identify a suspect or missing person (demographic information only).

CCMU teams are responsible for understanding the HIPAA Privacy Rule, but some general advice for preventing HIPAA privacy violations include:

1. Familiarize yourself and all staff you supervise with the HIPAA Privacy Rule.
2. Attempt to have individuals sign HIPAA consent forms if contact is made or maintained while the individual is not in active crisis.
3. Initiate disclosures to law enforcement only when there is a risk of serious harm or in case of a reportable crime (e.g., child, domestic, or elder abuse or neglect).
4. Whenever law enforcement asks for information about an individual who has not signed a HIPAA consent form, ask why they want this information.
5. Never provide PHI for the purpose of linking the individual to the past commission of a crime, without a court order, unless it is a crime you are required to report.
6. Disclose only as much information as is necessary. In some cases, this might be limited to information about the person's name and appearance.
7. If possible, disclose information to EMTs, who as noted by the National EMS Information System Technical Assistance Center are also covered entities, rather than law enforcement personnel.



42 CFR PART 2

Compared to HIPAA, Part 2 covers far fewer organizations and individuals and fewer types of records, but Part 2 places much stricter limits on sharing covered information. Part 2 applies only to records of individuals seeking substance use disorder (SUD) treatment from a "Part 2 program"—an individual or organization that is federally assisted and identifiable as SUD treatment provider. It should be noted that "federally assisted" is defined broadly to include any federal funding or federal authorization to prescribe controlled substances.

A person (or team) whose primary role is providing mental health services might not be considered a Part 2 program. The relevant question is whether disclosure of the records "would identify 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" (42 CFR § 2.12). A good illustration is that an addiction medicine physician could not acknowledge that she had prescribed a migraine medication to a patient, because this information would reveal that the person is receiving SUD treatment. This example is included in a helpful document for determining whether Part 2 applies, released by the Office of the National Coordinator for Health Information Technology and the Substance Abuse and Mental Health Services Administration. Conversely, a primary care physician who only occasionally provides SUD treatment would not be covered by Part 2 but would still need to comply with HIPAA regarding SUD treatment information, as noted in the same publication.

Part 2 has far fewer provisions for sharing information without a patient's consent than HIPAA does. In the case of a medical emergency, the program may release patient identifying information (for example, name, address, or photograph) but *not* information about diagnosis or treatment (42 CFR § 2.51). This exception applies to disclosures to medical personnel, such as EMTs, but not to law enforcement. The program must keep detailed records of this disclosure.

Without a court order or patient consent, the circumstances under which a Part 2 program may provide information to law enforcement are strictly limited (42 CFR § 2.12). First, if a crime is committed on the premises of the program or against its staff, the program may release information to law enforcement about the incident, confirm that the person is a patient, and provide the person's name, address, and last known whereabouts. Second, if the program suspects child abuse or neglect, they may report it to law enforcement. In neither case may the program disclose treatment records without consent or a court order.

Part 2 has strict requirements for releasing information under a court order (42 CFR § 2.65). The court may order disclosure only for investigation of violent crimes and only if disclosure is absolutely necessary. The court must also limit what is disclosed and how the records will be used. Another way that Part 2 is stricter than HIPAA is that the restrictions "follow" the information. In other words, if a Part 2 program shares information with a health care provider, insurer, or someone else who is not a Part 2 program, then that other entity is subject to Part 2. Additionally, Part 2 programs are required to include a notice that the information is restricted by Part 2.

CCMU teams should assume they are covered by Part 2 if they provide a significant percentage of SUD services, include SUD professionals, or are associated with an SUD treatment provider. If there is any doubt, it is safer to assume coverage by Part 2 or seek a legal opinion.

If the CCMU team is certain that it is not covered by Part 2, then it should still follow the HIPAA Privacy Rule regarding the disclosure of SUD diagnoses and treatment to law enforcement.

If the CCMU team is (or might be) a Part 2 program, then the team should strictly limit any disclosure to law enforcement that would suggest that any individual has a past or present SUD. The limited exceptions would be for crimes on program premises, crimes against a team member, or child abuse and neglect. Otherwise, law enforcement should be required to provide a very specific court order, and the CCMU team has the right to have a hearing to determine whether the request is valid.

ILLUSTRATIONS

The following scenarios illustrate some of the situations where law enforcement might ask for PHI or personally identifying information about an individual served by the CCMU team. In each scenario, assume the individual has not signed a consent form.

SCENARIO 1

The CCMU team knows that John has schizophrenia and sometimes threatens people when he has not been taking his medication. After responding to a dispatch about a man screaming threats at people entering and leaving a coffee shop, the team encounters John, who by then is carrying a broken bottle and talking about cutting someone's throat. The team is unable to de-escalate and determines they need law enforcement support.

HIPAA Analysis: John's diagnosis, his history of threatening behavior, and his inconsistent use of medication are all PHI covered by HIPAA. However, the situation involves a serious and imminent threat to the public and therefore would fall under an exception to the HIPAA Privacy Rule. Explaining the medical situation could help divert John from jail to treatment, but the team should provide no more information than necessary. For example, there is probably no reason to reveal his specific diagnosis or his medication history, and instead explain he requires emergency psychiatric care.

Part 2 Analysis: Unless the team reporting the information primarily addresses substance use crises, Part 2 probably does not apply, even if John also has a history of SUD. Releasing information that John is experiencing a mental health crisis would not identify him as a person who has received treatment for an SUD. If the team primarily addresses SUD crises, then Part 2 might limit the team's ability to acknowledge that they are familiar with his medical history. They could protect themselves by simply calling in a report of an unidentified person making threats and providing a detailed description of John.

SCENARIO 2

Sheriff's deputies respond to a report of a scuffle at a "tent city," and find an unconscious woman. It's not clear whether she was injured in the scuffle or for some other reason. As the deputies wait for emergency medical personnel to arrive, they determine from others that the woman's first name is Jane, and she has a distinctive tattoo on her neck. A deputy contacts the CCMU team to find out whether the team knows her full name, whether she has any medical conditions the EMTs should know about, whether she could have overdosed, and whether she has any relatives who should be contacted.

HIPAA Analysis: Revealing Jane's last name and emergency contact information indicates that she is known to a behavioral health treatment team, and thus is protected. However, if the purpose is to connect her to someone responsible for her care, then it would fall under an exception to the HIPAA Privacy Rule. Jane's medical history and history of substance use (if any) are PHI. If the deputies are trying to determine whether Jane is unconscious as the result of the assault or for another reason, then the exception for investigating crimes would apply. Alternatively, if the team believes that Jane may be experiencing intimate partner violence, they could disclose this information under the exception covering abuse, neglect, and domestic violence. If the deputies are trying to get a warrant to search Jane's tent for drugs, however, then disclosure of past drug use would violate HIPAA.

Part 2 Analysis: If the CCMU team is considered a Part 2 program, then acknowledging that the team had interacted with Jane would reveal a history of SUD treatment, and disclosure of any information to the deputies would likely violate Part 2. Neither the exception for crimes against program staff nor the exception for child abuse and neglect applies. The medical emergency exception would not apply, as the deputies are not medical personnel. However, the CCMU team could reveal information to the EMTs when they arrive, as they are medical personnel.

SCENARIO 3

Paul, who has bipolar disorder and currently has a strong smell of alcohol on his breath, punches a CCMU team member, injuring her. The other team member calls 911, and the responding officer asks for as much information as possible about Paul.

HIPAA Analysis: Despite the unfortunate situation, Paul still has HIPAA rights. Because this is a crime against program staff, an exception to the HIPAA Privacy Rule applies. The CCMU team may therefore provide information necessary to finding him, such as name, address, age, gender, appearance, etc. They may also note that he appeared to be intoxicated at the time of the assault, as this information is relevant to the incident. Informing the officer about his bipolar disorder diagnosis, however, would most likely violate the HIPAA Privacy Rule.

Part 2 Analysis: If the CCMU team is considered a Part 2 program, then acknowledging that the team had interacted with Paul would reveal a history of SUD treatment, and thus disclosure of information to the police would be covered by Part 2. Because the exception for a crime against program staff applies, they could provide a description of Paul, along with his name, address, and last known

whereabouts, regardless of whether the team is considered a Part 2 entity. The team probably also could reveal that Paul appeared intoxicated at the time of the assault, as it is a description of the incident, rather than an indicator of SUD. However, if the team is considered a Part 2 entity, they would not be able to reveal any details of his treatment history, even if it helps to explain his behavior.

SCENARIO 4

Deputies book Sally into the county jail after they arrest her for shoplifting from a liquor store. Believing her to be experiencing homelessness, they ask the CCMU team whether they have any information about her history of mental illness or SUD.

HIPAA Analysis: The HIPAA Privacy Rule specifically allows the sharing of information with law enforcement for the purposes of providing or continuing care within a correctional institution. If the deputies say they need this information for this purpose, then it probably can be shared without consent without violating the privacy rule. However, it would be wiser to ask that the jail's medical personnel contact them directly, unless there is an urgent need for immediate treatment (e.g., to initiate medically supervised withdrawal).

Part 2 Analysis: If the CCMU team is considered a Part 2 program, then it would not be allowed to share information about Sally unless she has consented to sharing information. It does not appear that Sally requires emergency treatment.

Resource List

HIPAA Administrative Simplification: Regulation Text, U.S. Department of Health and Human Services (2013).

HIPAA Helps Caregiving Connections, U.S. Department of Health and Human Services Office of Civil Rights (n.d.)

Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule: A Guide for Law Enforcement,
U.S. Departments of Justice and Health and Human Services (2004).

Sharing Behavioral Health Information: Tips and Strategies for Police-Mental Health Collaborations, Council of State Governments Justice Center (2019).

An Imaginary Barrier: How HIPAA Promotes Bidirectional Patient Data Exchange with Emergency Medical Services, National EMS Information System Technical Assistance Center (2020).

Confidentiality of Substance Use Disorder Patient Records (42 CFR Part 2), U.S. Department of Health and Human Services (2017).

Disclosure of Substance Use Disorder Patient Records: Does Part 2 Apply to Me?, Office of the National Coordinator for Health Information Technology and Substance Abuse and Mental Health Services Administration (n.d.).