Colorado Health Information Governance Guidebook

SEPTEMBER 2021
Version 1.3

OeHI
Office of eHealth Innovation

Contents

Introduction

Information governance is the act of establishing standard policies and procedures for using information in a responsible manner. Information governance is especially important in health care, social services, and other settings where personally identifiable information (PII) is needed to provide care and other services. Effective information governance promotes accessibility of high-quality data across the spectrum of health and social services through secure, trusted mechanisms and ensures those data are appropriately used.

In Colorado, many organizations, including those in health care, health information technology (health IT), social services, and state agencies, are working together to expand health information sharing to improve health outcomes for individuals and families. For example, a primary care provider might work with a substance use disorder (SUD) treatment specialist to help someone battle an opioid addiction. Or, a patient navigator might connect someone to a local program that offers lifestyle coaching to manage diabetes. These efforts require cross-sector information sharing, which can be difficult due to the complex federal and state regulations and standard practices that apply to different settings. Organizations are seeking more guidance to help them understand how to responsibly share information with new partners. The *Colorado Health Information Governance Guidebook* (Guidebook) was developed to meet this need.

The Colorado Office of eHealth Innovation (OeHI) and eHealth Commission developed this Guidebook with support from Colorado Health Institute to advance Colorado's Health IT Roadmap Information Governance Initiative. This Guidebook aims to inform and align information sharing and information governance efforts underway across Colorado.

This Guidebook is an appendix of Colorado's Health IT Roadmap. The use cases outlined in this Guidebook were identified by OeHI and the eHealth Commission based on key state priorities.

This Guidebook will be updated quarterly. Each update is reviewed and approved by the Statewide Information Governance Committee and subcommittees that report to OeHI and the eHealth Commission. A description of each update throughout this process will be provided in the Revision Table. To learn more about OeHI and the eHealth Commission's efforts, please contact Carrie Paykoc, Director, Office of eHealth Innovation, at carrie.paykoc@state.co.us.

Revision Table

Version Number:	Date:	Update Description:
1.0	09/30/2020	• Introduction • Outline
1.1	03/31/2021	• Outline • How To Use This Guidebook • Health Information Sharing Principles • Physical Health Provider Organization to Behavioral Health Provider Organization Use Case • Behavioral Health Provider Organization to Physical Health Provider Organization Use Case
1.2	06/30/2021	• Guidebook structure • Introduction • Outline • How To Use This Guidebook • Health Information Sharing Principles • Physical Health Provider Organizations ○ Data Sharing in Medical Emergencies ○ Data Sharing with Patients • Behavioral Health Provider Organizations ○ Data Sharing in Medical Emergencies ○ Data Sharing with Patients • Appendix A: Compendium of Federal and State Regulations for Data Sharing ○ HIPAA ○ 42 CFR Part 2 • Appendix C: Health Information Exchange and Data Format Standards
1.3	09/30/2021	• "What Work Remains" section of all use cases updated to be sorted by technical and policy barriers • Physical Health Provider Organizations – Data Sharing with Social Service Provider Organizations • Behavioral Health Provider Organizations – Data Sharing with Social Service Provider Organizations • Social Service Provider Organizations – Data Sharing for Care Coordination Among Provider Organizations • Inclusion of HIPAA Proposed Changes • Appendix A: Compendium of Federal and State Regulations for Data Sharing ○ Colorado Regulations for Data Sharing

Principles for Developing this Guidebook

The eHealth Commission's Statewide Information Governance on Health Committee has identified the following principles to inform this Guidebook's development process:

- This Guidebook will support Colorado's health care transformation efforts.
- An inclusive and equitable approach will lead the development of this Guidebook and recommendations focused on information governance and the use of data.
- Existing governance infrastructure and examples will be leveraged, where possible, and new procedures will be developed when needed.
- Diverse geographic and demographic considerations will inform the development of this Guidebook.
- Ethical considerations of existing and future systems and structures that extend beyond legal compliance will be applied to this Guidebook and its recommendations to promote equity and to ensure sound information governance stewardship.

How to Use this Guidebook

What types of organizations should use this Guidebook?

This Guidebook focuses on information sharing across three provider organization types with specific use cases:

- Physical health provider organizations,
- Behavioral health provider organizations, including mental health and substance use disorder (SUD) treatment provider organizations, and
- Social service provider organizations, including community-based organizations (CBOs) and state and county human service agencies.

This Guidebook promotes a common statewide approach to managing the health information shared among these types of provider organizations. This resource is for organizations and providers interested in improving existing information governance practices or establishing future information governance systems. Note that health insurance payers will be included in future iterations of this Guidebook.

What is included in this Guidebook?

This Guidebook pulls from both prior and ongoing information governance efforts to capture best practices and inform future data-sharing projects. It provides considerations for the consent, standardization, sharing, and application of health and health-related data across Colorado within each provider organization use case where applicable. Each section of this Guidebook reflects existing efforts (established and in development) by provider organization use case that may contribute to information governance in Colorado.

How is this Guidebook structured?

This Guidebook is structured around data-sharing use cases by provider organization type. Each provider organization section follows the same format, which includes two sections (see Figure 1): Overview of Data Sharing; and Data-Sharing Platforms, Protocols, and Elements.

Figure 1. Example of the Guidebook's structure by provider organization type and connection to Colorado's Health IT Roadmap

Overview of Data Sharing *(By Provider Organization Type)*	
Data-Sharing Platforms, Protocols, and Elements *(By Use Case)*	
• **How to Share** • **Existing Resources** • **What Work Remains** • **Considerations**	• **Goal of this Section:** Map Colorado's existing data repositories and the information governance frameworks for sharing health information; Describe data-sharing best-practices, including data elements to be included when sharing health and health-related data • **Connection to Colorado's Health IT Roadmap:** Initiative #4 Integrate Behavioral, Physical, Claims, Social, and Other Health Data; Initiative #5, Statewide Health Information Governance

The ***Overview of Data Sharing*** section provides a high-level summary of how data can be shared by provider organization type. The purpose of this section is to orient the reader to the most important points of guidance for data sharing that originates from the defined provider organization type, before delving into details and use cases in the following section.

The ***Data-Sharing Platforms, Protocols, and Elements*** section focuses on the technical aspects of how to share data by use case scenario. For example, sharing data from a physical health provider organization to another health care provider organization, or sharing data from a physical health provider organization to a social service provider organization. The purpose of this section is to provide the reader with details on the technologies and best practices that exist for sharing data by use case. Each use case is divided into four subsections: The ***How to Share*** section outlines Colorado's existing repositories for data sharing, best practices for how to share data, and the type of information that should be included when transferring data; the ***Existing Resources*** section provides additional materials related to data sharing under the specified use case; the ***What Work Remains*** section provides an overview of known technical or policy-related barriers to data sharing under the specified provider type and use case; and the ***Considerations*** section lists information that readers should keep in mind when using this Guidebook and sharing data under the specified use case.

Federal and state regulations that are applicable to multiple provider organizations can be found in [Appendix A: Compendium of Federal and State Regulations for Data Sharing](). Each regulation includes the following sections (see Figure 2): Clarification of Regulation for Health Information Sharing; Patient or Client Consent and Consent Management; and Accountability. The ***Clarification of Regulation for Health Information Sharing*** section provides an overview of permissible data sharing under the regulation. The ***Patient or Client Consent and Consent Management*** section focuses on the rules around when – and how – to obtain patient or client consent. The ***Accountability*** section provides an overview of the provider organization's responsibilities around security, or other policies and procedures. Each section includes pertinent resources related to the topic.

Note that the Social Service Provider Organization section follows this format and outlines the current landscape for how to share data, including resources, and work that remains to promote interoperability. However, the regulatory landscape governing social data sharing is fragmented and, as a result, this section suggests an incremental approach to sharing social service data for care coordination purposes.

Figure 2. Appendix A: Compendium of Federal and State Regulations for Data Sharing and connection to Colorado's Health IT Roadmap

Name of Regulation	
Clarification of Regulation for Health Information Sharing • **Overview** • **Pertinent Resources**	• **Goal of this Section:** Provide clarification on how the regulation relates to health information sharing • **Connection to Colorado's Health IT Roadmap:** Initiative #3, Harmonize and Advance Data Sharing and Health Information Exchange Capabilities Across Colorado
Patient Consent and Consent Management • **Overview** • **Pertinent Resources**	• **Goal of this Section:** Provide information related to collecting and managing patient and client consent in data sharing • **Connection to Colorado's Health IT Roadmap:** Initiative #10, Consent Management
Accountability • **Overview** • **Pertinent Resources**	• **Goal of this Section:** Provide guidance on creating a framework for holding organizations accountable for the data they store, share, and use • **Connection to Colorado's Health IT Roadmap:** Initiative #6, Health IT Portfolio/Program Management

Who should use this Guidebook?

Individuals in the following roles can use this Guidebook to inform their information governance efforts. Users may see themselves in a single role or addressing portions of multiple positions. These roles may be identified throughout this Guidebook for their unique responsibilities developing, implementing, or enforcing governance policies.

- The “Chief Data Officer,” who develops and leads an organization’s information governance strategy.
- The “Chief Privacy Officer,” who develops and implements policies to protect health and health-related data from unauthorized access and use.
- The “Governance Committee Member,” who sets policies and procedures for information governance.
- The “Data Steward,” who manages system-level data collection, storage, and transfer and enforces policies on information governance.
- The “Data Owner,” who is involved in the protection of data as an asset.
- The “Product Owner,” who builds features, delivers software, and is thinking through the collective impact of data on populations served.
- The “Data Lead,” who pulls and analyzes data for clinic strategy or operations.

What is not provided in this Guidebook?

While this Guidebook is designed to be helpful and authoritative, it is specifically not designed, nor does the State of Colorado intend through its publication, to provide legal counsel. This is for informational purposes only and should not be construed as legal advice or policy of the State. OeHI, the eHealth Commission, and Colorado Health Institute make no warranties, expressed or implied, regarding errors or omissions and assume no legal liability or responsibility for loss or damage resulting from the use of information contained herein. Due to the complexity of laws related to personally identifiable information, readers are encouraged to consult legal counsel prior to developing and implementing operational policies and procedures governing the use and disclosure of such information.

Glossary

Below are definitions for acronyms and terms commonly used in this Guidebook.

Term	Definition
CBO	Community-based organization – an organization that improves a community’s social health and well-being.
CCD	Continuity of Care Document – a standardized medical summary for one or more patient encounters built on clinical document architecture (CDA). CCDs contain patient data such as a problem list, medications, allergies, immunizations, lab results, patient notes, and other summarized data. CCDs are electronically exchanged with other providers, usually through a health information exchange (HIE).
CCDA	Consolidated Clinical Document Architecture – a standard that allows documents to be formatted to contain structured and unstructured patient data and can be used to support health information exchange (HIE) with other electronic health record (EHR) systems.

CDA	Clinical Document Architecture – a base standard that provides common architecture, coding, semantic framework, and markup language for the creation of electronic clinical documents.
CDHS	Colorado Department of Human Services – Colorado has a state-supervised and county-administered human services system. Under this system, county departments are the main provider of direct services to Colorado's families, children, and adults.
CDPHE	Colorado Department of Public Health & Environment – Protects and maintains the health and environment of Coloradans.
CMS	Centers for Medicare & Medicaid Services – administers Medicare, Medicaid, and the Children's Health Insurance Program (CHIP).
Colorado WIC	The Colorado Special Supplemental Nutrition Program for Women, Infants, and Children – ensures the health and well-being of pregnant and breastfeeding women and children under the age of five. Administered by the Colorado Department of Public Health & Environment.
CORHIO	Colorado Regional Health Information Organization – one of two statewide health information exchanges.
Covered Entity	Covered entities are defined in the HIPAA rules as (1) health plans, (2) health care clearinghouses, and (3) health care providers who electronically transmit any health information in connection with transactions for which HHS has adopted standards. Individuals, organizations, and agencies that meet the definition of a covered entity under HIPAA must comply with HIPAA's requirements to protect the privacy and security of health information and must provide individuals with certain rights with respect to their health information.
EHR	Electronic health record – a digital version of the paper charts in the clinician's office that contains the medical and treatment history of patients. For the purposes of this Guidebook, this term is used interchangeably with electronic medical record (EMR).
EMR	Electronic medical record – a digital version of the paper charts in the clinician's office that contains the medical and treatment history of patients. For the purposes of this Guidebook, this term is used interchangeably with electronic health record (EHR).
FHIR	The Fast Healthcare Interoperability Resource – a standard for exchanging health information electronically using internet technologies that allow information to be shared between systems regardless of how they are stored in those systems.
Health IT	Health information technology – supports a variety of health care services using information technology. Information technology includes the use of computerized systems and the secure exchange of data in support of health care delivery. Electronic health records and health information exchanges are examples of health IT.
HHS	The U.S. Department of Health and Human Services – administrators of the HIPAA Privacy Rule and the Security Rule.
HIE	Health information exchange – the electronic movement of health-related information among organizations according to nationally recognized standards. The goal of health information exchange is to facilitate access to and retrieval of clinical data to provide safer, timelier, efficient, effective, equitable, patient-centered care.
HIPAA	The Health Insurance Portability and Accountability Act; 45 CFR Part 164 – a federal law that requires the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge.

	See **Appendix A: Compendium of Federal and State Regulations for Data Sharing** for more information.
HL7	Health Level 7 – provides a framework and standards for the exchange, integration, sharing, and retrieval of electronic health information. HL7 standards support clinical practice and the management, delivery, and evaluation of health services. These standards define how information is packaged and communicated from one party to another, setting the language, structure and data types required for seamless integration between systems. AND The name of the organization (Health Level Seven International) that oversees the standards.
OBH	The Colorado Department of Human Services' (CDHS) Office of Behavioral Health – Colorado agency responsible for policy development, service provision and coordination, program monitoring and evaluation, and administrative oversight for the public behavioral health system.
OeHI	The Colorado Office of eHealth Innovation – responsible for defining, maintaining, and evolving Colorado's Health IT strategy concerning care coordination, data access, health care integration, payment reform, and care delivery.
ONC	Office of the National Coordinator for Health Information Technology – the principal federal entity charged with coordination of nationwide efforts to implement and use the most advanced health information technology and the electronic exchange of health information.
Part 2	Title 42 of the Code of Federal Regulations Part 2: Confidentiality of Substance Use Disorder Patient Records; 42 CFR Part 2 – a federal law that protects the confidentiality of substance use disorder treatment records. See **Appendix A: Compendium of Federal and State Regulations for Data Sharing** for more information.
Part 2 Program	A Part 2 program is an individual, entity, or identified unit within a general medical facility that is federally assisted and holds itself out as providing, and provides, SUD diagnosis, treatment, or referral for treatment. See **Appendix A: Compendium of Federal and State Regulations for Data Sharing** for more information.
PHI	Protected health information – any information about health status, provision of health care, or payment for health care that is created or collected by a covered entity (or a business associate of a covered entity) and can be linked to a specific individual.
PII	Personally identifiable information – any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means.
QHN	Quality Health Network – one of two statewide health information exchanges.
QSO	Qualified service organization – an individual or entity who provides services to a Part 2 program, such as data processing, bill collecting, population health management, medical staffing, etc. and has a written agreement (qualified service organization agreement, or QSOA) with a Part 2 program. See 42 CFR Part 2.11 for a full definition.
SAMHSA	Substance Abuse and Mental Health Services Administration – the agency within HHS that leads public health efforts to advance the behavioral health of the nation. SAMHSA's mission is to reduce the impact of substance abuse and mental illness on America's communities.

SNAP	Supplemental Nutrition Assistance Program – provides monthly benefits to low-income households to help individuals and families buy nutritious food. Administered by the Colorado Department of Human Services.
SUD	Substance use disorder
TEFCA	Trusted Exchange Framework and Comment Agreement – outlines a common set of principles, terms, and conditions to support the development of a common agreement that would help enable nationwide exchange of electronic health information across disparate health information networks.

Health Information Sharing Principles

Across all instances of sharing health and health-related information, common best practices and key regulations must be maintained.

Best Practices for Health Information Sharing

The following best practices should be considered and upheld when sharing health and health-related information across all use cases. Notably, some of these best practices may be upheld by various state and federal regulations:

- All data-sharing efforts should begin with a clear articulation of the principles.
- Data are reflective of people and should be used to improve health outcomes and advance population health equity.
- A patient generally has the right to inspect, review, and obtain copies of their patient health information, and a provider is responsible for enabling such patient access.
- Organizations that exchange personal and protected information will seek to prevent, reduce, and remediate harm from such exchanges.
    - Information governance, including the reliability and security of data, is the responsibility of each entity that collects, stores, shares, or analyzes data, and entities will be held accountable.
    - When health information is requested, used, or disclosed, steps should be taken to limit the information to only what is relevant and necessary to accomplish the intended purpose. Patient identifiers, such as name and date of birth, should be included.
    - When sharing data, health information technology (health IT) and health information exchange (HIE) should be used when possible. Other regulatory compliant methods for sharing information, such as U.S. mail, should be avoided to ensure better security and privacy of protected health information (PHI). Using health IT and HIE also allows for more timely sharing of PHI between providers.
    - Entities should create a log of what is shared, when, and with whom. This functionality is often available in electronic health records (EHRs), including electronic medical records (EMRs).

- Leveraging current Colorado efforts and organizations, such as the state Joint Agency Interoperability project and existing data-sharing agreements, should be considered. Additionally, recommendations on the governance structures needed at the state, regional, and local levels to support the sustainability of these technologies are needed.

Key Regulations

- The Health Insurance Portability and Accountability Act (HIPAA) is a federal law that requires the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge. The U.S. Department of Health and Human Services (HHS) issued the HIPAA Privacy Rule (Privacy Rule) to implement the requirements of HIPAA. The HIPAA Security Rule (Security Rule) protects a subset of information covered by the Privacy Rule. See **Appendix A: Compendium of Federal and State Regulations for Data Sharing** for more information on HIPAA.
    - In December 2020, the Office of Civil Rights at HHS announced proposed modifications to HIPAA that may change how information sharing occurs. These changes would strengthen individuals' rights to access their own health information, improve information sharing for care coordination and case management for individuals, facilitate greater family and caregiver involvement in the care of individuals experiencing emergencies and health crises, enhance flexibilities for disclosures in emergency or threatening circumstances, and reduce administrative burdens on HIPAA-covered entities. See Modifications to the HIPAA Privacy Rule to Support, and Remove Barriers to, Coordinated Care and Individual Engagement for more information on the proposed rule. Summaries of the major provisions are highlighted where applicable throughout this Guidebook.
- Information governance efforts will be conducted in a transparent manner, and data will be accessible to stakeholders. The Office of the National Coordinator for Health Information Technology's (ONC) Cures Act Final Rule aims to improve interoperability and patient access, and prevents information blocking – a practice that interferes with access, exchange, or use of electronic health information – from occurring.
    - Eight categories of reasonable and necessary activities are identified that do not constitute information blocking provided certain conditions are met.
    - Other federal efforts to reduce barriers to information sharing include the voluntary Trusted Exchange Framework and Comment Agreement (TEFCA). TEFCA outlines a common set of principles, terms, and conditions to support the development of a Common Agreement that would help enable nationwide exchange of electronic health information across disparate health information networks. Final TEFCA rules and guidance have not yet been published.
- 42 CFR Part 2 (Part 2) is a federal regulation that applies to PHI of individuals who receive drug and alcohol abuse treatment in federally funded programs. Part 2 is administered by HHS' Substance Abuse and Mental Health Services Administration

(SAMHSA). Regulations apply to information that would identify a patient as having a substance use disorder (SUD) and allow very limited disclosures of information without patient authorization. See **Appendix A: Compendium of Federal and State Regulations for Data Sharing** for more information on Part 2.
- Colorado has several regulations regarding the confidentiality and protection of PHI, enabling patient access, and maintaining compliance with federal regulations. See **Appendix A: Compendium of Federal and State Regulations for Data Sharing** for more information.

Priority Provider Organization Types and Use Cases

Opportunities exist to develop robust data-sharing capabilities not only between health care provider organizations, but also when linking Coloradans with resources to help meet basic health and social needs, and in a medical emergency. In direct collaboration with the eHealth Commission Consent Workgroup and with input and guidance from the Colorado Department of Human Services' Office of Behavioral Health (OBH), the Colorado Office of eHealth Innovation (OeHI) identified the following provider organization types and use cases as priorities to be included in this Guidebook:

1. Physical Health Provider Organizations
   a. Data Sharing with Other Health Care Provider Organizations
   b. Data Sharing in Medical Emergencies
   c. Data Sharing with Patients
   d. Data Sharing with Social Service Provider Organizations
2. Behavioral Health Provider Organizations
   a. Data Sharing with Other Health Care Provider Organizations
   b. Data Sharing in Medical Emergencies
   c. Data Sharing with Patients
   d. Data Sharing with Social Service Provider Organizations
3. Social Service Provider Organizations
   a. Data Sharing for Care Coordination Among Provider Organizations

This Guidebook details best practices and remaining work for these use cases. Note that behavioral health was identified as a priority focus for this Guidebook as currently, numerous policy opportunities exist for sharing behavioral health data.

Physical Health Provider Organizations

To provide effective treatment and coordinated care, a physical health provider organization may need to send patient information to another entity, including mental health and substance use disorder (SUD) treatment provider organizations or social service provider organizations. Examples of sharing protected health information (PHI) regarding a patient may include:

- Sharing patient identifiers like name and date of birth, prescribed medications – which is necessary to avoid contraindications with medications prescribed by another health care provider – or known allergies, illnesses, or conditions that may negatively interact with medications and treatments to a specialty health care provider;
- Sharing or accessing PHI for a patient in the event of a medical emergency; or
- Referring a patient with a food security need to a social service agency.

This section applies to data sharing that originates from a physical health provider who is not serving as a behavioral health provider and is not subject to federal regulation 42 CFR Part 2 (Part 2). For providers and organizations subject to Part 2, see the **Behavioral Health Provider Organizations** section of this Guidebook.

Overview of Data Sharing

Entities should comply with best practices outlined in the **Health Information Sharing Principles** section of this Guidebook.

Under the Health Insurance Portability and Accountability Act (HIPAA, 45 CFR Part 164), physical health provider organizations (or covered entities) not subject to Part 2 are permitted to **share PHI with other health care provider organizations** without patient consent and authorization for treatment, payment, and health care operation activities.

This includes disclosing PHI to another health care provider organization who has a medical responsibility for the patient, or **to public or private-sector entities providing social services** (such as housing, income support, or job training), if social service entities are a necessary component of, or may help advance, the individual’s health or mental health care.

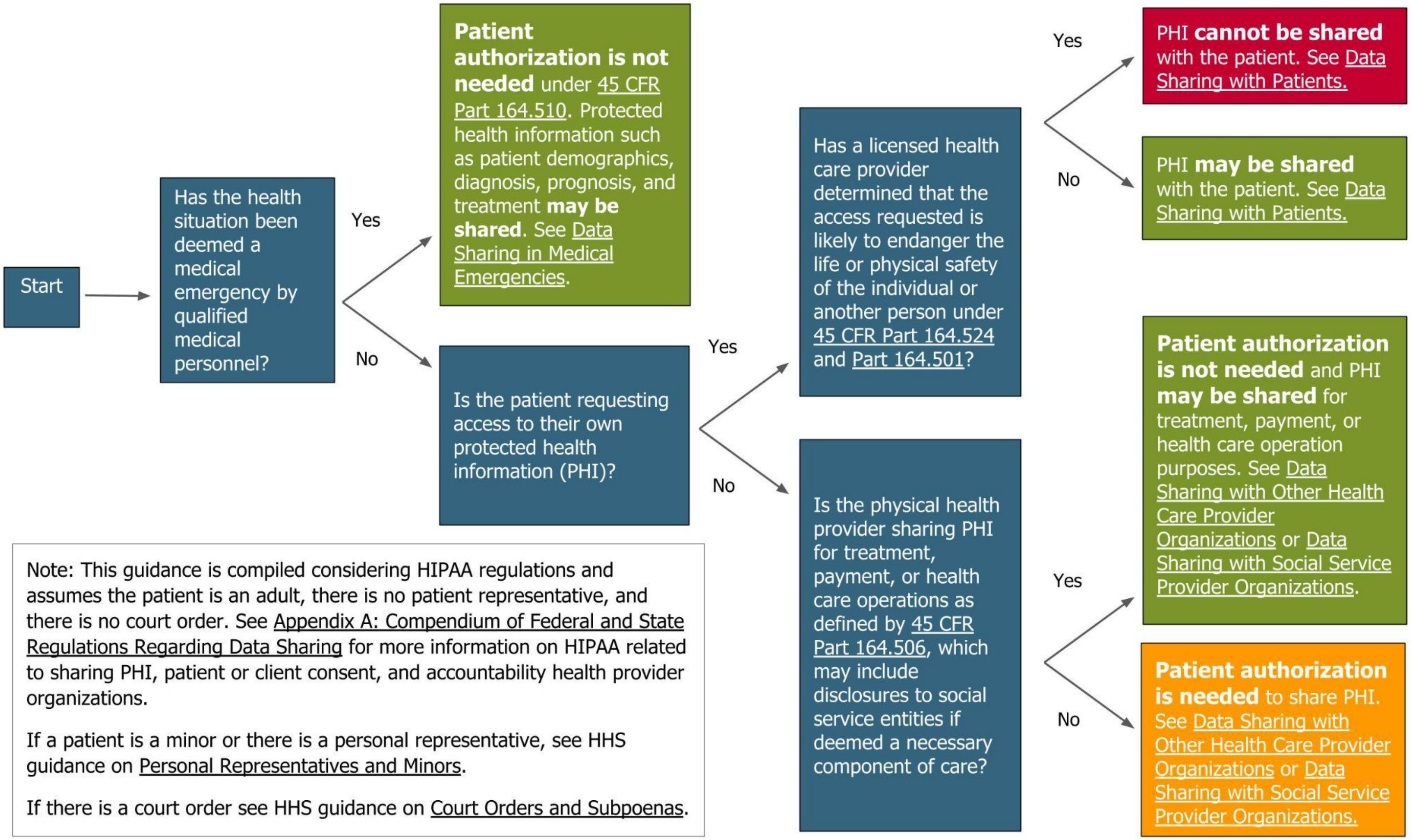
In the event of a **medical emergency**, PHI may be disclosed by a physical health provider organization and accessed by the treating health provider organization.

In all other instances, patient authorization is required to disclose PHI.

Patient access is permitted, and a patient has the right to inspect, review, and obtain copies of their PHI unless a licensed health care provider has determined the access is reasonably likely to endanger the life or physical safety of the individual or another person.

See **Appendix A: Compendium of Federal and State Regulations for Data Sharing** for more information on HIPAA and Colorado regulations related to sharing PHI, patient or client consent, and accountability of covered entities.

Figure 3. Overview of data sharing by physical health provider organization use cases



Start

Has the health situation been deemed a medical emergency by qualified medical personnel?

Patient authorization is not needed under 45 CFR Part 164.510. Protected health information such as patient demographics, diagnosis, prognosis, and treatment **may be shared**. See Data Sharing in Medical Emergencies.

Is the patient requesting access to their own protected health information (PHI)?

Has a licensed health care provider determined that the access requested is likely to endanger the life or physical safety of the individual or another person under 45 CFR Part 164.524 and Part 164.501?

PHI **cannot be shared** with the patient. See Data Sharing with Patients.

PHI **may be shared** with the patient. See Data Sharing with Patients.

Is the physical health provider sharing PHI for treatment, payment, or health care operations as defined by 45 CFR Part 164.506, which may include disclosures to social service entities if deemed a necessary component of care?

Patient authorization is not needed and PHI **may be shared** for treatment, payment, or health care operation purposes. See Data Sharing with Other Health Care Provider Organizations or Data Sharing with Social Service Provider Organizations.

Patient authorization is needed to share PHI. See Data Sharing with Other Health Care Provider Organizations or Data Sharing with Social Service Provider Organizations.

Note: This guidance is compiled considering HIPAA regulations and assumes the patient is an adult, there is no patient representative, and there is no court order. See Appendix A: Compendium of Federal and State Regulations Regarding Data Sharing for more information on HIPAA related to sharing PHI, patient or client consent, and accountability health provider organizations.

If a patient is a minor or there is a personal representative, see HHS guidance on Personal Representatives and Minors.

If there is a court order see HHS guidance on Court Orders and Subpoenas.

Data-Sharing Platforms, Protocols, and Elements

Data Sharing with Other Health Care Provider Organizations

- **How to Share:** Sharing PHI must be done through HIPAA-compliant methods that are adequately protected. As a best practice, secured health information technology (health IT), such as health information exchanges (HIEs) should be used to disclose PHI. Information that is exchanged through health IT uses a set of common terminology, content, and transport standards that connect systems. See **Appendix C: Health Information Exchange and Data Standards** for more information. PHI may also be shared through other HIPAA-compliant methods such as certified electronic health records (EHRs), secure fax or email, or mail.

  For disclosures to or requests from a health care provider for treatment purposes, HIPAA's Minimum Necessary Standard does not apply. However, as a best practice, when PHI is requested, used, or disclosed, steps should be taken to limit the information to only what is relevant and necessary to accomplish the intended purpose. This includes patient identifiers, such as name and date of birth, and the extent to which medical history is shared. Health IT content standards, such as continuity of care documents (CCDs) can provide a template for data elements to include when sharing PHI.
- **Existing Resources**: (See **Appendix B: Resources** for additional resources)
  - Colorado Regional Health Information Organization (CORHIO) and Quality Health Network (QHN) are two organizations that provide HIE services in the state of Colorado. HIEs help promote interoperability and ensure that provider organizations are exchanging PHI in accordance with HIPAA and other standard data formats. Individuals should consult CORHIO's website and QHN's website to learn more about services provided.
- **What Work Remains**:
  - **Technical Barriers:**
    - Systems are disparate. There are a multitude of EHR vendors whose products differ in functionality, which makes interoperability across providers and health care systems difficult. While HIE services promote interoperability, they can be costly, which may prevent some health care provider organizations from being connected to an HIE.
    - Health care provider organizations should be able to obtain all relevant PHI for a patient through both HIEs from a single request. CORHIO and QHN are working to make this functionality more reliable and widely available.
  - **Policy Barriers:**
    - Currently, there is no standard for which data elements should be disclosed and the information necessary may vary case by case. However, the Minimum Necessary Standard and CCDs may provide guidance on information that should be included. (See **Appendix C: Health Information Exchange and Data Standards** for more information on data standards).
- **Considerations**:

  - Due to the centralized nature of HIEs, providers may be worried about security and privacy of data. Individuals should consult CORHIO and QHN for more information on how HIEs operate.
  - HIEs in Colorado use an opt-out policy for HIPAA-regulated PHI. To share PHI via HIEs, health care provider organizations must notify patients of HIE use and allow them the right to opt-out of having their PHI accessible through an HIE. It is the health care provider organization's responsibility to manage opt-out and opt-back-in forms.
  - HIEs supporting the exchange of PHI should have built-in records that log the exchange of PHI, including to whom the PHI was disclosed and when the disclosure occurred.
  - Under the HIPAA Privacy Rule, data use agreements ensuring specified safeguards for the PHI are required for use and disclosure of limited data sets (PHI from which certain specified direct identifiers of individuals and their relatives, household members, and employers have been removed) for research, health care operations, and public health purposes.

Data Sharing in Medical Emergencies

- **How to Share:** While data sharing can be done through any HIPAA-compliant platform, in the event of a medical emergency, a query-based exchange through an HIE allows the treating provider to obtain the most up-to-date and immediate access to PHI (see **Appendix C: Health Information Exchange and Data Standards** for more information on HIEs). Accessing data this way without the patient's consent is permissible under HIPAA. Treating health care providers may "break the glass" to access PHI. This requires health care providers to verify they are permitted to access PHI under a special circumstance, for example, in the event of a medical emergency.

  Under HIPAA, PHI shared for emergency medical treatment purposes is generally not required to be documented outside of the medical record, for example for accounting of disclosure purposes. Note that an audit log of "break glass" access should be maintained.

  HIPAA's Minimum Necessary Standard does not apply to disclosures to or requests from a health care provider for treatment purposes, but covered entities should continue to ensure access to PHI to only those workforce members who need it to carry out their duties.
- **Existing Resources**: (See **Appendix B: Resources** for additional resources)
  - Break Glass Procedure: Granting Emergency Access to Critical ePHI Systems – Yale University guidance on breaking glass to access PHI.
  - COVID-19 & HIPAA Bulletin – U.S. Department of Health and Human Services (HHS) guidance on sharing PHI during COVID-19 Nationwide Public Health Emergency and during more general emergency situations.

  - Emergency Situations: Preparedness, Planning, and Response – HHS guidance on the release of PHI for planning or response activities in emergency situations.
- **What Work Remains:**
  - **Technical Barriers:**
    - The amount or quality of data available for a patient in an HIE is subject to whether their health care providers participate in an HIE. Therefore, technical and policy barriers that prevent health care provider organizations from being connected to an HIE may limit available data.
    - Conversely, treating providers in a medical emergency may encounter a plethora of patient data when using "break glass" to access PHI via an HIE. Solutions that enable providers to quickly access and review the most pertinent PHI, such as a consolidated care summary – a single document that includes previous hospital patient data, laboratory and diagnostic results, and clinical documents from community providers – are needed to deliver care efficiently in crisis situations.
  - **Policy Barriers:**
    - Using the "break glass" functionality to access PHI may not limit inappropriate access to a patient's PHI.
    - Policies that rely on audit logs may create administrative burden on provider organizations to review access to a patient's PHI.
- **Considerations:**
  - Per HIPAA (45 CFR Part 164.510), the covered entity should get verbal permission from individuals or otherwise be able to reasonably infer that the patient does not object, when possible; if the individual is incapacitated or not available, covered entities may share information for these purposes if, in their professional judgment, doing so is in the patient's best interest. This includes sharing relevant information about the patient with family, friends, or others involved in the patient's care or payment for care, if the health care provider determines, based on professional judgment, that doing so is in the best interest of the patient if the patient is unconscious or incapacitated.

Data Sharing with Patients

- **How to Share**: Patient portals allow individuals to access their health records at any time. If a portal is unavailable, health care provider organizations must provide the individual with access to their PHI in the form and format requested, if readily producible in that form and format, or in a readable hard copy form or other form as agreed to by the covered entity and individual. Reasonable steps must be taken to verify the identity of an individual making a request for access as under 45 CFR Part 164.514(h). HIPAA does not mandate the form of verification used and leaves the type and manner of the verification to the discretion and professional judgment of the health care provider organization. However, verification processes and measures must not create barriers to or unreasonably delay the individual from accessing their PHI. Verification may be done orally or in writing. Access to the PHI requested, in whole, or in part (if certain access may be denied as outlined in **Appendix A: Compendium of Federal and State Regulations for Data Sharing**), must be provided no later than 30 days from receiving the individual's request. The 30 days is an outer limit and covered entities should respond as soon as possible.

Health care provider organizations may provide a summary of the PHI requested, in lieu of access to the PHI, or an explanation of the PHI to which access has been provided in addition to that PHI, so long as the individual, in advance:

- Chooses to receive the summary or explanation (including in the electronic or paper form being offered by the covered entity); and
- Agrees to any fees that may be charged by the covered entity for the summary or explanation.

A cost-based fee may be imposed if the individual requests a copy of the PHI (or agrees to receive a summary or explanation of the information). The fee may include only the cost of:

- Labor for copying the PHI requested by the individual, whether in paper or electronic form;
- Supplies for creating the paper copy or electronic media (e.g., CD or USB drive) if the individual requests that the electronic copy be provided on portable media;
- Postage, when the individual requests that the copy, or the summary or explanation, be mailed; and
- Preparation of an explanation or summary of the PHI, if agreed to by the individual.

The fee may not include costs associated with verification; documentation; searching for and retrieving the PHI; maintaining systems; recouping capital for data access, storage, or infrastructure; or other costs not listed above even if such costs are authorized by State law. A flat fee may be used for all requests for electronic copies of PHI maintained electronically, provided the fee does not exceed $6.50.

Note: Proposed Modifications to HIPAA would strengthen a patient's ability to access their data by:

- Strengthening an individual's rights to inspect their PHI in person, including allowing them to take notes or use personal resources to view or capture images of their PHI;
- Shortening the required response time for covered entities to no later than 15 days, with opportunity for an extension of no more than 15 days;
- Clarifying the form and format required for responding to an individual's request for PHI;
- Requiring covered entities to inform individuals that they retain their right to obtain or direct copies of PHI to a third party when a summary of PHI is provided in lieu of a copy;
- Reducing the identity verification burden on individuals exercising their access rights;
- Requiring covered health care providers and health plans to submit an individual's access request to another health care provider and receive the requested electronic copies of the individual's PHI in an EHR;
- Requiring covered health care providers and health plans to respond to certain records requests received from other covered health care providers and health plans when directed by individuals pursuant to the right of access;
- Limiting the individual right of access to direct the transmission of PHI to a third party to electronic copies of PHI in an EHR;
- Specifying when electronic PHI must be provided to the individual at no charge;
- Amending the permissible fee structure for responding to requests to direct records to a third party; and
- Requiring covered entities to post estimated fee schedules on their websites for access and for disclosures with an individual's valid authorization and, upon request, provide individualized estimates of fees for an individual's request for copies of PHI, and itemized bills for completed requests.

This Guidebook will be updated to reflect the HIPAA modifications if they are approved.

- **Existing Resources**: (See **Appendix B: Resources** for additional resources)
  - Individuals' Right under HIPAA to Access their Health Information – HHS guidance on patient access to PHI.
- **What Work Remains:**
  - **Technical Barriers:**
    - Patient portals provide the most convenient access to data for both patients and health care providers. However, many health care provider organizations, regardless of size, lack this capability.
  - **Policy Barriers:**
    - When PHI must be provided through methods other than a patient portal, there is no standardized process for enabling access, including obtaining written patient requests and verification processes. This may

        cause inefficiencies and delays for patients. Use of electronic verification methods may help to streamline the process.
    - Future improvements can also be made to enhance patient access and should be considered. An example may be allowing patients to access data stored across multiple providers through a single portal, such as the Care Everywhere feature of the Epic EHR system. HIEs could potentially offer a similar feature across EHRs, although notably, there may be legal and policy barriers to this data sharing that should be explored.

  Importantly, consumer perspective on accessing data should be the primary driver of future work to ensure patients' needs are met.

  Note that the proposed modifications to HIPAA, as outlined, and the Cures Act Final Rule, as discussed in **Appendix A: Compendium of Federal and State Regulations for Data Sharing** and the **Key Regulations** section, may impact these processes and patient access.

- **Considerations:**
  - The Office of the National Coordinator for Health Information Technology's (ONC) Cures Act Final Rule supports a patient's control of their health care and their medical record through smartphones and software apps. The goal of the Cures Act Final Rule is to allow patients to access electronic medical records at no additional cost. Patients must be able to access the following PHI:
    - Discharge summary note,
    - History and physical,
    - Progress note,
    - Consultation note,
    - Imaging narrative,
    - Laboratory report narrative,
    - Pathology report narrative, and
    - Procedures note.
  - The Centers for Medicare & Medicaid Services' (CMS) Interoperability and Patient Access Final Rule finalized new policies that help advance interoperability and patient access through regulation of CMS-regulated payers, including Medicare Advantage, Medicaid, Children's Health Insurance Program, and qualified health plan issuers on federally facilitated exchanges.

Data Sharing with Social Service Provider Organizations

- **How to Share:** Currently, health care provider organizations have several options to connect to social service networks and refer their patients. Many of these options are offered by private vendors such as Aunt Bertha, Unite Us, NowPow, and others. Please see the **Social Service Provider Organizations** section of this Guidebook for more information on these data-sharing platforms.

Alternatively, some health care provider organizations have developed unique partnerships directly with local social service organizations, including county agencies or community-based organizations. These partnerships may allow referrals and data sharing among a limited set of partners who frequently work together; however, this approach is resource-intensive and not easily scalable.

Under HIPAA, health care provider organizations may disclose the minimum necessary PHI to social service provider organizations without the individual's consent if the provider believes such disclosures are a necessary component of, or may help further, the individual's health or mental health care.

Note: Proposed Modifications to HIPAA may create an exception to the "minimum necessary" standard for individual-level care coordination and case management uses and disclosures. The minimum necessary standard generally requires covered entities to limit uses and disclosures of PHI to the minimum necessary information needed to accomplish the purpose of each use or disclosure. This proposal would relieve covered entities of the minimum necessary requirement for uses by, disclosures to, or requests by, a health plan or covered health care provider for care coordination and case management activities with respect to an individual, regardless of whether such activities constitute treatment or health care operations. This Guidebook will be updated to reflect the HIPAA modifications if they are approved.

- **Existing Resources:** (See **Appendix B: Resources** for additional resources)
  - FAQ 3008 – HHS FAQ on sharing PHI for continuity of care purposes.
  - See the **Social Service Provider Organizations** section of this Guidebook for more information on social service referral and data-sharing platforms.
- **What Work Remains:**
  - **Technical Barriers:**
    - Existing platforms serve as an intermediary for connecting patients to social service provider organizations, but these platforms have different policies, processes, and networks. They may also have various costs for joining the platform. An interoperable ecosystem in which data can be shared between platforms would promote more effective and efficient data-sharing capabilities to connect patients to food, housing, employment, and other needed resources across networks.
    - One-off partnerships between health care provider organizations and social service provider organizations may be effective for specific data sharing goals, but these arrangements are limited in scope and scale. Efficiencies can be gained by joining broader, interoperable networks.
  - **Policy Barriers:**
    - Providers may be hesitant to share PHI due to a lack of clarity on how data can be shared under HIPAA. However, proposed modifications to

HIPAA may clarify the scope of how data can be shared with social service provider organizations.

- **Considerations:**
    - While not required, health care provider organizations sharing data with social service provider organizations for treatment purposes should obtain patient consent and create a log or audit to track disclosures as a best practice. This information should include, for each disclosure, the name(s) of the entity(-ies) to which the disclosure was made, the date of the disclosure, and a brief description of the patient identifying information disclosed.
    - EHR integration is a priority for most health care providers. Integration allows a single sign-on and facilitates effective closed-loop referrals. Several social service referral and care coordination platforms offer integration, but cost and compatibility with the provider's existing EHR must be considered.

Behavioral Health Provider Organizations

To provide effective treatment and coordinated care, a behavioral health provider organization, including mental health provider organizations and substance use disorder (SUD) treatment provider organizations, may need to send patient information to another health care or social service provider organization for that provider's treatment of the patient. Examples of sharing protected health information (PHI) regarding a patient may include:

- Sharing the patient's name and address, prescribed medications, diagnoses or treatments, including programs/services utilized, and discharge plans to a primary care provider;
- Sharing or accessing PHI for a patient in the event of a medical emergency; or
- Referring a patient with a food security need to a social service agency.

This section applies to data sharing that originates from a behavioral health provider organization, including those subject to federal regulation 42 CFR Part 2 (Part 2).

Overview of Data Sharing

Entities should comply with best practices outlined in the **Health Information Sharing Principles** section of this Guidebook.

Under the Health Insurance Portability and Accountability Act (HIPAA), behavioral health providers not subject to Part 2 (covered entities) are permitted to share PHI, excluding psychotherapy notes, without patient consent and authorization for treatment, payment, and health care operation activities.

This includes disclosing PHI to another health care provider organization who has a medical responsibility for the patient or to public or private-sector entities providing social services (such as housing, income support, or job training), if social service entities are a necessary component of, or may help advance, the individual's health or mental health care.

If an entity is subject to both Part 2 and HIPAA (a Part 2 program), it is responsible for complying with the more protective Part 2 rules, as well as with HIPAA. Under Part 2, SUD patient-identifying information such as patient demographics, diagnosis, prognosis, and treatment information may only be **shared with other health care provider organizations** without written patient consent when:

- PHI is being disclosed to a health care provider who is a treatment/prevention program professional in the same facility/treatment program as the behavioral health SUD treatment provider (employed by the same SUD program);
- A qualified service organization agreement (QSOA) exists; or
- When exchange takes place between a Part 2 program and an entity with administrative control over that program.

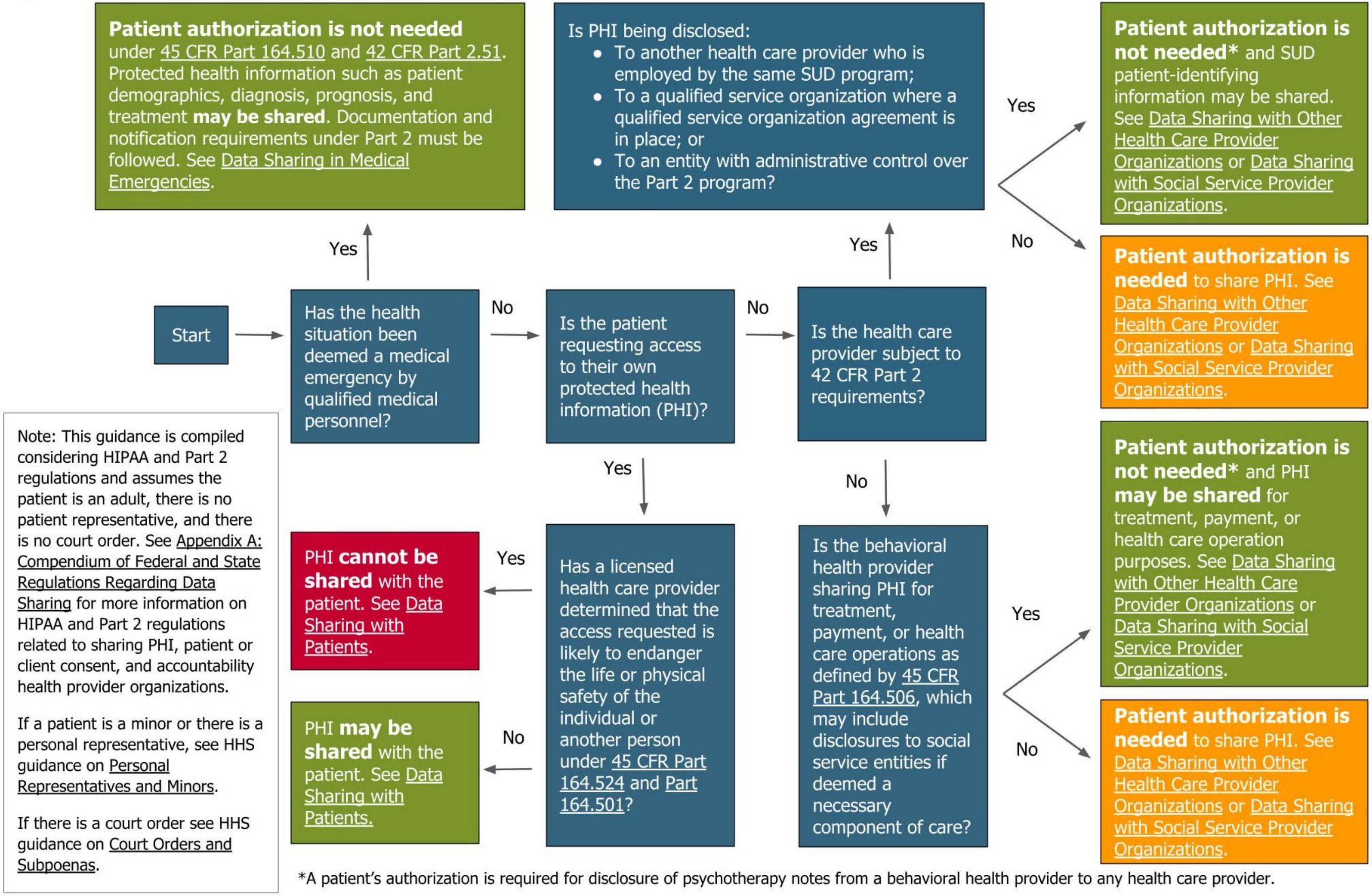
Both HIPAA and Part 2 allow PHI to be **shared during medical emergencies**, but documentation and notification requirements pertaining to Part 2 programs must be followed.

In all other instances, patient authorization is required.

Patient access is permitted under HIPAA and Part 2, including the right to inspect, review, and obtain copies of PHI unless a licensed health care provider has determined the access is reasonably likely to endanger the life or physical safety of the individual or another person.

See **Appendix A: Compendium of Federal and State Regulations for Data Sharing** for more information on HIPAA, Colorado regulations, and 42 CFR Part 2 related to sharing PHI, patient or client consent, and accountability of covered entities and Part 2 programs. Additionally, note that proposed modifications to HIPAA may result in conflicts between HIPAA and Part 2 specifications.

Figure 4. Overview of data sharing by behavioral health provider organization use cases



Start

Has the health situation been deemed a medical emergency by qualified medical personnel?

Patient authorization is not needed under 45 CFR Part 164.510 and 42 CFR Part 2.51. Protected health information such as patient demographics, diagnosis, prognosis, and treatment **may be shared**. Documentation and notification requirements under Part 2 must be followed. See Data Sharing in Medical Emergencies.

Is the patient requesting access to their own protected health information (PHI)?

Has a licensed health care provider determined that the access requested is likely to endanger the life or physical safety of the individual or another person under 45 CFR Part 164.524 and Part 164.501?

PHI **cannot be shared** with the patient. See Data Sharing with Patients.

PHI **may be shared** with the patient. See Data Sharing with Patients.

Is the health care provider subject to 42 CFR Part 2 requirements?

Is PHI being disclosed:

- To another health care provider who is employed by the same SUD program;
- To a qualified service organization where a qualified service organization agreement is in place; or
- To an entity with administrative control over the Part 2 program?

Patient authorization is not needed* and SUD patient-identifying information may be shared. See Data Sharing with Other Health Care Provider Organizations or Data Sharing with Social Service Provider Organizations.

Patient authorization is needed to share PHI. See Data Sharing with Other Health Care Provider Organizations or Data Sharing with Social Service Provider Organizations.

Is the behavioral health provider sharing PHI for treatment, payment, or health care operations as defined by 45 CFR Part 164.506, which may include disclosures to social service entities if deemed a necessary component of care?

Patient authorization is not needed* and PHI **may be shared** for treatment, payment, or health care operation purposes. See Data Sharing with Other Health Care Provider Organizations or Data Sharing with Social Service Provider Organizations.

Patient authorization is needed to share PHI. See Data Sharing with Other Health Care Provider Organizations or Data Sharing with Social Service Provider Organizations.

Note: This guidance is compiled considering HIPAA and Part 2 regulations and assumes the patient is an adult, there is no patient representative, and there is no court order. See Appendix A: Compendium of Federal and State Regulations Regarding Data Sharing for more information on HIPAA and Part 2 regulations related to sharing PHI, patient or client consent, and accountability health provider organizations.

If a patient is a minor or there is a personal representative, see HHS guidance on Personal Representatives and Minors.

If there is a court order see HHS guidance on Court Orders and Subpoenas.

*A patient's authorization is required for disclosure of psychotherapy notes from a behavioral health provider to any health care provider.

Data-Sharing Platforms, Protocols, and Elements

Data Sharing with Other Health Care Provider Organizations

- **How to Share:** For sharing PHI regulated by HIPAA with another health care provider organization, see **Physical Health Provider Organizations; Data-Sharing Platforms, Protocols, and Elements: Data Sharing with Other Health Care Provider Organizations** and **Appendix C: Health Information Exchange and Data Standards** for more information on data-sharing platforms and elements. Note that psychotherapy notes from a behavioral health provider organization require a patient’s authorization for disclosure to any health care provider.

  To disclose PHI regulated by Part 2 to another health care provider organization through a health information exchange (HIE), a patient’s consent must be obtained before disclosing the PHI to an HIE or a QSOA with the HIE must be executed. See 42 CFR Part 2.11 and 42 CFR Part 2.12(c)(4) for more information. If a QSOA is executed, a patient consent form is still needed to enable providers participating in the HIE to view that patient’s SUD patient records (see **Appendix A: Compendium of Federal and State Regulations for Data Sharing** for more information related to obtaining patient consent). HIEs must be able to restrict re-disclosing of a patient's PHI to HIE-participating providers who are not named on a patient’s consent form.

  Part 2 also states that disclosures of PHI must be limited to that information which is necessary to carry out the purpose of the disclosure (see 42 CFR Part 2.13). Each disclosure made with the patient’s written consent must be accompanied by a written statement restricting re-disclosure. See 42 CFR Part 2.32 for acceptable statements. Note that under a Part 2 consent, information may be disclosed multiple times to the physical health provider as long as the consent has not yet expired, and the entities to whom the information is disclosed, the nature of the information, and the purpose for the disclosure specified in the consent form are still the same. Under Colorado regulation 2 CCR 502-1, Section 21.170.3, signed releases of information for behavioral health information are time limited for up to two years. See **Appendix A: Compendium of Federal and State Regulations for Data Sharing** for more information related to obtaining patient consent.
- **Existing Resources**: (See **Appendix B: Resources** for additional resources)
  - Substance Abuse Confidentiality Regulations – Substance Abuse and Mental Health Services Administration (SAMHSA) web page with FAQs and fact sheets regarding substance abuse confidentiality regulations.
    - Disclosure of Substance Use Disorder Patient Records: How Do I Exchange Part 2 Data? – Describes how 42 CFR Part 2 applies to the electronic exchange of health care records with a Part 2 program.
    - Frequently Asked Questions: Applying the Substance Abuse Confidentiality Regulations to Health Information Exchange – SAMHSA FAQs on conducting HIE under Part 2 Regulations.

- Information Related to Mental and Behavioral Health, including Opioid Overdose – U.S. Department of Health and Human Services (HHS) one-stop resource for guidance and other materials on how HIPAA applies to mental health and substance use disorder information.
- Behavioral Health Compliance Toolbox – Resources from Colorado's Office of Behavioral Health (OBH) on compliance with state and federal laws, including examples of HIPAA and Part 2 compliant consent forms.
- Authorization and Consent Forms – Examples of HIPAA and Part 2 authorization, consent, and notice of privacy practice forms from the Colorado Department of Human Services, available in Spanish and English.
- Colorado Regional Health Information Organization (CORHIO) and Quality Health Network (QHN) – CORHIO and QHN are two organizations that provide HIE services in the state of Colorado. HIEs help promote interoperability and ensure that provider organizations are exchanging PHI in accordance with HIPAA and other standard data formats. Individuals should consult CORHIO's website and QHN's website to learn more about services provided.

- **What Work Remains:**
  - **Technical Barriers:**
    - Systems are disparate. There are a multitude of EHR vendors whose products differ in functionality, which makes interoperability across providers and health care systems difficult.
    - Bifurcation of general behavioral health data from Part 2 regulated data may be difficult to operationalize. As a result, all data may need to be treated as being regulated by Part 2, especially when using an HIE for data sharing.
    - Upon a patient's request, a health care provider organization must be able to provide logs that satisfy the requirements of a Part 2 disclosure of PHI using a general designation. HIEs should have these readily available through an automated process. Provider organizations should also be able to obtain all relevant PHI for a patient through both HIEs from a single request.
  - **Policy Barriers:**
    - Adoption of health IT among behavioral health providers is minimal, with upfront cost, consent, and sustainability reported as primary constraints. There are no requirements in place to mandate or incentivize use of health IT for all behavioral health providers. Psychiatrists and psychiatric nurse practitioners were eligible for Meaningful Use EHR incentive programs. However, other behavioral health providers, such as psychologists, clinical social workers, community mental health centers, psychiatric hospitals, residential treatment centers, substance abuse treatment programs, opioid treatment programs, licensed therapists, etc. were ineligible.
    - Currently, there is no standard for which data elements should be disclosed and the information necessary may vary case by case.

However, the Minimum Necessary Standard and 42 CFR Part 2.13 may provide guidance on information that should be included. (See **Appendix C: Health Information Exchange and Data Standards** for more information on data standards).

        - There is also a lack of standard policies and practices in place to dictate how Part 2 PHI can be shared through HIEs, including consent management between provider organizations and HIEs. Lack of centralized storage for patient consent makes the original executed consent difficult to trace and reference. However, solutions to these issues may be informed by OBH, the Behavioral Health Administration, and a Notice of Proposed Rulemaking yet to be released by SAMHSA.

- **Considerations:**
    - For entities using EHRs and HIEs that are unable to bifurcate general behavioral health data and SUD treatment data, all PHI may need to be treated as being regulated by Part 2.
    - Under the HIPAA Privacy Rule, data use agreements ensuring specified safeguards for the PHI are required for use and disclosure of limited data sets (PHI from which certain specified direct identifiers of individuals and their relatives, household members, and employers have been removed) for research, health care operations, and public health purposes.
    - Due to the centralized nature of HIEs, providers may be worried about security and privacy of data. Individuals should consult CORHIO and QHN for more information on how HIEs operate.
    - While HIEs in Colorado operate under an opt-out policy for HIPAA-regulated PHI, this is not the case for Part 2 regulated data. Patient consent must be obtained to share Part 2 data in most situations.
    - Notably, patients may be wary of granting consent to share mental health and SUD data. Patient perspective and education campaigns may be needed to promote data sharing.
    - CORHIO has merged with Health Current, an HIE servicing the state of Arizona which uses a statewide data sharing model. Colorado-specific solutions should leverage current models, such as Health Current's and others. An environmental scan of consent models is being conducted by OeHI in Fall 2021.

Data Sharing in Medical Emergencies

- **How to Share:** Data sharing is permitted in the event of a medical emergency, including sharing Part 2 regulated data. See **Physical Health Provider Organizations; Data-Sharing Platforms, Protocols, and Elements: Data Sharing in Medical Emergencies** for more information on how data may be accessed under HIPAA regulations.

  Under 42 CFR Part 2.51(c), immediately following disclosure, the Part 2 program must document, in writing, the disclosure in the patient's records, including:

  - The name of the medical personnel to whom disclosure was made and their affiliation with any health care facility;
  - The name of the individual making the disclosure;
  - The date and time of the disclosure; and
  - The nature of the emergency.
- **Existing Resources**: (See **Appendix B: Resources** for additional resources)
  - Substance Abuse Confidentiality Regulations – SAMHSA web page with FAQs and fact sheets regarding substance abuse confidentiality regulations.
    - Disclosure of Substance Use Disorder Patient Records: How Do I Exchange Part 2 Data? – Describes how 42 CFR Part 2 applies to the electronic exchange of health care records with a Part 2 program.
    - Frequently Asked Questions: Applying the Substance Abuse Confidentiality Regulations to Health Information Exchange – SAMHSA FAQs on conducting HIE under Part 2.
  - Information Related to Mental and Behavioral Health, including Opioid Overdose – HHS one-stop resource for guidance and other materials on how HIPAA applies to mental health and SUD information.
- **What Work Remains:**
  - **Technical Barriers:**
    - Due to issues with bifurcation of data, lack of standard policies on sharing Part 2 data through HIEs, and patient concerns with disclosing mental health and SUD data as discussed in the **Data Sharing with Other Health Care Provider Organizations** section, pertinent Part 2 data may not be accessible via HIEs during a medical emergency. Patient data may also be limited due to barriers that prevent health care provider organizations from connecting to an HIE.
  - **Policy Barriers:**
    - Using the "break glass" functionality to access PHI may not limit inappropriate access to a patient's PHI.
    - Policies that rely on audit logs may also create administrative burden on provider organizations to review access to a patient's PHI.
- **Considerations:**
  - It is the responsibility of the Part 2 health care provider organization to ensure documentation has occurred when a disclosure is made in connection with a medical emergency. Therefore, data systems must be designed to ensure that the Part 2 program is notified when a "break the glass" disclosure occurs and Part 2 records are released pursuant to a medical emergency. The notification should include all information that the Part 2 program is required to document in the patient's records.

Data Sharing with Patients

- **How to Share:** Patient access is not prohibited under Part 2 regulations. See **Physical Health Provider Organizations; Data-Sharing Platforms, Protocols, and Elements: Data Sharing with Patients** for more information on how data may be accessed as well as any existing resources, work that remains, and considerations.

Data Sharing with Social Service Provider Organizations

- **How to Share:** Behavioral health provider organizations can share data regulated by HIPAA using the same methods as outlined in the Physical Health Provider Organizations section of this Guidebook. See **Physical Health Provider Organizations; Data-Sharing Platforms, Protocols, and Elements: Data Sharing with Social Service Provider Organizations**.

  Patient consent must be obtained to share data regulated by Part 2 with social service providers in most cases. Part 2 data may only be shared without obtaining the individual's consent when the social service provider is employed by the same SUD program or when a QSOA exists with the social service provider. See **Appendix A: Compendium of Federal and State Regulations for Data Sharing**.
- **Existing Resources**: (See **Appendix B: Resources** for additional resources)
  - See the **Social Service Provider Organizations** section of this Guidebook for more information on social service referral and data-sharing platforms.
- **What Work Remains:**
  - **Technical Barriers:**
    - In addition to the technical barriers that are presented in the Data Sharing with Social Service Provider Organizations under the Physical Health Provider Organization section of this Guidebook, bifurcation of HIPAA and Part 2 data may further complicate data sharing capabilities and future solutions, such as system integration.
  - **Policy Barriers:**
    - In addition to the policy barriers that are presented in the Data Sharing with Social Service Provider Organizations under the Physical Health Provider Organization section of this Guidebook, patients may be more hesitant to grant consent to share their behavioral health data. Patient feedback and education campaigns may be needed to guide solutions to sharing PHI from a behavioral health organization to a social service provider organization.
    - Lack of policies around consent management between provider organizations may also create difficulties with promoting interoperability.
- **Considerations:**
  - Health care provider organizations sharing data with social service provider organizations should create a log or audit to track disclosures. This information should include, for each disclosure, the name(s) of the entity(-ies) to which the disclosure was made, the date of the disclosure, and a brief description of the patient identifying information disclosed.

Social Service Provider Organizations

There is growing recognition that social factors have a significant impact on health outcomes. This recognition has been accompanied by a push to share information between health care provider organizations and social service provider organizations. In Colorado, many efforts are underway to share social service data. Collectively, these efforts are fueling a statewide movement toward social-health information exchange (S-HIE). This section of the Guidebook outlines the current landscape for sharing data, such as personally identifiable information (PII) or protected health information (PHI), for care coordination purposes, including the work that remains to promote interoperability among systems. As Colorado makes progress in S-HIE, this Guidebook will be updated accordingly.

Overview of Data Sharing

The category of “social service provider organizations” includes an enormous variety of organization types, such as community-based organizations (CBOs) and state agencies, which are all subject to differing privacy requirements and regulations. Not only can regulations differ by organization and agency, but they may also differ by program, such as food security, housing security, housing quality, employment, and others.

As there is currently no overarching regulatory framework that governs social service data, organizations that are interested in sharing social service data must take a more targeted approach:

Step 1: Specify the data to be shared in as much detail as possible. For example, organizations may wish to share enrollment data for a specific government program or to send a closed-loop referral to a trusted community partner.

Step 2: Understand the regulations and policies that govern the data of interest. Various federal and state regulations may be relevant, depending on the source of the data. Organizational policies may also be important, especially if the data is not subject to regulations.

Step 3: Identify existing solutions and best practices to share the data of interest, if available. Research existing solutions that may meet the data-sharing need. If none exist, partners may wish to develop a new solution.

Social service provider organizations have several existing options for sharing different types of social data with other organizations; however, it is not currently possible to share all types of data through a statewide system. The targeted approach described above can assist social service provider organizations in selecting the best option to meet data sharing goals.

Data-Sharing Platforms, Protocols, and Elements

Data Sharing for Care Coordination Among Provider Organizations

- **How to Share:** There are several platforms that enable social data sharing. Although the platforms share similar capabilities, they can be categorized into the following:
    - **National Referral Networks:** These commercial platforms seek to close health care gaps by connecting care providers with community resources in their area. They partner with clients across the country to enable data sharing for care coordination among physical health, behavioral health, and social service provider organizations in the client's region. Most integrate with several EHRs and have the ability to conduct population health analytics. These networks include, but are not limited to:
        - Aunt Bertha
        - Unite Us
        - NowPow
        - Activate Care
    - **Colorado Referral Networks:** These platforms provide many of the same features as the national referral networks, but were developed by and for specific regions of Colorado:
        - Community Resource Network – a community information exchange developed and operated by Quality Health Network (QHN) that centralizes social, behavioral, and medical data.
        - Boulder County Connect – a platform that allows clients to track and manage the benefits they receive through the Boulder County Department of Housing and Human Services. Clients can also manage existing benefits and supports, learn about additional services, and connect with county staff. The platform also serves as a case management and referral system for community-based organizations in Boulder County.
        - Colorado Community Managed Care Network's "Community Care Team Models" – an interoperable community strategy that builds on and integrates existing systems while building capacity in communities to support their ability to work on shared goals.
    - **Community Resource Inventories:** The primary feature of these platforms is providing access to a database of information about community resources:
        - 211 Colorado – a platform for individuals to access a statewide online database of community resources and contact someone at the 211 Help Center to learn about available services.
        - Hunger Free Colorado – the statewide nonprofit organization maintains an online food finder database and operates a food resource hotline to connect people to food resources.
    - **Community Interoperability Platform:** While referral networks focus on building out a network of connected partners, a community interoperability platform focuses on automating workflows between partners working together on a specific program or initiative.

    - Julota – an interoperable platform that offers the ability to manage the consent and multidirectional sharing of PII and PHI between health care, including behavioral health, and emergency responders, law enforcement, public health, and social service organization providers to support specific initiatives.

  These existing platforms are taking the targeted approach recommended in this Guidebook to share social data. For example, the Julota platform is Criminal Justice Information System (CJIS) compliant to enable the platform's focus on law enforcement and first responder programs. As another example, the Aunt Bertha platform has partnered with housing agencies to integrate homeless management information systems (HMIS). Over time, platforms will be able to share additional types of social data.

- **Existing Resources:** (See **Appendix B: Resources** for additional resources)
  - Community Resource Referral Platforms: A Guide for Health Care Organizations – An overview of community resource referral platforms developed by the Social Interventions Research & Evaluation Network.
  - Advancing a Coordinated Ecosystem for a Social Health Information Exchange in Colorado – An overview of S-HIE in Colorado, including benefits, governance, and ongoing efforts.
  - OeHI and the Colorado Health Institute are working with stakeholders to develop a Manual for Social Data Interoperability Standards in Colorado, which will be referenced in this Guidebook for use once finalized.
- **What Work Remains:**
  - **Technical Barriers:**
    - While there are several platforms for data sharing, interoperability remains a challenge. Efforts are underway to connect specific platforms, but it is not currently possible to share information among all networks and across the state. An interoperable S-HIE ecosystem is needed. This refers to a coordinated infrastructure that would enable safe and secure information sharing among health care and social service provider organizations, regardless of what technology users choose to adopt.
  - **Policy Barriers:**
    - Policies pertaining to privacy, consent, and data management are significant concerns due to the privacy of information as well as the varying strict federal regulations that govern different agencies and ensuring these regulations are met.
    - There are significant financial and operational differences between health care provider organizations and social service provider organizations. Partners will need to identify and navigate those differences to work together effectively. For example, there may be a financial incentive for a physical health provider to refer a patient to a social service provider, while there may be a financial *dis*incentive for the social service provider to accept that referral.
- **Considerations:**

- When developing and using platforms, the following best practices should be followed:
    - The platform should have a standardized, consistent screening protocol. The screening process should capture a set of standardized domains, use an established screening tool, and use established code sets for interoperability.
    - The platform should have or be integrated with a comprehensive resource inventory for health and community-based social services that is easily accessible to the public.
    - The platform should enable bidirectional referrals, meaning that not only can provider organizations make referrals to one another, but they can also determine whether the services were furnished and met the needs of the individual.
    - Fully interoperable platforms can allow for data to be aggregated for the purposes of population health analytics. This may provide a more complete view of population health within communities and inform community-level assessment and planning.
- Strong partnerships among health care provider organizations, state agencies, CBOs, and others are needed to support an S-HIE ecosystem. Regional collaborations are building these relationships across the state. For example, the Metro Denver Partnership for Health (MDPH) – a cross-sector collaboration of local public health agencies, health care systems, human service agencies, and other partners – is working to advance the vision for an interoperable S-HIE ecosystem in the metro Denver area. This includes creating a collaborative governance structure, establishing agreements among partners to prevent siloes across care management systems and platforms, and designing a funding model to support the S-HIE ecosystem.

Appendix A: Compendium of Federal and State Regulations for Data Sharing

HIPAA

The Health Insurance Portability and Accountability Act (HIPAA, 45 CFR Part 164) is a federal law that requires the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge. The U.S. Department of Health and Human Services (HHS) issued the HIPAA Privacy Rule (Privacy Rule) to implement the requirements of HIPAA. The Privacy Rule addresses the use and disclosure of individuals' protected health information (PHI) by entities subject to the Privacy Rule. The HIPAA Privacy Rule protects all individually identifiable PHI held or transmitted by a covered entity or its business associates in any form (electronic, paper, or oral).

The HIPAA Security Rule (Security Rule) protects a subset of information covered by the Privacy Rule, including all individually identifiable health information a covered entity creates, receives, maintains, or transmits in electronic form. This information is called "electronic protected health information" (e-PHI). The Security Rule does not apply to PHI transmitted orally or in writing.

Clarification of Regulation for Health Information Sharing

- **Overview:** Under the Privacy Rule, 45 CFR Part 164.506, a health care provider organization (a covered entity) can disclose PHI (including e-PHI) about an individual, without the individual's authorization, for treatment, payment, and health care operation activities. See 45 CFR Part 164.506 for the exact definition of treatment, payment, and health care operations, including examples. This includes a physical or behavioral health provider not regulated by 42 CFR Part 2, sharing PHI with another health care provider without patient authorization and consent, assuming both covered entities have or had a relationship with the individual and the PHI pertains to the relationship. Note that a patient's authorization is required for disclosure of psychotherapy notes from a behavioral health provider to any health care provider.

  HIPAA's definition for treatment includes the coordination or management of health care by a health care provider with a third party. Health care means care, services, or supplies related to the health of an individual. Thus, health care providers who believe that disclosures to certain social service entities are a necessary component of, or may help further, the individual's health or mental health care may disclose the minimum necessary PHI to such entities without the individual's authorization. Examples include a provider disclosing PHI about a patient needing mental health care supportive housing to a service agency that arranges such services for individuals. A covered entity may also disclose PHI to such entities pursuant to an authorization signed by the individual.

Note: Proposed Modifications to HIPAA may amend the definition of health care operations to clarify the scope of permitted uses and disclosures for individual-level care coordination and case management that constitute health care operations.

The modifications may further clarify the scope of covered entities' abilities to disclose PHI to social services agencies, community-based organizations, home and community-based service (HCBS) providers, and other similar third parties that provide health-related services, to facilitate coordination of care and case management for individuals.

This Guidebook will be updated to reflect the HIPAA modifications if they are approved.

Under HIPAA, 45 CFR Part 164.510(3), if an individual is not present, or the opportunity to agree or object to the use or disclosure cannot practicably be provided because of the individual's incapacity or an emergency circumstance, the covered entity may, in the exercise of professional judgment, determine whether the disclosure is in the best interest of the individual and, if so, disclose only the PHI that is directly relevant to the person's involvement with the individual's care or payment related to the individual's health care or needed for notification purposes. A covered entity may also use or disclose PHI, if the covered entity, in good faith, believes the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public and is disclosed to persons reasonably able to prevent or lessen the threat or is necessary for law enforcement authorities. See 45 CFR Part 164.512 for more information.

Note: Proposed Modifications to HIPAA may replace the privacy standard that permits covered entities to make certain uses and disclosures of PHI based on their "professional judgment" with a standard permitting such uses or disclosures based on a covered entity's "good faith belief" that the use or disclosure is in the best interest of the individual. The proposed standard is more permissive in that it would presume a covered entity's good faith, but this presumption could be overcome with evidence of bad faith.

Further, the modifications would expand the ability of covered entities to disclose PHI to avert a threat to health or safety when a harm is "serious and reasonably foreseeable," instead of the current stricter standard which requires a "serious and imminent" threat to health or safety.

This Guidebook will be updated to reflect the HIPAA modifications if they are approved.

Individuals have the right to authorize sharing of their own personally identifiable information. Under the Privacy Rule, a patient also has the right to inspect, review, and obtain copies of their patient health information, including the right to receive an accounting of disclosures of protected health information made by a covered entity in the six years prior to the date on which the accounting is requested. A provider is responsible for enabling such patient access. Psychotherapy notes and information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding are excluded from the right of access. Access to PHI may be denied if a licensed health care provider determines that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person. See 45 CFR Part 164.524 and 45 CFR Part 164.501 for a complete list of the grounds and conditions for denial of access and for the definition of psychotherapy notes.

- **Pertinent Resources:** (See **Appendix B: Resources** for additional resources)
  - Permitted Uses and Disclosures: Exchange for Treatment – HHS fact sheet that provides a brief overview of data-sharing for covered entities.
  - 45 CFR Part 164.501 – Definition of treatment and psychotherapy notes.
  - 45 CFR Part 164.506 – Uses and disclosures to carry out treatment, payment, or health care operations.
  - 45 CFR Part 164.524 – Access of individuals to PHI.
  - 45 CFR Part 164.528 – Accounting of disclosures of PHI.
  - FAQ 2046 – HHS FAQ on circumstances in which a covered entity may deny an individual's request for access to the individual's PHI.
  - FAQ 2088 – HHS FAQ on HIPAA protections on mental health information compared to other health information.
  - FAQ 3008 – HHS FAQ on sharing PHI for continuity of care purposes.
  - Information Related to Mental and Behavioral Health, Including Opioid Overdose – HHS one-stop resource for guidance and other materials on how HIPAA applies to mental health and SUD information.

Patient or Client Consent and Consent Management

- **Overview:** Under the HIPAA Privacy Rule, covered entities must develop a Notice of Privacy Practices to be provided to patients at their first office visit and receive the patient's written acknowledgement that notice has been received. A patient may refuse to sign the acknowledgement; in which case, the refusal must be documented in the patient record.

  In emergency treatment situations, the provider is relieved of the need to request acknowledgement. However, the provider must furnish its privacy practice notice to the patient as practicable after the emergency abates.

Note: Proposed Modifications to HIPAA may eliminate the requirement to obtain an individual's written acknowledgement of receipt of a direct treatment provider's Notice of Privacy Practices.

Further, the required contents of a Notice of Privacy Practices may be modified to clarify an individual's rights with respect to their PHI and how to exercise those rights.

This Guidebook will be updated to reflect the HIPAA modifications if they are approved.

The Privacy Rule permits, but does not require, a covered entity to voluntarily obtain patient consent for uses and disclosures of PHI for treatment, payment, and health care operations. However, use of a patient consent form that specifies methods by which a patient agrees to use their PHI for routine purposes as identified by 45 CFR Part 164.506 may provide an extra measure of protection if investigated for HIPAA noncompliance.

Authorizations are required by the Privacy Rule for uses and disclosures of PHI not otherwise allowed by the Privacy Rule. Where the Privacy Rule requires patient authorization, voluntary consent is not sufficient to permit a use or disclosure of protected health information unless it also satisfies the requirements of a valid authorization. An authorization gives covered entities permission to use PHI for specified purposes, which are generally other than treatment, payment, or health care operations, or to disclose PHI to a third party specified by the individual. An authorization must specify a number of elements, including a description of the protected health information to be used and disclosed, the person authorized to make the use or disclosure, the person to whom the covered entity may make the disclosure, an expiration date, and, in some cases, the purpose for which the information may be used or disclosed. Note that under Colorado regulation 2 CCR 502-1, Section 21.170.3, signed releases of information for behavioral health information are time limited for up to two years.

For patient access, a covered entity may require individuals to request access to PHI in writing, provided individuals are informed of this requirement. Electronic means of requesting access, such as email or secure web portal, are permissible. In addition, a covered entity may require individuals to use the entity's own supplied form, provided use of the form does not create a barrier to or unreasonably delay the individual from obtaining access to the PHI. Under 45 CFR Part 164.514(h), covered entities must take reasonable steps to verify the identity of an individual making a request for access.

- **Pertinent Resources:** (See **Appendix B: Resources** for additional resources)
    - Summary of the HIPAA Privacy Rule – HHS guidance on when to use an authorization and information that must be included in the authorization.

    - 45 CFR Part 164.520 – Notice of Privacy Practices for Protected Health Information.
    - HHS FAQs on Authorizations – FAQs regarding patient authorizations.
    - Authorization and Consent Forms – Examples of HIPAA and Part 2 authorization, consent, and notice of privacy practice forms from the Colorado Department of Human Services, available in Spanish and English.
    - Model Notices of Privacy Practices – HHS model notices of privacy practices using plain language and approachable designs as required under HIPAA Privacy Rule.
    - The HIPAA Privacy Rule: Three Key Forms – American Academy of Family Physicians guidance on notice of privacy practices, authorization form, and patient consent form with sample forms for use.
    - Behavioral Health Compliance Toolbox – Resources from Colorado's Office of Behavioral Health (OBH) on compliance with state and federal laws.
        - HIPAA Elements of a Valid Authorization – Uses and Disclosures for Which an Authorization is Required: Core Elements and Requirements – OBH checklist for provider organizations to determine if the consent form they are using is HIPAA-compliant.

Accountability

- **Overview:** Under the HIPAA Privacy Rule, a covered entity or its business associates must maintain reasonable and appropriate administrative, technical, and physical safeguards to prevent intentional or unintentional use or disclosure of PHI. The Security Rule further specifies that covered entities must maintain the same level of safeguards to protect e-PHI.

  For internal uses, under the HIPAA Privacy Rule, a covered entity must develop and implement policies and procedures that restrict access and uses of PHI based on the specific roles of the members of their workforce. These policies and procedures must identify the persons, or classes of persons, in the workforce who need access to PHI to carry out their duties, the categories of PHI to which access is needed, and any conditions under which they need the information to do their jobs. After a receiving provider organization has obtained the PHI, in accordance with HIPAA, it is responsible for safeguarding the PHI and otherwise complying with HIPAA, including with respect to subsequent uses or disclosures or any breaches that occur. The disclosing entity is responsible under HIPAA for disclosing the PHI to the receiving provider organization in a permitted and secure manner, which includes sending the PHI securely and taking reasonable steps to send it to the right address.

  Covered entities must also establish and implement policies and procedures (which may be standard protocols) for routine, recurring disclosures, or requests for disclosures, that limit the PHI disclosed to the minimum amount reasonably necessary to achieve the purpose of the disclosure. Individual review of each disclosure is not required. For non-routine, non-recurring disclosures, or requests for disclosures that it makes, a covered entity must develop criteria designed to limit disclosures to the information reasonably necessary to accomplish the purpose of the disclosure and review each of these requests individually in accordance with the established criteria. Provider organizations may implement a procedure that includes records request/release forms that specify the type of records requested, the type of records that should be excluded, and the timeframe for which the records are requested. Entities should also develop protocols that outline who is authorized to request and release PHI. Common routine and recurring disclosures entities should consider include, but are not limited to:

- An initial referral from a physical health provider to a behavioral health provider.
- A patient-initiated contact with a behavioral health provider that results in a records request from the behavioral health provider organization to the physical health provider organization.
- An ongoing relationship between a physical health provider, a behavioral health provider, and a mutual patient during which a concerted effort to coordinate care and continuously disclose PHI arises.

Under [45 CFR Part 164.528](), an individual has a right to receive an accounting of disclosures of PHI made by a covered entity in the six years prior to the date on which the accounting is requested, except for disclosures:

- To carry out treatment, payment and health care operations;
- To individuals of protected health information about them;
- Incident to a use or disclosure otherwise permitted or required by this subpart;
- Pursuant to an authorization;
- For the facility's directory or to persons involved in the individual's care or other notification purposes;
- For national security or intelligence purposes;
- To correctional institutions or law enforcement officials;
- As part of a limited data set in accordance with Part 164.514; or
- That occurred prior to the compliance date for the covered entity.

However, creation of a log to account for all disclosures may be useful in the event of an audit or security breach.

Under the Breach Notification Rule, following a breach of unsecured PHI, covered entities are required to provide notification of the breach to the affected individuals, the HHS Secretary, and in some circumstances, to the media.

- **Pertinent Resources:** (See **Appendix B: Resources** for additional resources)
    - 45 CFR Part 164.528 – Accounting of Disclosures of Protected Health Information.
    - 45 CFR Part 164.408 – Notice of a Breach to the Secretary.
    - Incidental Uses and Disclosures – General provision and reasonable safeguards.

- Security Rule Guidance Material – HHS materials providing guidance on the HIPAA Security Rule.
- Submitting Notice of a Breach to the Secretary – HHS guidance on how and when to submit a notice of a breach to the HHS Secretary.

42 CFR Part 2

Title 42 of the Code of Federal Regulations Part 2: Confidentiality of Substance Use Disorder Patient Records (42 CFR Part 2 or Part 2) is a federal law administered by the Substance Abuse and Mental Health Services Administration. Part 2 ensures that a patient receiving substance use disorder (SUD) treatment in a Part 2 program does not face adverse consequences in relation to issues such as criminal proceedings and domestic proceedings or employment. Part 2 protects the confidentiality of SUD patient records and protected health information (PHI) by restricting the circumstances under which Part 2 Programs or other lawful holders can disclose such records. If an entity is subject to both Part 2 and HIPAA, it is responsible for complying with the more protective Part 2 rules, as well as with HIPAA.

A Part 2 program is an individual, entity, or identified unit within a general medical facility that is federally assisted and holds itself out as providing, and provides, SUD diagnosis, treatment, or referral for treatment. A Part 2 program also includes medical personnel or other staff in a general medical facility whose primary function is the provision of SUD diagnosis, treatment, or referral and who are identified as such providers. See 42 CFR Part 2.11 and Disclosure of Substance Use Disorder Patient Records: Does Part 2 Apply to Me? for additional guidance and applicability.

Clarification of Regulation for Health Information Sharing

- **Overview:** Under Part 2, SUD patient identifying information such as patient demographics, diagnosis, prognosis, and treatment information can be shared without patient authorization for treatment, payment, or health care operations in the following circumstances:
  - When a qualified service organization agreement (QSOA) exists; or
  - When the exchange takes place between a Part 2 program and an entity with administrative control over that program.

  Therefore, to share PHI with another health care provider, including a social service provider organization, without patient authorization, both providers must be employed by the same SUD program, or the provider must be employed by a qualified service organization (QSO) that is providing services to the SUD program. See 42 CFR Part 2.11 for more information. In all other instances, patient authorization is required.

  Each disclosure made with the patient's written consent must be accompanied by a prohibition on redisclosure statement. See **Behavioral Health Provider**

Organizations; Data-Sharing Platforms, Protocols, and Elements: Data Sharing with Other Health Care Providers for more information on this data-sharing protocol.

Note that while Part 2 PHI can be shared within a Part 2 program or between a Part 2 program and an entity that has direct administrative control over the program, PHI may not be exchanged among all of the programs and personnel that fall under the umbrella of the entity that has administrative control over the Part 2 program. A QSOA would be required to enable information exchange without patient consent in this situation.

Under 42 CFR Part 2.51 PHI regulated by Part 2 may be disclosed in a medical emergency. PHI may be disclosed to medical personnel or accessed by a treating provider to the extent necessary to:

- Meet a medical emergency in which the patient's prior written consent cannot be obtained; or
- Meet a medical emergency in which a Part 2 program is closed and unable to provide services or obtain the prior written consent of the patient, during a temporary state of emergency declared by a state or federal authority as the result of a natural or major disaster, until such time that the Part 2 program resumes operations.

Any health care provider who is treating the patient for a medical emergency can make the determination that a medical emergency exists. The Part 2 program is not required to make the determination. Health care providers regulated by Part 2 must document a number of elements immediately following the disclosure of PHI. See **Behavioral Health Provider Organizations; Data-Sharing Platforms, Protocols, and Elements: Data Sharing in Medical Emergencies** for more information on data-sharing protocols.

Under 42 CFR Part 2.23, patient access is not prohibited. A Part 2 program is not prohibited from giving a patient access to their own records, including the opportunity to inspect and copy any records that the Part 2 program maintains about the patient. Information obtained by patient access is subject to the restriction on use of this information to initiate or substantiate any criminal charges against the patient or to conduct any criminal investigation of the patient as provided for under 42 CFR Part 2.12(d)(1).

- **Pertinent Resources:** (See **Appendix B: Resources** for additional resources)
  - 42 CFR Part 2 – Confidentiality of SUD patient records.
  - Fact Sheet: SAMHSA 42 CFR Part 2 Revised Rule – Outlines several major sections of Part 2 that were revised in July 2020.
  - Disclosure of Substance Use Disorder Patient Records: Does Part 2 Apply to Me? – Defines a 42 CFR Part 2 program and how health care providers can determine how Part 2 applies to them.

  - Frequently Asked Questions: Applying the Substance Abuse Confidentiality Regulations to Health Information Exchange – SAMHSA FAQs on conducting HIE under Part 2 Regulations, including in medical emergencies.

Patient or Client Consent and Consent Management

- **Overview:** A written consent to a disclosure of PHI under Part 2 regulations may be paper or electronic and must include a number of specifications. See 42 CFR Part 2.31 for required consent elements. Note that under Colorado regulation 2 CCR 502-1, Section 21.170.3, signed releases of information are time limited for up to two years. Patients may revoke their consent at any time and disclosures for the purpose of payment and health care operations are permitted with written consent. Each disclosure made with the patient's written consent must be accompanied by a written statement restricting re-disclosure. See 42 CFR Part 2.32 for acceptable statements.

  Note that patients may disclose their PHI using a general designation under a Part 2 consent but as a best practice should be advised by the health care provider organization of the extent to which their information can be disclosed under a general designation.

  Under 42 CFR Part 2.23, a patient's written consent or other authorization under the regulations is not required in order to provide a patient access to their own records.
- **Pertinent Resources:** (See **Appendix B: Resources** for additional resources)
  - Fact Sheet: SAMHSA 42 CFR Part 2 Revised Rule – Outlines several major sections of Part 2 that were revised in July 2020.
  - Behavioral Health Compliance Toolbox – Resources from Colorado's Office of Behavioral Health on compliance with state and federal laws.
    - 42 CFR Part 2 Elements of a Valid Consent: Elements and Requirements – Checklist for provider organizations to determine if the consent form they are using is compliant with Part 2 regulations.
  - Authorization and Consent Forms – Examples of HIPAA and Part 2 authorization, consent, and notice of privacy practice forms from the Colorado Department of Human Services, available in Spanish and English.

Accountability

- **Overview:** Under 42 CFR Part 2.16, the Part 2 program or other lawful holder of PHI must have formal policies and procedures in place to reasonably protect against unauthorized use and disclosure of PHI and to protect against reasonably anticipated threats or hazards to the security of PHI. These formal policies and procedures must address paper records and electronic records and how they are created, transferred and transmitted, received, removed, destroyed, maintained, accessed, and rendered in a manner that creates low risk of re-identification.

Under 42 CFR Part 2.13(d), patients who have consented to disclose their patient identifying information using a general designation must be provided a list of entities to which their information has been disclosed pursuant to the general designation, when requested. Patient requests must be made in writing and are limited to disclosures made within the past two years. The entity that discloses the information must respond within 30 or fewer days of receipt of the written request, and must provide, for each disclosure, the name(s) of the entity(-ies) to which the disclosure was made, the date of the disclosure, and a brief description of the patient identifying information disclosed.

- **Pertinent Resources:** (See **Appendix B: Resources** for additional resources)
    - 42 CFR Part 2 – Confidentiality of SUD patient records.
    - Fact Sheet: SAMHSA 42 CFR Part 2 Revised Rule – Outlines several major sections of Part 2 that were revised in July 2020.

Colorado Regulations for Data Sharing

Colorado has several regulations applicable to data sharing and privacy of protected health information (PHI) and personally identifiable information (PII). The most pertinent guidance of each is summarized below. Note that, under 45 CFR Part 160, Subpart B, state laws that are contrary to HIPAA's Privacy Rule are preempted by the federal requirements unless a specific exception applies. Examples of exceptions include if the state law:

1. Relates to the privacy of individually identifiable health information and provides greater privacy protections or privacy rights with respect to such information.
2. Provides for the reporting of disease or injury, child abuse, birth, or death, or for public health surveillance, investigation, or intervention; or
3. Requires certain health plan reporting, such as for management or financial audits. In these circumstances, a covered entity is not required to comply with a contrary provision of the Privacy Rule.

Clarification of Regulation for Health Information Sharing

- **Overview:** Several Colorado regulations require patient health information to be held confidential, unless permitted to be disclosed by federal law, or for other exceptions, such as with the expressed consent of the patient. These regulations are summarized below:
    - CRS 10-16-423: Medical information in the custody of health maintenance organizations must be kept confidential and shall not be disclosed to any person unless required or permitted by state or federal law or for other exceptions, such as with the expressed consent of the enrollee or applicant.
    - CRS 10-16-1003: PHI collected for or by a health cooperative is subject to HIPAA. This includes ensuring information disclosed is restricted to the minimum amount of information necessary to accomplish the purpose and allowing individuals the right to know how PHI has been used or maintained, and to review and copy the information.

- CRS 12-245-220: Mental health professionals are prevented from disclosing any confidential communications made by the client or advice given to the client without the consent of the client. Exceptions described in CRS 12-245-220(2) include when a lawsuit or complaint is filed; services provided are being reviewed by a board, governing board, or professional review committee; and if there is a threat or behavior that in the reasonable judgment of the licensee, creates an articulable and significant threat to health or safety against a school or its occupants.
- CRS 27-81-113: Pertaining to persons with substance use disorders, persons intoxicated by alcohol and persons under the influence of substances, registration and other records of treatment facilities are confidential and fully protected as outlined in 42 CFR Part 2 and are privileged to the patient (see **42 CFR Part 2**).
- 2 CCR 502-1 Rule 21.170.3: An agency that is licensed or designated by the Colorado Department of Human Services must comply with release of information regulations pursuant to 42 CFR Part 2 and HIPAA.
- CRS 6-1-715: Social security numbers (SSN) must be kept confidential, and persons and entities are restricted from publicly posting or displaying an individual's SSN, printing an SSN on a card or mailings, or requiring an individual to transmit or use their SSN without proper secured connection, authentication, or encryption, as described. Note that this section does not apply to:
    - Documents or records that are recorded or required to be open to the public pursuant to the constitution or laws of this state or by court rule or order, and this section shall not limit access to these documents or records;
    - An entity that is subject to the federal HIPAA as amended, 42 U.S.C. sec. 1320d to 1320d-9; or
    - Collection, use, or release of an SSN as required, permitted, or authorized by state or federal law or the use of an SSN for internal verification or administrative purposes.

  Note that exceptions are permissible only if conditions outlined in CRS 6-1-715(2) are met.
- CRS 25-3.5-501: Specific to ambulance service reports, the Colorado Department of Public Health and Environment is required to make individualized patient information from its emergency medical service agency patient care database available to health information organization networks for uses allowed under HIPAA.
- CRS 25-1-801 and CRS 25-1-802: Patient records in the custody of a health facility and individual health care providers shall be available to the patient or the patient's personal representative for inspection through the attending health care provider at reasonable times and upon reasonable notice, except records withheld in accordance with 45 CFR 164.524 (see the **HIPAA** section of this Guidebook). A summary of records pertaining to a patient's mental health problems may, upon written request and signed and dated

authorization, be made available to the patient or the patient's personal representative following termination of the treatment program. Copies of the patient's record, in the format requested, must be provided upon request. Fees for these copies may be imposed as in accordance with HIPAA but may not be charged for inspection of records. Note that these parts do not limit the right of a patient, the patient's personal representative, or a person who requests the medical records upon submission of a HIPAA-compliant authorization, or limit or expand a right to inspect the patient's records that is otherwise granted by state statute to the patient, the patient's personal representative, or a person who requests the medical records upon submission of a HIPAA-compliant authorization (see CRS 25-1-803).

- **Pertinent Resources:** (See **Appendix B: Resources** for additional resources)
  - FAQ 399 – U.S. Department of Health and Human Services (HHS) FAQ on HIPAA privacy Rule preempting state laws.

Patient or Client Consent and Consent Management

- **Overview:** 2 CCR 502-1 Rule 21.170.3 requires that signed releases of information for behavioral health data (HIPAA and Part 2 regulated) shall state, at a minimum:
  - Persons who shall receive the information;
  - For what purpose;
  - The information to be released;
  - That it may be revoked by the individual, parent, or legal guardian at any time; and
  - That the release of information shall be time limited up to two years.

  Under CRS 25-1-801(2) and 802(4), all requests by a patient or the patient's personal representative for inspection of the patient's medical records shall be noted with the time and date of the request and the time and date of inspection noted by the attending health care provider or his or her designated representative. The patient or personal representative shall acknowledge the fact of the inspection by dating and signing the record file.
- **Pertinent Resources:** (See **Appendix B: Resources** for additional resources)
  - Behavioral Health Compliance Toolbox – Resources from Colorado's Office of Behavioral Health (OBH) on compliance with state and federal laws.
  - Authorization and Consent Forms – Examples of HIPAA and Part 2 authorization, consent, and notice of privacy practice forms from the Colorado Department of Human Services, available in Spanish and English.

Accountability

- **Overview:** Several Colorado regulations require entities to ensure confidentiality of data and to develop policies and procedures related to securing, accessing, storing, or disposing of PHI and PII, and security breaches. These regulations are summarized below:
  - CRS 25-1-1203: Health plans, health care clearinghouses, and health care providers shall develop policies, procedures, and systems to comply with

federal regulations promulgated by the HHS related to electronic storage and maintenance of medical record information pursuant to federal law.

- CRS 10-16-1003: Health care cooperatives must implement administrative, technical, and physical safeguards for the security of PHI.
- CRS 12-240-142: Each licensed physician and physician assistant must develop a written plan to ensure the security of patient medical records to address storage and proper disposal of patient medical records; and the disposition of patient medical records in the event the licensee dies, retires, or otherwise ceases to practice or provide medical care to patients, including the method by which patients may access or obtain medical records promptly if any of the described events occur.
- 2 CCR 502-1 Rule 21.170.1 and Rule 21.170.2: The confidentiality of the individual record, including all medical, mental health, substance use, psychological, and demographic information shall be protected at all times, in accordance with all applicable state and federal laws and regulations. Agencies shall prevent unauthorized access to paper and electronic records in accordance with HIPAA and 42 CFR Part 2. Individual records for adults must be retained for seven years from date of discharge from the agency if the agency is an outpatient agency, or 10 years from date of discharge if the agency is an inpatient agency. Individual records for those who are under 18 years of age must be retained until the individual is 25 years of age if an outpatient agency, or 28 years of age if an inpatient agency. Records must be disposed of in accordance with state and federal confidentiality statutes and regulations, including signing a qualified service organization agreement (QSOA) or business associate agreement if services are commissioned. Guidelines must also be established for reporting a breach or potential loss of individual identity in accordance with state and federal confidentiality statutes and regulations.
- CRS 6-1-713: Covered entities in the state of Colorado that maintain paper or electronic documents that contain PII shall develop a written policy for the destruction or proper disposal of documents containing PII. Unless otherwise required by state or federal law or regulation, the written policy must require that, when such paper or electronic documents are no longer needed, the covered entity shall destroy or arrange for the destruction of such paper and electronic documents within its custody or control that contain PII by shredding, erasing, or otherwise modifying the PII in the paper or electronic documents to make the PII unreadable or indecipherable through any means. See CRS 6-1-713(2) for the definition of covered entity and PII.
- CRS 6-1-713.5: A covered entity that maintains, owns, or licenses PII of an individual residing in the state shall implement and maintain reasonable security procedures and practices that are appropriate to the nature of the PII and the nature and size of the business and its operations. Note that if PII is disclosed to a third-party service provider, the covered entity must provide its own security protection for the information disclosed, or the third-party

  service provider must implement and maintain reasonable security procedures and practices as outlined in CRS 6-1-713.5(2).
  - CRS 6-1-716: In the event of a security breach, a covered entity must prompt an investigation to determine the likelihood that PII has been or will be misused. Notice must be given to affected Colorado residents unless the investigation determines that misuse of PII has not occurred and is not reasonably likely to occur. Notification must be made no later than 30 days after the date of determination that a security breach occurred. See CRS 6-1-716(2) for more details on notice requirements.
- **Pertinent Resources:** (See **Appendix B: Resources** for additional resources)
  - Behavioral Health Compliance Toolbox – Resources from Colorado's Office of Behavioral Health (OBH) on compliance with state and federal laws.

Appendix B: Resources

Applicability					**Topic Area**	**Resource**	**Description**
HIPAA	**42 CFR Part 2**	**Social Service Provider Organizations**	**Colorado Regulations**	**General/ Data Sharing and Standards**			
X					Regulations	Summary of the HIPAA Privacy Rule	**Overview** of key elements of the HIPAA Privacy Rule including who is covered, what information is protected, and how protected health information can be used and disclosed.
X				X	Regulations	Permitted Uses and Disclosures: Exchange for Treatment	**Fact sheet** for data sharing under HIPAA**.**
X					Regulations	Incidental Uses and Disclosures	**Overview** of incidental uses and disclosures under HIPAA.
X	X		X		Regulations	Information Related to Mental and Behavioral Health, including Opioid Overdose.	**Overview** and **other resources** on how HIPAA applies to mental health and substance use disorder information. See also: • FAQ 2088 • Additional FAQs on Sharing Health Information Related to Treatment for Mental Health or Substance Use Disorder – Including Opioid Abuse • HIPAA Privacy Rule and Sharing Information Related to Mental Health

	X				Regulations	Fact Sheet: SAMHSA 42 CFR Part 2 Revised Rule	**Overview** of several major sections of Part 2 that were revised in July 2020.
	X			X	Regulations, Data Sharing, HIE	Substance Abuse Confidentiality Regulations	**Frequently asked questions** and **Fact Sheets** regarding Part 2. See also: • Disclosure of Substance Use Disorder Patient Records: Does Part 2 Apply to Me? • Disclosure of Substance Use Disorder Patient Records: How Do I Exchange Part 2 Data? • Applying the Substance Abuse Confidentiality Regulations to Health Information Exchange
X					Regulations, Patient Access	FAQ 2046	**Frequently asked question** on when a covered entity may deny a patient's request for access to the individual's PHI.
X				X	Regulations, Security	Security Rule Guidance Material	**Educational materials** to learn more about the HIPAA Security Rule and other sources of standards for safeguarding electronic protected health information (e-PHI).
X				X	Regulations, Security	Submitting Notice of a Breach to the Secretary	**Guidance** on submitting a notice of a breach to the secretary.
			X		Regulations, Security	Overview of Colorado's Data Security Laws	**Frequently asked questions** for businesses and government agencies on Colorado's Consumer Data Protection Laws.

X					Consent	FAQs on Authorization; see specifically: FAQ 264, FAQ 271 and FAQ 481	**Frequently asked questions** on patient authorization provided by the U.S. Department of Health and Human Services.
X	X		X		Regulations, Consent	Behavioral Health Compliance Toolbox	**Resources** from Colorado's Office of Behavioral Health on compliance with state and federal laws. See also: • Checklist: HIPAA Elements of a Valid Authorization – Uses and Disclosures for which an Authorization is Required: Core Elements and Requirements • Checklist: 42 CFR Part 2 Elements of a Valid Consent: Elements and Requirements
X	X		X		Consent	Authorization and Consent Forms	**Examples** of HIPAA and Part 2 authorization, consent, and notice of privacy practice forms from the Colorado Department of Human Services, available in Spanish and English.
X					Consent	Model Notices of Privacy Practices	**Examples** of notices of privacy practices using plain language and approachable designs as required under HIPAA Privacy Rule developed by the U.S. Department of Health and Human Services.
X					Consent	The HIPAA Privacy Rule: Three Key Forms	**Examples** of notice of privacy practices, authorization, and patient consent from the American Academy of Family Physicians guidance.

X	X	X		X	Regulations	California State Health Information Guidance	**Guidance** and overview of data-sharing use cases in California. Includes resources such as authorization form requirements.
				X	Data Standards	Consolidated-Clinical Document Architecture (C-CDA) Overview	**Overview** on basic concepts of the HL7 C-CDA standard from HealthIT.Gov.
				X	Data Sharing, Data Standards	Health Information Exchange	**Overview** of health information exchanges from HealthIT.gov.
				X	Data Standards	2017 Interoperability Standards Advisory	**Overview** of recognized interoperability standards and implementation specifications for industry use.
				X	Data Standards	Fast Healthcare Interoperability Resources	**Overview** of the Fast Healthcare Interoperability Resources (FHIR) developed by HL7 International.

Appendix C: Health Information Exchange and Data Format Standards

Health Information Exchange

Health information exchange (HIE) is the electronic mobilization of health care information. HIE allows health care provider organizations and patients to appropriately access and securely share a patient's vital medical information, which improves the speed, quality, safety, and cost of patient care. HIE models may differ, and information can be exchanged in various ways.

There are three types of HIE architecture: federated (decentralized); repository (centralized); and a hybrid model.

- Federated (Decentralized) Model: Data stay at the source.
- Repository (Centralized) Model: Data from health care provider organizations are collected and stored in a central repository.
- Hybrid Model: Federated and repository architectures are combined.

Information can be exchanged through either of these forms:

- Directed Exchange: Health care provider organizations can electronically send and receive secure information through messaging.
- Query-Based Exchange: Health care provider organizations can find and/or request information on a patient, for example, through a web-based portal.
- Consumer Mediated Exchange: Patients can manage their health information, including transferring information between providers.

Colorado currently has two existing HIEs operated by Colorado Regional Health Information Organization (CORHIO) and Quality Health Network (QHN). Both are repository (centralized) models that enable directed exchange and query-based exchange of PHI.

Data Format Standards

Information that is exchanged through health information technology, such as HIE, is done so through a set of common standards that connect systems. Standards may pertain to security, data transport, data format or structure, or the meanings of codes or terms. Common standards are listed below.

Vocabulary/Terminology Standards

These standards address the ability to represent concepts in an unambiguous manner between a sender and receiver of information. Commonly used health care vocabulary standards include:

- Current Procedural Terminology (CPT) Codes – Numerical codes used primarily to identify medical services and procedures furnished by health care providers.
- Healthcare Common Procedure Coding System (HCPCS) – Collection of standardized codes that represent medical procedures, supplies, products, and services.
- International Classification of Diseases (ICD) 10 and ICD-11 – Classification system for diagnosis coding.
- Logical Observation Identifiers Names and Codes (LOINC) – Common set of identifiers, names, and codes for identifying health measurements, observations, and documents.
- Systematized Nomenclature of Medicine-Clinical Terms (SNOMED) – Standardized, international, multilingual core set of clinical health care terminology.

Content Standards

These standards relate to structure and organization of the electronic message or document's content, including the definition of common sets of data for specific message types. Some common examples of content standards are:

- Continuity of Care Documents (CCD) – A standardized medical summary for one or more patient encounters built on clinical document architecture. CCDs are patient-specific clinical summaries that are electronically generated and contain a variety of data elements such as patient demographics, history, medications, allergies, diagnoses, and more. CCDs can improve communication during transitions of care and can provide a standard for data elements.
- Clinical Document Architecture (CDA) – A base standard that provides common architecture, coding, semantic framework, and markup language for the creation of electronic clinical documents.
- Consolidated-CDA (C-CDA) – A standard that allows documents to be formatted to contain structured and unstructured patient data and can be used to support HIE with other EHR systems.
- Health Level 7 (HL7) – A quasi-standard format for point-to-point messages sent between health care providers or departments.

Transport Standards

Transport standards address the format of messages exchanged between computer systems, document architecture, clinical templates, user interface, and patient data linkage. Common transport standards are:

- Digital Imaging and Communications in Medicine (DICOM) – A standard for the communication and management of medical imaging information and related data.
- Direct Standard™ – A set of standards and protocols to allow participants to send authenticated, encrypted health information directly to known, trusted recipients over the internet.
- The Fast Healthcare Interoperability Resource (FHIR) – A standard using internet technologies that allows HL7 messages and CCDs to be shared between systems regardless of how they are stored in those systems.