Sharing Sensitive Health Information

Provider Discussion Document

Revised July 2021

This document is intended for informational purposes only. The content is not guaranteed to be accurate, does not constitute legal advice, and cannot be relied upon to comply with federal, state, or local regulations.

For informational purposes only

Contents

1. Purpose of This Document

Healthcare providers appreciate the value of sharing their patients' mental health, substance use, and other sensitive health information to support better, safer, more comprehensive care. However, federal and state laws that place special restrictions on sharing this information pose challenges. Complex restrictions may give rise to differences in interpretation by providers. This may in turn make providers reluctant to take on the risks of information-sharing. The purpose of this document is to provide a starting point for overcoming these challenges and developing a common understanding of benefits and risks.

It can be difficult for different types of providers to understand the kind of patient information each needs from the other, why it is needed, and what restrictions may apply. This document seeks to identify obstacles to information-sharing and reduce challenges by providing a starting point for mutual understanding, as well as resources for further discussion.

The document was originally developed in the fall of 2016 by a group of 15 behavioral health and medical provider organizations in Massachusetts. It was revised in 2021 by a group representing 12 healthcare organizations. It is targeted to providers who are considering, planning, or already engaged in sharing sensitive health information. The original 2016 group developed other related documents, including materials for patients and administrators.

This document addresses the following:

- Information-sharing among providers, including both sensitive and non-sensitive patient information.
- Information-sharing among providers for the purpose of treatment. It does not address sharing with employers, insurance companies, regulatory agencies, or any other non-provider entity, or for purposes other than treatment.
- Information-sharing within Massachusetts. The document does not address requirements in other states.

This document does not provide legal advice. Any individual or organization that uses this document must put in place its own practices, obtain legal review, and make sure the information in the document is consistent with internal policies and procedures.

2. Benefits of Sharing Patient Information

Sharing patient information can result in safer, better, faster, and more comprehensive care for the patient. It can help providers to:

- Focus time on the patient's clinical needs rather than information collection.
- Take into account current and past diagnoses, treatments, and outcomes not reported by the patient and caregivers.
- Reduce the risk of error resulting from lack of important information.
- Reduce delays in providing care when information is needed from another provider.
- Reduce costs associated with redundant tests and treatments.
- Better understand the patient's health needs and special circumstances.

These factors and others can positively influence both outcomes and patient satisfaction.

3. Obtaining and Communicating Patient Consent

The Privacy Rule of the Health Insurance Portability and Accountability Act (HIPAA) permits sharing of most patient information without patient consent for the purposes of treatment, payment, and operations. However, other federal and state laws impose a variety of additional requirements to obtain verbal and/or written consent to share "sensitive" information. These laws introduce variations on when consent must be obtained, when it expires, exceptions when the consent requirements do not apply, what a written consent form must include, and whether consent is required to redisclose information.

This section discusses approaches to consider for obtaining and communicating patient consent to help reduce the complexity and risk of information-sharing.

- **Consider how to discuss with patients the benefits of sharing their medical information among their providers.**

  See Section 2, "Benefits of Sharing Patient Information," for a list of potential benefits.

- **Consider obtaining patient consent for information-sharing even when it may not be legally required.**

  Some providers may believe that obtaining patient consent is not legally required for them and therefore unnecessary. For example, some medical providers may believe that HIPAA exempts them from obtaining patient consent, even though the records they share may contain sensitive information. In fact, these providers may be in violation of policies and regulations other than HIPAA that impose additional requirements on sharing sensitive information.

Providers may believe that obtaining consent from all patients is too cumbersome. However, if their current procedures require their staff to make decisions on when to get patient consent, for what types of information, and in what form, they may be able to simplify procedures and reduce the risk of inappropriate sharing by always requesting consent.

Providers should consider obtaining written patient consent for all information-sharing in a form that includes consent for sensitive information they may need to disclose. Many providers are moving in this direction.

- **Consider using a single patient consent form that covers requirements for sharing all types of patient information. The form might include the following:**

  - The purpose of the disclosure—to allow providers to communicate about the patient in order to evaluate needs, provide services, and coordinate care.

  - The types of information that may be requested, received, or provided.

  - The option to exclude sharing of certain types of information.

  - A statement to inform the patient that the provider may be allowed to exchange information without the patient's consent where permitted or required by law, including common examples.

  - The individual and/or organizational healthcare providers who may provide or receive information, including a general designation allowing exchange of information between any of the patient's treating providers.

  - A statement that the patient's decision to give or deny consent will not affect their right to receive care or benefits and will not affect the cost of their care.

  - A statement to inform the patient of methods of information exchange that may be used.

  - The option to give or deny consent.

  - A statement that the patient may withdraw consent at any time, and instructions on how to do so.

  - The date, condition, or event on which the consent will expire.

  All providers should consult their legal advisors about their consent form.

- **Consider how to address informing patients that their information may sometimes be shared without their consent according to law.**

  When requesting patient consent for information-sharing, providers may wish to inform patients that there are situations in which their information may be shared without consent, including but not limited to: in medical emergencies, with health insurers to obtain payment, with public health agencies, and upon certain requests from law enforcement. Providers should consider each patient's specific situation when discussing the conditions under which information may be shared without consent. For some patients, drawing attention to this issue may cause undue concern and disrupt the patient's trust in the healthcare organization.

- **Consider having a separate appointment for new patient onboarding and having designated staff who assist patients with consent forms and other paperwork.**

  Providers may want to schedule an onboarding visit for new patients, in which a trained staff person can review consent forms and any other paperwork. Setting aside a separate time for patients to review consent forms may help patients better understand how their sensitive health information may be shared, as well as the potential benefits of more coordinated care.

- **Consider using the same or similar consent form across frequent healthcare partners.**

  Providers are sometimes unfamiliar with the policies and procedures of their care partners and as a result can be reluctant to share information for fear that it may be handled improperly. If a network of provider organizations adopts the same or similar forms, they may reduce the uncertainty of whether each provider's procedures and forms are adequate.

- **Consider communicating that patient consent has been obtained when requesting or providing patient information.**

  To enhance the receiving provider's confidence in the appropriateness of the information-sharing, providers may wish to always communicate to the other provider that patient consent has been obtained. For example, providers may agree on a statement to be included with a request for information or a transmission of information. Or they might choose to transmit the signed patient consent form itself along with the request or the information.

Making communication of patient consent part of the organization's procedures will help to satisfy the receiving provider's requirement for evidence of consent and may expedite care.

- **Consider the needs of the receiving provider.**

  The amount and type of information needed will vary by receiving provider. In many cases, the receiving provider may not need all of the patient's information. Consider what is relevant to the receiving provider's specialty and the care they are providing. At the same time, providers should also ensure that they are not actively restricting appropriate, authorized information-sharing.

- **Consider your organization's policies and procedures for not sharing information when a patient has denied consent or not explicitly provided consent.**

  If the provider organization requests consent from all patients, it is possible that some patients will refuse, while others may take no action. Also, a previous consent may have expired. Providers should consider procedures to allow or avoid information-sharing based on the patient's consent status. These procedures should address both manual and electronic means of information-sharing.

  Provider organizations should make sure that patients understand both the benefits and risks of allowing or not allowing their information to be shared. Providers should consider their procedures for addressing patient concerns, such as a separate patient onboarding visit with a staff person trained in patient consent policies and procedures, and further discussion with the patient's clinician when warranted.

- **Consider your policy regarding providing information in emergencies.**

  Providers should consider adopting a policy regarding whether and how they will provide information in medical emergencies if patient consent is not in place.

- **For providers subject to 42 CFR Part 2, consider your policies and communications regarding redisclosure.**

  Federal Regulation 42 CFR Part 2 specifies certain policies about redisclosing substance use disorder information, and the CARES Act further refines these policies. Please see the Substance Abuse Confidentiality Regulations section of the Substance Abuse and Mental Health Services Administration (SAMHSA) website for more information. As of July 2021, SAMHSA has not yet issued a Notice of Proposed Rule-Making (NPRM) related to the changes required by the CARES Act. See the SAMHSA statement here.

4. How Sensitive Information-Sharing is Different from HIPAA-Compliant Sharing

The federal HIPAA Privacy Rule (HIPAA) places few restrictions on sharing of patient information between providers for treatment. HIPAA considers most patient information to be "protected health information (PHI)" and most providers to be "covered entities." HIPAA permits covered entities to use and disclose PHI for treatment without the patient's authorization.

For the most part, HIPAA does not distinguish between general medical information and other more sensitive types of information. One exception to this general rule is psychotherapy notes. See Appendix A, "HIPAA Protections regarding Psychotherapy Notes," for these restrictions.

Medical providers are accustomed to the rules of patient information-sharing under HIPAA. Providers may also be familiar with Massachusetts protections for sensitive medical information such as HIV/AIDs and genetics. However, they may not be familiar with special restrictions imposed by federal and state laws on sharing behavioral health information, substance use disorder information, and other sensitive health information. The following summarizes these additional rules in very general terms.

- **Federal and Massachusetts laws may impose special privacy protections beyond HIPAA on behalf of mental health and substance use patients, for whom disclosure may have the potential to cause social, psychological, economic harm (e.g., employment discrimination), or stigmatization.** Behavioral health and substance use disorder providers should consider relevant federal and Massachusetts restrictions before sharing a patient's behavioral health and/or substance use disorder information with any other provider.

For more information on federal regulations, please see Appendix B, "Federal Regulation 42 CFR Part 2." For more information on relevant Massachusetts law, visit the "Massachusetts Law about Medical Privacy" and the "Massachusetts Law about Mental Health Issues" pages on the mass.gov website.

5. Defining, Storing, and Managing Sensitive Information

Providers should consider that the definition of "sensitive health information" may vary from patient to patient, and even from provider to provider. While there are federal and state regulations surrounding the sharing of behavioral health information, substance use disorder information, and the results of certain types of testing, there may be other types of information that a particular patient may consider sensitive.

Current capabilities of EHRs and other systems that store sensitive information also pose challenges for the provider. Consider that some of these systems:

- May not be able to capture or enforce the patient's consent instructions.
- May not be able to segregate sensitive information from general medical information.
- May not allow the provider to choose which information to share.
- May be limited by the format of the information (CCDA, pdf, etc.)

Providers should consider that since regulations may vary from state to state, and many EHR vendors operate across state lines, it may be difficult to automate data segregation and electronically capture the nuances of patient consent.

Providers usually reject "workarounds." For example:

- Maintaining sensitive information separate from the EHR compromises the reliability of the patient's primary medical record.
- Manually "scrubbing out" sensitive information before sharing the patient's record is often too cumbersome.

In the future, some EHR systems may allow providers to designate certain information as sensitive even if there is no law or regulation restricting the sharing of that information. As the capabilities of EHRs mature, it may be possible to record the patient's preferences in more detail and electronically suppress certain types of sensitive information. In the meantime, providers may wish to consider obtaining patient consent to share all information, including sensitive information, as well as the potential disadvantages of such an "all or nothing" approach.

6. Methods and Risks of Sharing Sensitive Information

How providers exchange patient information depends on their systems capabilities, their organization's policies, the format of the information, and sometimes the preferences of the providers. The method of exchange sometimes defaults to the least technically advanced method with the lowest perceived risk.

Some providers may believe information is more secure on paper and/or transmitted via fax than stored in a system or transmitted electronically from one system to another. These beliefs may be influenced by lack of familiarity with technical safeguards as well as reports of "hacking" and information theft. **The reality is that information in electronic form is usually just as secure, or in many cases even more secure, than paper or fax.** Consider that:

- **Systems that have patient information in them require IDs and passwords** before they allow people to see the private information, restricting access to only the people who have a right to see it. The information is also often encrypted.

- **Information transmitted electronically between systems must be sent via highly secure communication channels and must be encrypted.**

There are federal and state laws all providers must follow to make sure of this security. Unfortunately, information can never really be 100% secure whether it is on paper, faxed, sent over the internet, or in a system, but awareness of cybersecurity is a priority for many organizations. An objective understanding of risks and mitigations will help to improve mutual trust among providers and improve overall confidence in secure patient information exchange. For more information about cybersecurity issues, visit the Mass Cyber Center website.

7. Consequences of Unauthorized Sharing

Certain types of legal recourse are available to regulatory authorities and patients in the event of improper disclosures of protected information. Penalties can include fines and even criminal charges. For discussion purposes, the following briefly summarizes a few examples:

- In the event of HIPAA or HITECH privacy/security violations, the provider or organization could be subject to substantial administrative fines.

- Patients can file various types of complaints and lawsuits, including but not limited to:

    - Complaints with regulatory agencies like the federal Office for Civil Rights (OCR) of the Department of Health and Human Services (HHS) for improper disclosures under HIPAA.
    - Complaints with the Massachusetts Attorney General.
    - Complaints with state licensing boards.
    - Grievances or reports with third-party payers, such as Medicare or the VA.
    - Breach of privacy lawsuits against individuals or organizations.

Fear of such actions, and fear of adverse impact on patient and provider relations, can make providers reluctant to share patient information. Some considerations to mitigate this fear include:

- Understanding that all providers are subject to the same rules. All providers must have the same kinds of strict procedures to protect patient privacy, monitor access to patient information, and impose penalties for violations.

- Careful consideration of your organization's policies for ensuring that appropriate data-sharing agreements defining mutual responsibilities are in place and kept up to date.

- Familiarity with the information security procedures and practices of other providers with whom sensitive information is shared, in order to convey confidence to your staff and patients.

- Communication with patients about the rules surrounding information-sharing. Consider how to best convey to patients the procedures your organization has in place for protecting patient privacy and preventing breaches, as well as the recourse available to patients when they believe their information has been shared inappropriately. See the model Notice of Privacy Practices provided by the U.S. Department of Health and Human Services (HHS).

Appendix A. HIPAA Protections regarding Psychotherapy Notes

HIPAA requires a provider to obtain patient consent to disclose psychotherapy notes but defines such notes in a narrow sense. Psychotherapy notes are defined as: "notes recorded by a health care provider who is a mental health professional documenting or analyzing the contents of a conversation during a private counseling session or a group, joint, or family counseling session and that are separate from the rest of the patient's medical record." [1]

For more information, please see the Health Information Privacy page on the U.S. Department of Health and Human Services (HHS) website.

1 - https://www.hhs.gov/sites/default/files//hipaa-privacy-rule-and-sharing-info-related-to-mental-health.pdf

Appendix B. Federal Regulation 42 CFR Part 2

The privacy provisions of federal regulation 42 CFR Part 2 place special restrictions on sharing information about substance use disorder and treatment.

The following discussion describes the regulations in general terms. This document does not provide legal advice. It attempts to provide the basis for a common understanding among providers who may need to exchange substance use disorder information. Please see the Substance Abuse Confidentiality Regulations section of the SAMHSA website for more detailed information.

- The regulations apply only to federally-assisted substance use disorder programs. It is important to note that a program must meet BOTH of the following aspects of the definition in order to be subject to 42 CFR Part 2.

  - **The program must hold itself out as providing, and actually provide, substance use disorder diagnosis, treatment, or referral for treatment.** [2]

    AND

  - **The program must receive federal assistance.** Federal assistance is defined broadly enough that most substance use disorder programs meet this qualification. For instance, **programs are considered "federally assisted" if they are authorized, licensed, certified, or registered by the federal government, or if they receive federal funds in any form**.[2]

    Note that 42 CFR Part 2 does not apply to general medical providers or to settings providing a mix of healthcare services, even if the mix of services includes substance use disorder services. Some examples of entities and programs that may not be subject to 42 CFR Part 2 include:

    - General medical facilities, including but not limited to Federally Qualified Health Centers (FQHCs)
    - General emergency rooms
    - General inpatient facilities
    - General mental health facilities
    - Primary care practices treating patients who are opioid-dependent, as long as the care of these patients is delivered as part of the general primary care practice and NOT in a dedicated substance use disorder treatment unit

2 – 42 C.F.R. § 2.11; see also: SAMSHA FAQs at https://www.samhsa.gov/sites/default/files/faqs-applying-confidentiality-regulations-to-hie.pdf

- The regulations require the provider to obtain written patient consent to disclose information. The consent must include certain information, including but not limited to: who the patient is, the program that is releasing the information, the recipient(s) of the information, the reason for the disclosure, and the date or event on which the consent expires.

- The regulations currently require each disclosure that is made *with patient consent* to include a statement notifying the recipient that redisclosure is not permitted. In order to redisclose the information, the recipient would also need to obtain patient consent. Please note that as of July 2021, SAMHSA has not yet issued a Notice of Proposed Rule-Making (NPRM) related to the changes required by the CARES Act, which include updated regulations about redisclosure. See the SAMHSA statement here.

- The regulations permit initial disclosure or redisclosure of information *without patient consent* under certain circumstances. Some examples may include when there is an immediate threat to the health of any individual and immediate medical intervention is required, certain notifications to law enforcement, some notifications to state or local authorities, and court-ordered disclosures. In the case of a medical emergency, the disclosing organization is required to determine the existence of a medical emergency and document the disclosure in the patient's record.