**Behavioral Health Information Sharing**

**Administrator FAQs**

Contents

[1. Purpose of This Document 2](#_Toc472413535)

[2. What is Health Information Exchange? 2](#_Toc472413536)

[2.1. What is health information? 2](#_Toc472413537)

[2.2. How is behavioral health information different? 3](#_Toc472413538)

[2.3. Where does health information reside? 4](#_Toc472413539)

[2.4. What is health information exchange? 4](#_Toc472413540)

[2.5. What is an HIE? 5](#_Toc472413541)

[2.6. How does the Massachusetts Health Information Highway (the Mass HIway) work? 6](#_Toc472413542)

[3. What do I need to know about patient privacy? 7](#_Toc472413543)

[3.1. What is “patient consent”? 7](#_Toc472413544)

[3.2. What is the Health Insurance Portability and Accountability Act (HIPAA)? 7](#_Toc472413545)

[3.3. What is the HIPAA Privacy Rule? 5 8](#_Toc472413546)

[3.4. What is the Health Information Technology for Economic and Clinical Health Act (HITECH)? 10](#_Toc472413547)

[3.5. What is “sensitive information”? 10](#_Toc472413548)

[3.6. What is Federal Regulation 42 CFR Part 2? 11](#_Toc472413549)

[3.7. What Massachusetts laws pertain to patient privacy? 10 13](#_Toc472413550)

[3.8. In what circumstances may patient information be shared without patient consent? 15](#_Toc472413551)

[4. How do EHRs help to protect patient privacy? 15](#_Toc472413552)

[4.1. How do EHRs send and receive patient information? 15](#_Toc472413553)

[4.2. How do EHRs protect the privacy of the information they send and receive? 16](#_Toc472413554)

[4.3. How do EHRs handle patient consent and sensitive information? 17](#_Toc472413555)

[5. What are my responsibilities for protecting patient privacy? 18](#_Toc472413556)

[5.1. What privacy policies do provider organizations have? 18](#_Toc472413557)

[5.2. How are the policies enforced? 19](#_Toc472413558)

[5.3. What are the consequences of privacy violations? 19](#_Toc472413559)

[6. What kinds of agreements support Health Information Exchange? 20](#_Toc472413560)

[6.1. What is a Business Associate Agreement (BAA)? 20](#_Toc472413561)

[6.2. What is an HIE agreement? 20](#_Toc472413562)

[6.3. What are service agreements and data sharing agreements? 21](#_Toc472413563)

[6.4. What is a Qualified Service Organization Agreement (QSOA)? 21](#_Toc472413564)

[7. Where can I find more information? 21](#_Toc472413565)

[Appendix A. References 22](#_Toc472413566)

Purpose of This Document

This document is intended to provide Administrators and other Management Staff at healthcare provider organizations with a general understanding of:

* How patient health information is exchanged among providers.
* The privacy and confidentiality protections patients have when information is exchanged, particularly behavioral health information.

This document provides general information, not legal advice. Further information about topics in this document can be obtained from the documents cited in Appendix A, “References”.

What is Health Information Exchange?

What is health information?

Health information includes any information about a patient that is known to a healthcare provider or is recorded in a provider’s physical environment (e.g., paper copies of information) or in computer systems. It includes, but is not limited to:

* Identifying information about a patient, such as name, date of birth, address, phone number, and medical record number.
* Medical information about a patient, including problems and diagnoses, medications and allergies, visit summaries, tests and results, notes, histories, insurance claims and payments, and other pertinent information.

Health information is often referred to as Protected Health Information (PHI) because all patient information is considered private and protected under the Health Insurance Portability and Accountability Act (HIPAA). HIPAA identifies the many types of protected information and authorizes disclosure of PHI only for certain purposes, including treatment, payment, and operations. Providers must be careful to disclose PHI only when permitted by HIPAA. See Section 3.2, “What is the Health Insurance Portability and Accountability Act (HIPAA)?” for more information on HIPAA.

Other federal and state laws impose additional restrictions on what types of information may be disclosed and under what circumstances. Many of these laws pertain to behavioral health information. This topic is discussed in more detail in Section 3, “What do I need to know about patient privacy?”

How is behavioral health information different?

Behavioral health information is a subset of general medical information. This subset is generally understood to include two kinds of medical information:

* Mental health information.
* Substance use disorder information.

For both types, pertinent information may include anything that describes or refers to a patient or the patient’s mental health or substance use disorder status or treatment, including but not limited to:

* Which individuals or organizations provide assessment, referral, consultation, or treatment.
* Diagnoses and problems.
* Medications and allergies.
* Visit summaries.
* Tests and results.
* Notes.
* Histories.
* Insurance claims and payments.

As noted above, the privacy and confidentiality of behavioral health information is subject to stricter protections under federal and state law than some other types of medical information. This topic is discussed in more detail in Section 3, “What do I need to know about patient privacy?”

When discussing behavioral health care and behavioral health information, it is important to consider the level at which behavioral health care and medical care are integrated.

* Integrated care delivery. In an integrated care delivery system, providers work together in close communication and collaboration to deliver diagnosis, treatment, rehabilitation, and social services. Providers may deliver a variety of services within the same organization or across multiple collaborating organizations. Integrated care delivery relies on comprehensive communication about a patient among treating providers.
* Non-integrated care delivery. Currently, healthcare may be delivered in a less integrated way, where providers may communicate with one another about a patient but rely less heavily on developing a comprehensive, continuous understanding of the patient.

Where does health information reside?

In addition to being “known” to a patient’s providers, health information is stored in a number of forms and formats. It may exist on paper in the provider’s files, or it may be stored in a variety of electronic media.

Nearly all providers in Massachusetts have adopted Electronic Health Record systems (EHRs). Most of their patients’ medical information is stored electronically in these systems. Most providers also have other computer systems that store patient information, such as billing systems and various types of centralized or distributed databases. All patient information, whether it is maintained centrally or remotely on laptops, tablets, phones, CDs/DVDs, thumb drives, or other devices, is subject to federal and state privacy and confidentiality laws.

What is health information exchange?

Healthcare organizations exchange patient information in many ways, for example, by telephone, fax, secure email, and postal mail.

The term “Health Information Exchange” usually refers to health information that is moving electronically from a system in one organization to a system in another organization. The following are three examples of electronic Health Information Exchange:

* A hospital that uses Cerner’s EHR may send electronic patient information to a primary care practice that uses eClinicalWorks’s EHR.
* A practice that uses Epic’s EHR may send electronic patient information to an unaffiliated specialty practice that uses a separate instance of Epic’s EHR.
* A practice may use its EHR to send electronic immunization records to a state immunization registry.

When affiliated providers directly access the same EHR system, the access is usually not referred to as “Health Information Exchange”. For example, if a hospital and its affiliated practices all use the same instance of Epic, they can all view information in the same EHR, and this is not considered “Health Information Exchange”.

What is an HIE?

A Health Information Exchange (HIE) is an organization that facilitates communication of patient information among organizations and people who are involved in providing healthcare.

Most HIEs facilitate moving health information electronically from one organization to one or more other organizations. For example, the HIE may provide an electronic network that allows a provider organization to securely send a patient’s information to another provider organization, to an insurance company responsible for paying the patient’s insurance claims, or to a government agency that collects public health information.

Since HIEs usually require their member organizations to send and receive information using standardized methods and formats, HIEs often “connect” provider systems to each other by routing electronic documents in standard formats. Some examples are:

* ABC Practice may wish to send an electronic summary of a patient’s health to XYZ Practice. To do this, ABC Practice may use its EHR to create and send a standard “Continuity of Care Document (CCD)” via the HIE network. This kind of standard electronic document contains identifying information about the patient as well as problems and diagnoses, medications and allergies, visit summaries, tests and results, notes, histories, and other pertinent information.
* ABC Practice may wish to request information from XYZ Hospital. To do this, ABC Practice may send an electronic request to XYZ Hospital via the HIE network. If XYZ Hospital has information about the patient, they may send back an electronic “Continuity of Care Document” as described above.
* ABC Practice may be required to send immunization records to the Massachusetts Department of Public Health (DPH). To do this, ABC Practice will send a standard “Immunization Record” to the DPH’s immunization recordkeeping system via the HIE network. Massachusetts’s immunization recordkeeping system is called the Massachusetts Immunization Information System (MIIS).

HIEs may exist at any level. The following are examples of HIEs that operate at a state level, a private network level, and a regional level:

* The state of Massachusetts operates an HIE that offers services to any organization involved in providing healthcare in Massachusetts. This state-level HIE is called the Massachusetts Health Information Highway (Mass HIway). Many healthcare organizations in Massachusetts use the Mass HIway to exchange patient information.
* An Accountable Care Organization (ACO) may operate a “private” HIE that facilitates Health Information Exchange among some or all of its affiliated providers. In such a model, the ACO may require the use of standardized software and electronic message formats to send and receive electronic information among a variety of systems within the ACO network.
* A group of unaffiliated provider organizations may join together to operate a “regional” HIE to serve the patients in a shared geographical area. In such a model, the organizations may collaborate to adopt governance models and standardized software or message formats to facilitate electronic information exchange. For example, this model could be used to “connect” one or more “anchor” acute care hospitals with unaffiliated practices and long-term care facilities in the region.

How does the Massachusetts Health Information Highway (the Mass HIway) work?

The Mass HIway is the state-level HIE in Massachusetts. It currently provides three ways to exchange information:

* “Webmail” messaging. This is a service similar to secure email. Individual healthcare providers and healthcare organizations can register with the state to participate in this service. Once verified and registered, they can send and receive secure email messages and attachments with other providers both in and beyond Massachusetts.
* “Direct” messaging. Healthcare organizations can register with the state to participate in this service. Once verified and registered, they can send information about a patient electronically to another healthcare organization or public health agency that also uses the Mass HIway.
* “LAND” messaging. Healthcare organizations can register with the state to participate in this service. The service is similar to “direct” messaging except that the Mass HIway provides the healthcare organization with a device that stores incoming messages for the provider and stores and periodically forwards outgoing messages from the provider.

Patients have the right to “opt in” or “opt out” of having their information exchanged using the Mass HIway. If the patient wishes to allow his or her provider to send information via the Mass HIway, the patient signs a form (either an electronic form or a hard copy form) to “opt in”. This gives that provider permission to send out information. The patient must “opt in” with every provider to whom the patient wishes to give such permission. The patient can later “opt out” by signing another form that withdraws permission for information sharing.

The state of Massachusetts is currently considering relaxing the “opt in” requirement. In the future, providers may only need to inform the patient about the Mass HIway rather than obtain an explicit “opt in”.

In a later phase, the Mass HIway will provide the capability for registered entities to request and receive information about a patient. When this phase is implemented, the provider will be able to use the Mass HIway Relationship Listing Service to determine where a patient has received care and request information from those other provider(s). The patient will have the ability to opt in or opt out for this type of information exchange also.

What do I need to know about patient privacy?

What is “patient consent”?

“Patient consent” and “patient authorization” are terms used to describe a patient’s instructions regarding whether a healthcare provider or other organization may provide the patient’s medical information to others.1

There are a variety of laws governing the circumstances in which a healthcare provider may release a patient’s information without the patient’s consent. There are also a variety of laws regarding when a patient’s consent is required, and in what form (e.g., verbally or in writing, in a specific format), before a provider may release the patient’s information. Some of these laws are described in this section.

What is the Health Insurance Portability and Accountability Act (HIPAA)?

HIPAA is a federal law passed in 1996 that addresses the following:

* Provides the ability to transfer and continue health insurance coverage for some American workers and their families when they change or lose their jobs.
* Reduces health care fraud and abuse.
* Mandates industry-wide standards for health care information on electronic billing and other processes.
* Requires the protection and confidential handling of protected health information.

Under HIPAA, “covered entities” are organizations or corporations that directly handle PHI, such as hospitals, doctors’ offices, and health insurers. Covered entities are required to protect PHI in accordance with HIPAA guidelines. 2

Covered entities often work with “business associates”, which are organizations or persons who work with or provide services to the covered entity involving handling or disclosing PHI.3

It should be noted that some healthcare organizations are not subject to HIPAA. For example, if a healthcare organization does not use electronic transactions that are governed by HIPAA, the organization is not subject to HIPAA. 4

What is the HIPAA Privacy Rule? 5

The rule that addresses the privacy and confidentiality of Protected Health Information (PHI) is called the HIPAA Privacy Rule. The HIPAA Privacy Rule identifies the many types of protected information and authorizes disclosure without patient consent only for certain purposes, including treatment, payment, and operations.

|  |
| --- |
| ***Note: The HIPAA Privacy rule actually places few restrictions on sharing of patient information between providers without patient consent when the purpose is treatment. Also, HIPAA generally does not distinguish between general medical information and other more sensitive types of information, such as behavioral health and HIV/AIDS information. See the following paragraphs for more information on protections that may be imposed for sensitive information by other federal and state laws.*** |

One type of information that is actually restricted by the HIPAA Privacy Rule is psychotherapy notes. HIPAA requires a provider to obtain patient consent to disclose psychotherapy notes but defines such notes in a narrow sense. To require patient consent for disclosure, the notes must meet three tests: be prepared by a mental health professional, document or analyze the results of a counseling session, and be maintained separately from the rest of the patient’s medical record.

Not all notes that are written by licensed mental health professionals are psychotherapy notes. In many settings, licensed mental health professionals will write Behavioral Health Progress Notes. Progress Notes are notes that are kept as part of the medical record. Progress Notes include session start and stop times, medication details, modalities and frequencies of treatment, diagnoses, functional status, symptoms, prognosis, and progress to date. Behavioral Health Progress Notes are considered part of the medical record and under HIPAA are treated like other notes in the medical record, even if they are written by a licensed mental health professional.

In the event that a provider is required to obtain patient consent under HIPAA (e.g., if the purpose of the information exchange is other than treatment), the authorization must be obtained in writing and include specific elements such as a description of the information to be disclosed, who is making the disclosure, who is receiving the information, the purpose, an expiration date or event, the date of the authorization, and a signature by the patient or authorized representative. 6

Providers must be aware that although HIPAA permits most sharing among them for treatment purposes without patient consent, there are a variety of other federal and state laws that may impose protections over and above HIPAA. Providers may be in violation of laws other than HIPAA if the records they share contain types of information that are subject to additional restrictions, such as treatment of a substance use disorder in a 42 CFR part 2 covered program, HIV/AIDS, or genetic information. Some of these additional restrictions are discussed in the following sections:

* Section 3.5, “What is ‘sensitive information’?”
* Section 3.6, “What is Federal Regulation 42 CFR Part 2?”
* Section 3.7, “What Massachusetts laws pertain to patient privacy?”

There are some common misconceptions about HIPAA-compliant information sharing. They include7:

* **“HIPAA requires patient authorization whenever patient information is shared”.**

False. Except for special restrictions on psychotherapy notes, HIPAA does not require patient consent to share patient information between providers for treatment. However, as described elsewhere in this document, other federal and Massachusetts laws do require patient authorization before sharing certain types of information.

* **“HIPAA requires the provider to share only the minimum amount of patient information that is necessary for the purpose”.**

False. This “minimum necessary” provision does not apply when the purpose is treatment.

* **“HIPAA only allows patient information to be shared with another provider when that provider already has a care relationship with the patient”.**

False. This “pre-existing relationship” provision does not apply when the purpose is treatment. For example, patient information may be shared with a provider to whom the patient is being referred for the first time.

What is the Health Information Technology for Economic and Clinical Health Act (HITECH)?

Enacted in 2009, the HITECH Act gave the federal Department of Health and Human Services the authority to establish programs to improve health care quality, safety, and efficiency through the promotion of health IT, including electronic health records and private and secure electronic health information exchange.

Most healthcare providers are familiar with the provisions of the HITECH Act that established the “Meaningful Use” program. This program has provided incentives to providers for expanded use of electronic health records and electronic health information exchange. For the most part, the privacy and security provisions of the HITECH Act introduced new or stronger requirements for protecting patient information in electronic health records and other similar technologies, expanded requirements for breach notification, and extended HIPAA compliance requirements to business associates.

What is “sensitive information”?

“Sensitive information” is a term used for patient information that is more stringently regulated and protected because its disclosure has the potential to cause social, psychological, economic harm (e.g., employment discrimination), or stigmatization. Additionally, fear of disclosure can discourage patients from seeking treatment.

Sensitive information may be present in various components of a patient’s medical record, including but not limited to problem lists, medication lists, and notes. Sensitive information might include information pertaining to any of the following:

* Mental health disorders and treatment.
* Substance use disorders and treatment.
* HIV/AIDS.
* Sexually transmitted diseases.
* Rape/sexual assault.
* Domestic abuse.
* Abortion.
* Genetic testing.

Such information may be subject to special requirements and restrictions regarding disclosure, some of which are described in the following sections.

What is 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. 8,9,10

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.

* The regulations apply only to certain programs – 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 meet the definition of an individual or entity that holds itself out as providing, and actually provides, substance use disorder diagnosis, treatment, or referral for treatment.** This includes organizations and programs that are specially licensed to provide substance use disorder services or market themselves as providing these services. It includes units that are part of a larger entity *and* meet the definition.

**AND**

* **The program must receive federal assistance.** Federal assistance is defined broadly enough that most substance use disorder programs meet this qualification. Some examples are having tax-exempt status, being DEA-licensed, receiving federal grants, and receiving payments from Medicare or Medicaid.

**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 *not 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.
* The regulations require the provider to obtain written patient consent to disclose information for treatment, care coordination, or quality improvement. 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 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. Some limited exceptions are described below.
* The regulations permit initial disclosure or redisclosure of information *without patient consent* under certain circumstances. Some examples are when there is an immediate threat to the health of any individual and immediate medical intervention is required, some 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.

Some providers subject to 42 CFR Part 2 have a special arrangement called a Qualified Service Organization Agreement (QSOA) with each outside individual or organization that requires access to patient information in order to provide services to the 42 CFR Part 2 organization. See Section 6.4, “What is a Qualified Service Organization Agreement (QSOA)?”

What Massachusetts laws pertain to patient privacy? 10

* **Mental health information.**

Massachusetts laws generally require a provider to obtain patient consent to share mental health information, but they provide for exceptions based on the type of provider and whether the patient is a Medicaid patient. Some of these special restrictions include provisions that may not be clearly defined, such as “best interest” of the patient and “pursuant to a consultation”. The following provides general information about the categories of providers identified here:

* **Mental health providers.**

Psychologists are generally prohibited from disclosing identifiable patient information without patient consent. Some limited exceptions are cited, but there is no general exception for disclosures for treatment.

Psychiatrists are generally permitted by Massachusetts law to share mental health information with other providers without patient consent *for the purpose of treatment, payment, and operations*. The HIPAA exception for psychotherapy notes does apply, as does 42 CFR Part 2 for psychiatrists who are subject to Part 2.

Social workers are generally required to have patient consent for disclosures, including for disclosures for treatment. Disclosures may be subject to other restrictions regarding the type of recipient, whether the patient has been informed about the disclosure in advance, the reason for the disclosure, what information is disclosed, and redisclosure by the recipient.

Other allied mental health professionals (e.g., mental health counselors, marriage/family therapists, rehabilitation counselors, educational psychologists) are subject to restrictions similar to psychologists. They are generally prohibited from disclosing identifiable patient information, including for treatment, unless they have obtained a “waiver” from the patient.

Sexual assault counselors and domestic violence victim counselors are generally required to obtain patient consent for any disclosures.

* **Mental health facilities and community-based programs.** These facilities and programs are generally required to obtain written patient consent, including specific information, to disclose patient information. Exceptions apply when it is not possible or practical to obtain patient authorizations.
* **Medicaid patients.** For patients covered by MassHealth, Massachusetts law identifies specific consent and disclosure requirements for psychiatric hospitals, psychiatric day treatment programs, mental health center services, and psychologists that seem to override other applicable laws.
* **Massachusetts law related to 42 CFR Part 2.**

Massachusetts law imposes restrictions similar to 42 CFR Part 2 restrictions on some Massachusetts drug rehabilitation facilities and programs that might not otherwise be subject to 42 CFR Part 2 regulations. Specifically, Massachusetts law requires state-licensed substance use disorder treatment programs to comply with 42 CFR Part 2 even if they are not “federally assisted” according to the 42 CFR Part 2 regulations.

However, note that this law only overrides the “federally assisted” aspect of 42 CFR Part 2. Massachusetts law does not alter the definition of which entities are subject to Federal Regulation 42 CFR Part 2—providers and facilities that hold themselves out as providing, and provide, substance use disorder diagnosis, treatment, or referral for treatment, or whose primary function is identified as these services. See Section 3.6, “What is Federal Regulation 42 CFR Part 2?”

* **Other types of sensitive information.**

Massachusetts laws impose requirements on sharing of various types of sensitive information other than behavioral health information. Many of these laws specify rules for obtaining patient consent, special circumstances, and exceptions based on the type of information shared.

This document does not attempt to describe the rules and exceptions for each type of information. Providers should be aware that special protections may apply when sharing the following types of information:

* HIV/AIDS.
* Sexually transmitted diseases.
* Rape/sexual assault.
* Domestic abuse.
* Abortion.
* Genetic testing.

A provider organization’s policies for handling patient information should address Massachusetts requirements for handling sensitive information. The Blue Cross Blue Shield of Massachusetts Foundation has published a chart that may be helpful in determining when patient consent is required. 10

In what circumstances may patient information be shared without patient consent?

There are some circumstances when healthcare providers are allowed or required by law to share patient information, even if the patient has not given consent. Some examples include:

* Under HIPAA, providers may share medical information without patient consent in order to provide treatment, to receive payment from an insurance company, or to manage the services they provide to patients. However, because other federal and state laws are stricter than HIPAA, many provider organizations request patient consent for some or all information sharing. These organizations may have different policies regarding whether they will share medical information in the absence of explicit consent or when the patient has explicitly denied consent.
* Providers are generally allowed to share information without patient consent in medical emergencies. However, because there are exceptions, provider organizations’ procedures may differ based on whether the patient has authorized information sharing.
* Providers are required to report patient information to federal or state agencies that collect certain public health information.
* Providers are required to provide information in certain situations, including reporting child abuse or neglect, reporting threats against persons, and responding to a court order, a subpoena, or some other allowable request from law enforcement.

How do EHRs help to protect patient privacy?

How do EHRs send and receive patient information?

Capabilities for sharing information vary among EHRs. How information is actually exchanged depends on the capabilities of the two systems that are exchanging the information. Some examples:

* If both EHRs are capable of securely exchanging electronic documents, one may send a secure message like a patient’s health summary over the internet, and the message will be received by the other EHR. This is the most advanced form of patient information exchange. The sending EHR creates and sends an electronic document in a standard form to the other EHR via a highly secure internet connection. The receiving EHR can receive the electronic document, open it, and link it to the patient’s medical record.

The receiving system is usually an EHR if it is a provider’s system. The electronic document is often what is called a Continuity of Care Document (CCD). A CCD contains many standard sections of information, like patient identifying information, problem list, medications, allergies, test results, and other pertinent information.

If the receiving system belongs to a non-provider type of healthcare entity, the electronic document might be different. For example, if the receiving system is the state’s immunization registry, the electronic document might be an immunization message.

* If one or both systems (the sending system or the receiving system) is not capable of securely exchanging electronic documents, the information exchange may be manual or partially automated. For example, the sending provider’s staff may fax the information, or the sending EHR may be capable of directly faxing the information.
* Some systems use an HIE to facilitate secure information exchange. In this kind of exchange, the sending system may securely send the information to the HIE, and the HIE may securely deliver the information to one or more receiving systems. This can greatly simplify electronic information exchange since the sending system only needs to send information to the HIE instead of many other healthcare systems. Similarly, the receiving system only needs to receive information from the HIE. Over time, more and more healthcare organizations will exchange information via HIEs like the Mass HIway. See Section 2.6, “How does the Massachusetts Health Information Highway (the Mass HIway) work?”

How do EHRs protect the privacy of the information they send and receive?

Providers and other organizations that exchange electronic information are required to follow security practices that protect the patient information that is being exchanged:

* Wherever they are located, systems that contain patient information must be protected from access by unauthorized users. This is often accomplished by the use of unique user IDs and passwords. Only people who have a right to access a patient’s information can get it.
* When patient information is exchanged between systems, the internet connection must be highly secure so that the information can be accessed only by the intended parties. The data itself must be encrypted. “Encrypted” means that the information is in code, and only the systems that are authorized to send it or receive it can read the data.
* Healthcare organizations that use other methods of exchanging data, such as secure email and fax, are also required to take strict precautions to ensure the patient’s information does not become available to unauthorized persons.

How do EHRs handle patient consent and sensitive information?

Capabilities for tracking patient consent and differentiating between sensitive and non-sensitive information vary among EHRs.

Ideally, an EHR would be capable of tracking significant information about a patient’s consent status, including but not limited to:

* The patient’s identifying information, like name, date of birth, address, and medical record number.
* Whether the patient consented to or denied information sharing, by information type. For example, the system might keep track of the fact that the patient wishes to share mental health information but not HIV/AIDS or genetics testing information.
* Whom the patient consented to share information with, for example, with Provider A but not with Provider B.
* The date of the consent.
* The date or event upon which the consent expires. For example, an indication that the consent expires on January 14 or when a course of treatment ends.

Ideally, the EHR would also be able to execute the patient’s recorded instructions. For example, when sending out a patient’s information:

* Avoid sending out any information if the patient has given a blanket denial of information sharing or if consent has expired.
* Automatically remove information types for which consent is not in place, like removing HIV/AIDS diagnosis, medications, and any notes referring to HIV/AIDS, or removing all information about substance use disorder diagnosis and treatment. The underlying capability to support this is often called “data segmentation”. Data segmentation refers to the ability to identify different types of information within the patient’s record so that they can be accessed or not accessed depending on the situation.
* Automatically suppress sending information to a provider if the patient has either denied or not given authorization to share with that provider.

Most EHRs do not provide strong support for these capabilities. Complicating the problem is the fact that laws regarding what information may be shared, with whom, and under what circumstances vary significantly from state to state. Fully implementing in any EHR all of the rules and restrictions that might apply to information sharing is not practical at this time.

In the absence of fully automated support, most providers adopt operational procedures that provide reasonable protections for patient privacy. Some examples include:

* Using patient consent forms that address consent relatively broadly. For example, the consent form may indicate that the patient is consenting to sharing all information, including the various types of sensitive information. In this example, the provider may share information on an “all or nothing” basis—share all information if the patient has given consent and share no information if the patient has not.
* Allow the patient to give more detailed instructions than “all or nothing” and then select which information may be shared. This selection might occur within the EHR if the EHR supports it, or it may be done manually by the staff.

What are my responsibilities for protecting patient privacy?

What privacy policies do provider organizations have?

Provider organizations are required by law to have written policies addressing patient privacy, and they are required to educate their staff on these policies. Some of the policies that affect patient privacy include:

* User authentication and authorization. These policies describe how users receive and use credentials like IDs and passwords to gain access to information they are authorized to access.
* Handling of patient information in the environment. These policies address, for example, locating fax machines and paper files in secure areas and keeping patient information on computer screens private. They also address staff responsibilities for protecting patient information from unauthorized access.
* Obtaining patient consent. These policies describe the patients’ rights to give instructions on how their information may be shared or not shared.
* Information sharing. These policies describe how the patient’s consent instructions are followed in the environment.
* Methods of information exchange. These policies describe how secure methods for patient information exchange must be used to protect patient privacy. Some of these methods include whether secure email, secure text, and social media are allowed.
* Electronic exchange. These policies describe requirements for protecting patient information that is exchanged electronically.

How are the policies enforced?

Enforcement methods vary among provider organizations. Some methods include:

* Educating staff to be familiar with policies and report violations they are aware of.
* Walk-throughs of physical areas.
* Monitoring the use of secure systems, for example, by periodic automated or manual examination of reports and audit trails to detect unusual activity.

Patients can also receive reports of whom their information has been shared with, which could reveal inappropriate actions.

What are the consequences of privacy violations?

Certain types of legal recourse against provider organizations are available to regulatory authorities and patients in the event of improper disclosures of protected information. Penalties can include fines and even criminal charges. Inappropriate disclosures can affect patient confidence, the provider’s reputation, and the level of trust between providers.

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.

Provider staff who violate the provider organization’s patient privacy policies are usually subject to harsh disciplinary actions including suspension of privileges, probation, or firing.

What kinds of agreements support Health Information Exchange?

What is a Business Associate Agreement (BAA)?

HIPAA defines two types of entities that are subject to HIPAA, “covered entities” and “business associates”. See Section 3.2, “What is the Health Insurance Portability and Accountability Act (HIPAA)?”, for more information about these definitions.

Covered entities often work with business associates who provide services to the covered entity that require handling or disclosing PHI. A covered entity must have a Business Associate Agreement (BAA) in place with any such business associate. It should be noted that HIPAA does not require a BAA between providers for information exchange for the purpose of treatment.

At a minimum, the BAA describes how the business associate is permitted and required to use PHI, requires the business associate to have appropriate safeguards for PHI, requires the business associate to report data breaches and respond appropriately to them, and requires the business associate to respond appropriately to an investigation by the Office of Civil Rights (OCR).

What is an HIE agreement?

An HIE agreement is an agreement between an HIE and the organizations that participate in the HIE (the members). It describes the mutual roles and responsibilities of the HIE and its members. It includes provisions that describe the services the HIE provides, who is permitted to use the HIE’s services and for what purposes, policies and procedures for use of the HIE, required data safeguards, compliance with audits and investigations, liabilities, and fees. It may include additional sections that provide more detail for specific services used by specific members.

Healthcare organizations that use the Mass HIway must sign a Participation Agreement with the state of Massachusetts. This is an example of an HIE agreement.

What are service agreements and data sharing agreements?

Service agreements and data sharing agreements are similar to HIE agreements except that they describe the mutual roles and responsibilities of healthcare organizations that are exchanging information with each other without the use of an HIE. For example, two or more organizations that are not able to use an HIE or choose not to use an HIE will have service agreements and/or data sharing agreements that describe their mutual roles and responsibilities.

What is a Qualified Service Organization Agreement (QSOA)?

The term QSOA refers to a specific type of two-way agreement between a certain type of substance use disorder program and an entity that provide services to the program. It authorizes communication between the parties and restricts what information may be disclosed and/or redisclosed.

The QSOA is used only by substance use disorder programs that are subject to Federal Regulation 42 CFR Part 2. See Section 3.6, “What is Federal Regulation 42 CFR Part 2?” for more information.

Where can I find more information?

If you have questions on this document or need further information about any of the topics, please contact your supervisor, your Compliance Department, or your Human Resources Department. You may also reference Appendix A, “References”, for more information.

Appendix A. References

1 “What is the difference between ‘consent’ and ‘authorization’ under the HIPAA Privacy Rule?” U.S. Department of Health & Human Services, [www.hhs.gov/hipaa/for-professionals/faq/264/what-is-the-difference-between-consent-and-authorization/index.html](http://www.hhs.gov/hipaa/for-professionals/faq/264/what-is-the-difference-between-consent-and-authorization/index.html). Accessed January 12, 2017.

2 “Covered Entities and Business Associates”. U.S. Department of Health & Human Services, [www.hhs.gov/hipaa/for-professionals/covered-entities/index.html?language=es](http://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html?language=es). Accessed January 12, 2017.

3 “Business Associates”. U.S. Department of Health & Human Services, [www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html?language=es](http://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html?language=es). Accessed January 12, 2017.

4 “Administrative Simplification Coverage Entity Guidance”. Centers for Medicare & Medicaid Services, [www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/Downloads/CoveredEntitiesChart20160617.pdf](http://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/Downloads/CoveredEntitiesChart20160617.pdf). Accessed January 12, 2017.

5 “Summary of the HIPAA Privacy Rule”. U.S. Department of Health & Human Services, [www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html](http://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html). Accessed January 12, 2017.

6 “Authorization Requirements for the Disclosure of Protected Health Information (2013)”. American Health Information Management Association (AHIMA), <http://library.ahima.org/doc?oid=107284#.WHVZDE3rupp>. Accessed January 12, 2017.

7 Manatt, Phelps & Phillips—Robert Belfort, William Bernstein, and Susan Ingargiola. “Integrating Physical and Behavioral Health, Strategies for Overcoming Legal Barriers to Health Information Exchange”. Robert Wood Johnson Foundation, [www.manatt.com/uploadedFiles/Content/4\_News\_and\_Events/Newsletters/IntegratingPhysicalandBehavioralHealth.pdf](http://www.manatt.com/uploadedFiles/Content/4_News_and_Events/Newsletters/IntegratingPhysicalandBehavioralHealth.pdf). Accessed January 12, 2017.

8 ”Confidentiality of Substance Use Disorder Patient Records, A Proposed Rules by the Health and Human Services Department on 02/09/2016”. Federal Register, [www.federalregister.gov/documents/2016/02/09/2016-01841/confidentiality-of-substance-use-disorder-patient-records](http://www.federalregister.gov/documents/2016/02/09/2016-01841/confidentiality-of-substance-use-disorder-patient-records). Accessed January 12, 2017.

9 ”Substance Abuse Confidentiality Regulations, Frequently Asked Questions (FAQs) regarding the Substance Abuse Confidentiality Regulations.” Substance Abuse and Mental Health Services Administration (SAMHSA), [www.samhsa.gov/about-us/who-we-are/laws/confidentiality-regulations-faqs](http://www.samhsa.gov/about-us/who-we-are/laws/confidentiality-regulations-faqs). Accessed January 12, 2017.

10 Manatt, Phelps & Phillips, LLC—Robert D. Belfort and Alex Dworkowitz. “Sharing Behavioral Health Information in Massachusetts: Obstacles and Potential Solutions”. Blue Cross Blue Shield of Massachusetts Foundation, <http://bluecrossfoundation.org/publication/sharing-behavioral-health-information-massachusetts-obstacles-and-potential-solutions>. Accessed January 12, 2017.