CalHHS
California Health & Human Services Agency

Toolkit: **Navigating HIPAA and FERPA** for Integrated School Behavioral Health Services

JULY 2025

Table of Contents

Table of Contents

Introduction

Across California, initiatives like the statewide Children and Youth Behavioral Health Initiative (CYBHI)[1], the CYBHI **Fee Schedule Program**[2], and the California **Community Schools Partnership Program (CCSPP)**[3] are strengthening relationships between county and local education agencies (LEAs) (such as schools and districts), behavioral health agencies and providers, managed care organizations, and other community partners. These collaborations aim to improve behavioral health services available at and through schools, ensuring that children, youth, and their families can better access the support they need. Effective school-behavioral health partnerships create opportunities for prevention, early intervention, timely referrals, and comprehensive service delivery. This coordinated approach helps ease burdens on children, youth, and families while improving care across systems.

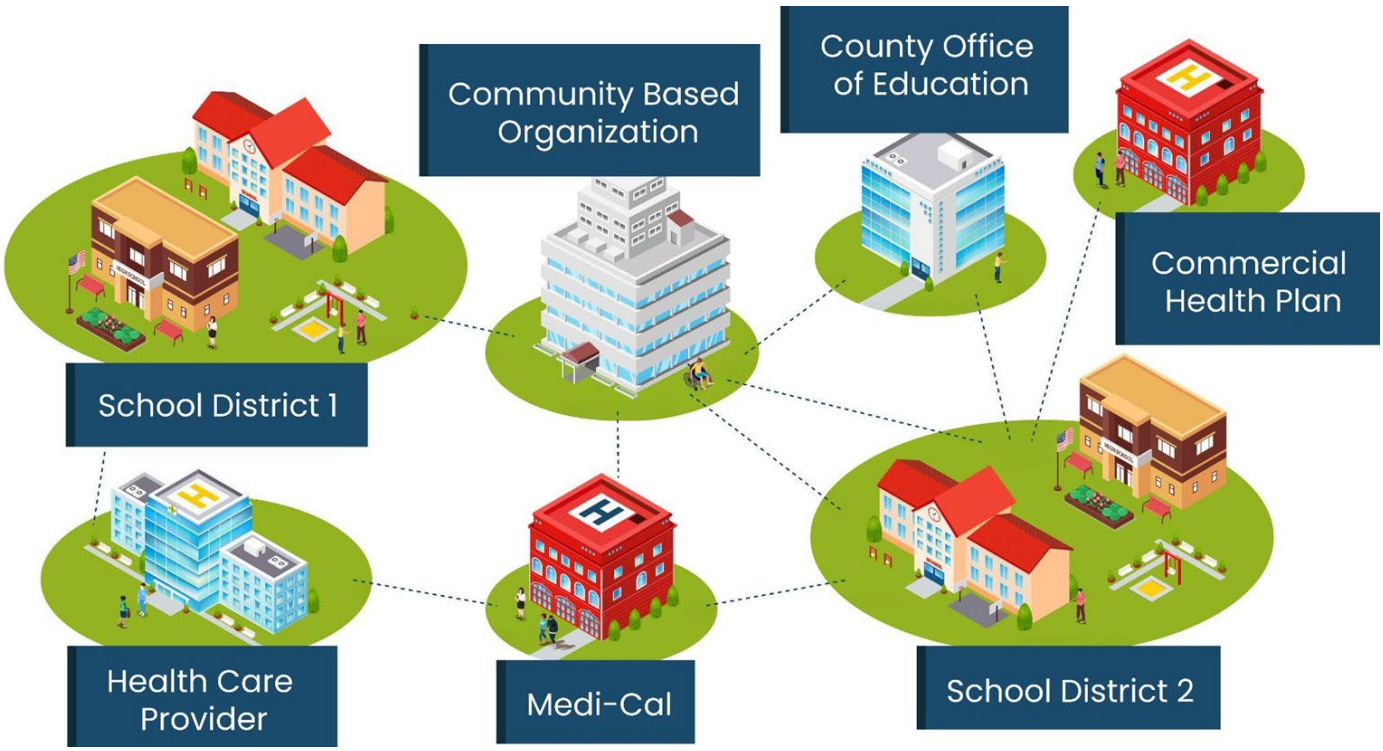
For these partnerships to succeed, it is necessary for education agencies and their partners to establish clear policies and protocols that consider the importance of information-sharing to facilitate and coordinate care, and the importance of privacy to maintain confidentiality and build trust between children, youth, families, and the professionals who support them, including school staff and health care providers. Data privacy laws, such as the Family Educational Rights and Privacy Act (FERPA) and the Health Insurance Portability and Accountability Act (HIPAA) - and specifically the HIPAA Privacy Rule – set boundaries regarding how, when, and with whom information may be shared. However, navigating these laws can be challenging when multiple systems are involved in delivering care.

This Toolkit explains how FERPA and the HIPAA Privacy Rule (the latter generally referred to throughout as "HIPAA") might apply in different school-behavioral health "network designs" in California, using hypothetical case examples to show how these laws can apply depending on the network design and how that can then shape policy and practice. FERPA and HIPAA are not the only laws that must be considered when

building information-sharing policies and practices, but they are a helpful place to start. Ultimately, knowing how FERPA and the HIPAA work ensures that education and behavioral health partners can design services and processes within legal guidelines that also meet the needs of children, youth, and families.

This Toolkit uses the term **"network design"** to describe how services are provided and funded within a school-behavioral health partnership. For example, a school district might contract with an outside health care provider to deliver services, with the district billing insurance when needed.

In some cases, several network designs may work together within a larger **"ecosystem"** to offer a full range of services and supports for children and youth. In this Toolkit, "ecosystem" refers to the various agencies, partners, funding sources, and administrative structures involved in the broader school-behavioral health partnership.



Who the Toolkit Is For

Understanding both FERPA and HIPAA is essential for education, behavioral health, and community partners working together to provide behavioral health services at or arranged by schools. This Toolkit is designed to help build that understanding, whether you're just starting a school-behavioral health program or have been running one for years. It can be used both by administrators who manage these programs, as well as frontline providers.

- If you **already have established network designs**, the Toolkit can offer insights on FERPA and HIPAA to help you check or improve information-sharing and confidentiality practices.
- For those looking to **expand services or explore new reimbursement opportunities**, the Toolkit provides examples of how FERPA and HIPAA apply to different service and payment models.
- If you're in the **early stages of building a behavioral health program**, the Toolkit can guide you in setting up strong information-sharing and confidentiality practices from the start and shape your approach to building any program(s). For example, how FERPA and HIPAA apply may inform whether you decide to provide services on campus funded fully by LEAs, or off-campus with behavioral health agencies billing insurance as needed.

Potential partners who might use the Toolkit include, but are not limited to:

- **Education agency representatives:** This might include superintendents, principals, county administrators, and/or school-based health team members such as nurses, counselors, health center coordinators.
- **School-based staff:** This might include administrative staff, program coordinators, resource specialists, teachers, and classroom aids or paraprofessionals.
- **Behavioral health representatives:** Depending on your partnerships, these might include county health and/or behavioral health teams, community-based organizations (CBOs) (e.g., Federally Qualified Health Centers (FQHCs), local behavioral health agencies/clinicians, hospital, or university-affiliated programs), or representatives from health plans or managed care plans.
- **Legal counsel:** This might include attorneys from multiple partner organizations.
- **Community partners:** These might include parent or family support groups to provide a broader perspective on the needs of the community.

The Toolkit is also flexible enough for individual agencies to use. However, we encourage integrated teams (e.g., Coordination of Services Teams (COST) or other cross-agency teams) to collaborate and discuss shared goals for confidentiality and information-sharing.

By working through the Toolkit together, you and your partners will be well-positioned to advance a shared vision that balances confidentiality and information-sharing to benefit children, youth, families and the systems that support them.

This document is meant to provide guidance only.
Always include legal counsel in discussions related to the law.
Legal decisions should not be made without their guidance.

How the Toolkit Can Help You

This Toolkit will help you

- Refresh your existing knowledge of FERPA and HIPAA;
- Learn how FERPA and HIPAA may apply to different network designs in your ecosystem;
- Reflect on the network designs you already have in place or plan to develop with partners, considering how FERPA and HIPAA apply to them;
- Understand key administrative and operational considerations that come with FERPA and HIPAA Privacy Rule compliance; and
- Explore practical tips for implementation, such as managing contracts, handling releases of information, and notifying families.

By the end of the Toolkit, you'll be able to answer common questions such as:

- May school staff refer students to behavioral health providers and share protected information without a release of information (ROI)?
- Do we need an ROI to bill health insurance for services?
- What content should our ROI forms include?
- What information must be shared with families, and what can be shared?

Whether you're working in an established school-behavioral health ecosystem or just starting to build one, we strongly recommend that you read through the entirety of the Toolkit fully before you start to work through the details. For more information about the guiding principles of this toolkit, please reference Appendix A.

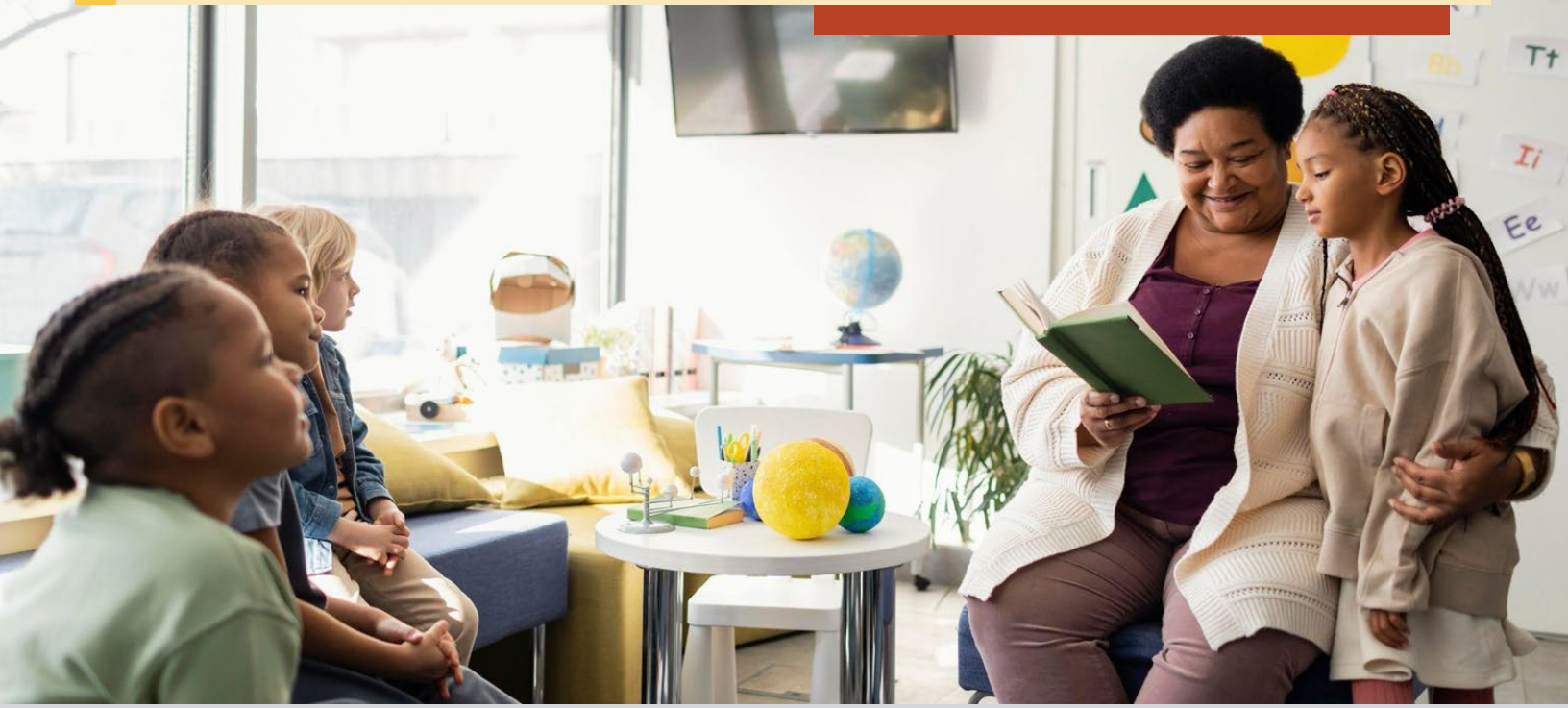
Limitations of the Toolkit

There are important limitations to this Toolkit:

- **The Toolkit does not address all confidentiality laws that must be considered.** This Toolkit focuses on FERPA and HIPAA, but other confidentiality laws may also apply and should be reviewed. Some of these key laws are mentioned throughout the Toolkit, though not all. For more details on the scope of the Toolkit and other important laws to consider, refer to Appendix B.
- **The Toolkit does not address confidentiality laws that apply to electronic record storage and transfer.** These laws may impose specific requirements for data storage systems, and it is critical to understand these requirements when building out systems for service delivery and insurance billing. For more details on the scope of the Toolkit and electronic data storage, refer to Appendix C.
- **The Toolkit is California-specific.** While this Toolkit focuses on two federal laws, it was written with California-specific laws and context in mind. Readers in other states should not assume that the Toolkit is relevant to their state.
- **The Toolkit has a behavioral health focus.** Because the Toolkit is developed to support implementation of CYBHI, it focuses on behavioral health services, not broader medical or physical health care. While some sections may also apply to physical health services, because both FERPA and HIPAA also govern those areas, readers should consult legal counsel and not make any assumptions regarding the applicability of the Toolkit's analyses.
- **The Toolkit was written for readers who are already somewhat aware of FERPA and HIPAA.** This Toolkit assumes readers already have a basic understanding of the common confidentiality issues that come up in school-behavioral health partnerships. Readers who are not familiar with FERPA and HIPAA, or who want a more detailed refresher, should review Appendix B, and the cited references throughout this document .

- **The Toolkit is a starting point, not a step-by-step guide.** This Toolkit should not be used in isolation for building or overhauling your network design(s) or overall ecosystem. Rather, it will help readers think about and understand how FERPA and HIPAA may apply differently in different network designs and how different design decisions can impact policy and practice.
- **Federal and state laws can change, so it is important to understand that the information in this Toolkit is up to date as of July 2025.** Readers should always consult their legal counsel to ensure the information is still relevant and stay informed of any updates after this date. Legal citations should not be construed, independently or together with anything in this document, as offering legal advice. Many of the citations are also exemplary, and you should consult with legal counsel to discuss the specific facts and law that apply to your situation.

This Toolkit offers information, not legal advice. Be sure to consult with experienced attorneys when making decisions or implementing any of the guidance provided.



Toolkit Sections

1. **FERPA & HIPAA Overview:** This section ensures that all partners have a shared understanding of FERPA, HIPAA, and key terms.
2. **Case Studies:** This section shows how FERPA and HIPAA apply in four different hypothetical network designs and illustrates the resulting implications on implementation using real-life case examples and process map visuals.
3. **Confidentiality and Information-Sharing Tools:** This section covers a few key tools—such as the ROI forms and agreements—often needed to manage confidentiality and information sharing.

FERPA & HIPAA Overview[4]

There are many federal and state confidentiality laws that control the release of health information, but two of the most important ones are FERPA and HIPAA, and particularly the HIPAA Privacy Rule. This section offers a short refresher on these two laws; if you are not familiar with FERPA or HIPAA, or want more detailed information, you should review additional resources[5] before using this Toolkit.

What is FERPA?

FERPA protects the privacy of students' education records held by "educational agencies or institutions" that receive federal funds under programs administered by the U.S. Department of Education (ED) and either provide direct instruction or educational services to students. These include schools and educational agencies that direct or control schools, such as school districts, county offices of education, and state education departments.[6]

FERPA controls the disclosure of individually identifiable student information maintained in the "education record." An **"education record"** is defined as records, files, documents, and other materials that contain information directly related to a student and are maintained by an educational agency or institution, or by a person acting for such agency or institution[7]. In California, the term "pupil record" is often used as well. **This Toolkit uses "pupil records" and "education records"[8] interchangeably.**

Education records may include health information, such as school nurse records. **However, FERPA does not apply to all information at a school:** there are several types of records that are exempt from FERPA, such as records "kept in the sole possession of the maker, …used only as a personal memory aid, and …not accessible or revealed to any other person except a temporary substitute for the maker of the record." For more examples of records[9] exempt from FERPA, see **HIPAA or FERPA? A Primer on Sharing School Health Information in California, 2nd Edition.**

Generally, FERPA prohibits educational agencies from disclosing any individually identifiable information in the education record unless they have written permission for the disclosure, or an exception allows disclosure without a written ROI[10]. There are several such exceptions. For example, FERPA allows educational agencies to disclose records "to other school officials, including teachers, within the agency or institution whom the agency or institution has determined to have legitimate educational interests" without need of a release [11].

It is important to note that there is no exception in FERPA that specifically allows disclosure to insurers[12] for insurance billing purposes, so a written release is typically required for insurance billing.

What Is HIPAA?

HIPAA is a federal law that protects the privacy of individually identifiable health information held by **"covered entities."**[13,14], HIPAA defines "covered entity" as health plans, health care clearinghouses, and health care providers who transmit health information in electronic form for certain transactions.[15]

HIPAA has several regulations, or "Rules," including the Privacy Rule, *Security* Rule, and the Enforcement Rule. The HIPAA Privacy Rule sets national standards for the confidentiality of protected health information (PHI) held by covered entities. The HIPAA *Security* Rule imposes rules for the confidentiality, integrity, security, storage and exchange of electronic protected health information (ePHI) held by covered entities, including Electronic Health Records (EHRs).[16]

The HIPAA Privacy Rule and *Security* Rule do not apply in exactly the same way or in the same situations. For example**, a covered entity can be subject to the HIPAA *Security* Rule even if some or all of its records are not subject to the HIPAA *Privacy* Rule.** This can happen when schools deliver health care and bill insurance for those services in certain network designs and thus has implications for the health information systems used by school-based health programs.

This Toolkit focuses exclusively on the HIPAA Privacy Rule. For the purposes of the toolkit, it will use "HIPAA" to refer to the HIPAA Privacy Rule.

In general, HIPAA says that health care providers and other covered entities cannot disclose individually identifiable health information without a signed authorization.[17] However, there are some exceptions that allow providers to share information without authorization in specific circumstances.[18] For example, HIPAA allows disclosure for treatment purposes (broadly defined to include care coordination), payment, and health care operations (certain administrative, legal, financial, and quality improvement activities, including care coordination and case management) without requiring a written release.[19]

For more information about the HIPAA Security Rule[20], and the administrative, physical, and technical safeguards and standards it sets for the protection and exchange of individuals' electronic personal health information created, received, used, or maintained by a covered entity, please refer to The Security Rule of the Health Insurance Portability and Accountability Act in Appendix B[21]

Key Points on FERPA and the HIPAA Privacy Rule

FERPA and the HIPAA Privacy Rule will never apply to the same record at the same time.

HIPAA explicitly states that its rules do not apply to individually identifiable health information held in an education record subject to FERPA.[22] This means that if FERPA applies to a particular record, the HIPAA Privacy Rule does not apply—even if the school or school health care provider otherwise qualifies as a covered entity under HIPAA. However, and as noted in Appendix C, the HIPAA Security Rule could still require a school to implement security measures when sharing a student's data under certain situations. **The HIPAA Privacy Rule applies to PHI created when a covered entity delivers services on a school campus – as long as FERPA does not apply.**

Application of FERPA to education records containing health information where the health care provider can be considered a "school official."

FERPA applies to the education records of public school students under 18 years of age that contain student health information and that are maintained by the school in the school's health clinic or nurse's office. Such records are subject to FERPA if the person or agency that created the record is an educational institution, the employee of an educational institution, or the agent or contractor of an educational institution and can be considered a "**school official.**" The term "school official" includes school staff, such as teachers, counselors, and school nurses.

It also can include a "board member, trustee, registrar, …attorney, accountant, human resources professional…, and support or clerical personnel."[23] Individuals and agencies, including health agencies that contract with an educational agency, can also be considered school officials in some cases, as discussed below.

Some contractors can be considered "school officials" for purposes of disclosing a student's PHI without consent under FERPA. ED guidance and FERPA regulations provide factors that help determine whether a provider of health care can or should be considered a school official. These factors include types of services offered, administrative and operational control of service delivery, and financing of the service delivery.[24] For more information, see HIPAA or FERPA? A Primer on Sharing School Health Information in California, 2nd Edition. Further, FERPA limits the scope of the PHI disclosed to only that information which matches the recipient's "legitimate educational interest" in the information.[25]

A **written release is often necessary to submit a reimbursement claim that contains FERPA-protected record information to an insurer**, unless the insurer is acting as a "school official" with "legitimate educational interest" in the information as defined by school policy and has a contract with the LEA that subjects the insurer to the confidentiality and disclosure requirements of FERPA.

Some health care providers/agencies contract with a "covered entity" and are "business associates" for purposes of HIPAA.

A **"business associate"** is an individual or organization that receives, creates, maintains, or transmits "protected health information" as part of work done on behalf of a "covered entity." This work must be directly related to HIPAA-regulated activities by the covered entity, such as claims processing or billing, or services that support that work.[26] A covered entity may share PHI with a business associate without an individual's authorization as long as the covered entity has a written agreement from the business associate in which the business associate commits to protect "protected health information" in compliance with HIPAA.[27] HIPAA specifies what this written agreement must include.[28] Further, the existence of a contract with a covered entity, on its own, does not make a contractor a "business associate." Health care providers should always consult legal counsel to determine whether a partnership may qualify as a business associate relationship.

Some health care providers are not "covered entities" for purposes of HIPAA.

HIPAA defines **"covered entities"** as health plans, health care clearinghouses, and health care providers who transmit health information electronically for certain types of transactions.[29] When done electronically, the transactions that will make HIPAA applicable include but are not limited to submitting claims to health insurers, making benefit and coverage inquiries to insurers, making inquiries about submitted claims, and sending health care authorization requests.

HHS provides additional guidance on what is considered a **"transaction."** [30]

In its 2019 Joint Guidance, ED and HHS suggest that traditional school-employed health care providers will not be considered covered entities because of the electronic transaction requirement and the fact that they do not traditionally bill insurance for services rendered. [31]

While FERPA and the HIPAA Privacy Rule will never apply at the same time, health information can be subject to both laws at various points.

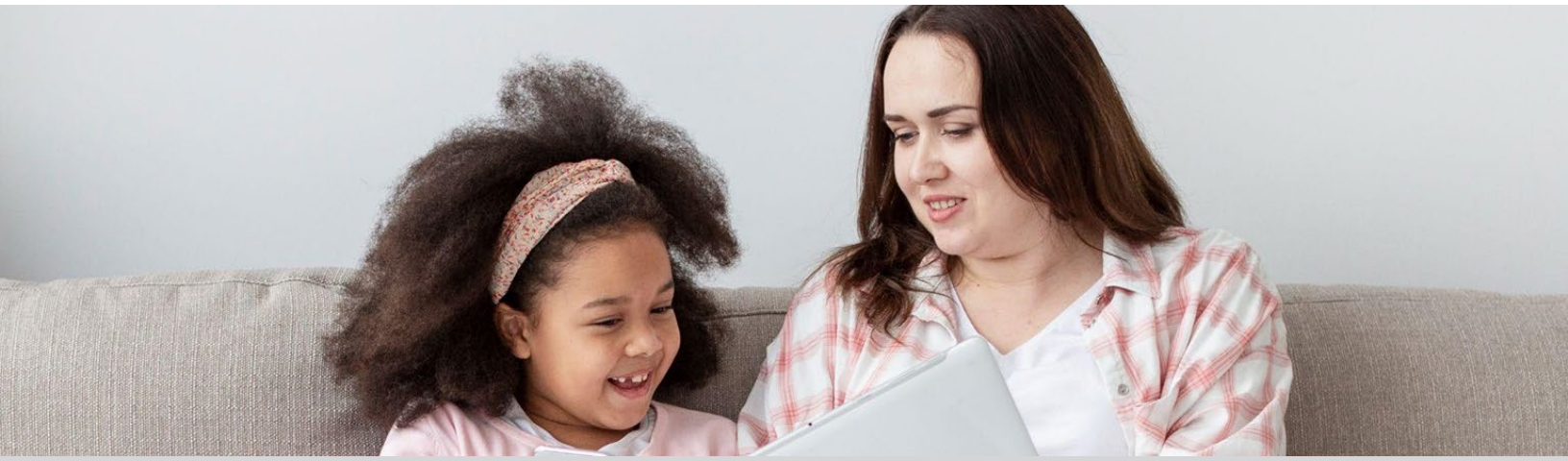
For example, a school-employed nurse may create health records that become part of an education record subject to FERPA. In order to bill insurance for the care delivered, the school must use some FERPA-protected information from the student's record to create the claim. Under FERPA, the school must get an ROI from the student's parent or the student (if the student is at least 18 years old or enrolled in a postsecondary school) to be able to submit the claim to the student's health insurer. Once the information is released to the insurer pursuant to a signed release, it is generally not subject to FERPA protections.[32] The insurer is a HIPAA-covered entity, so individually identifiable information that it holds, such as the claims information received from a provider, is protected by the HIPAA Privacy Rule. **Thus, the same information would go from being protected by FERPA while in the school's records to being protected by the HIPAA Privacy Rule once in the insurer's system.**

Note that this Toolkit and case examples focus exclusively on confidentiality (the HIPAA *Privacy Rule*) and not on security obligations for electronic data storage and transfer (the HIPAA *Security Rule*). While FERPA and the HIPAA Privacy Rule will never apply at the same time, FERPA and the HIPAA Security Rule can. See Appendix C for more information.

This document is meant to provide guidance only. Always include legal counsel in discussions related to the law. Legal decisions should not be made without their guidance.

Other federal and state confidentiality laws may apply alongside FERPA and HIPAA.

Other federal and state confidentiality laws may apply in addition to HIPAA and FERPA. For example, California's **CMIA** protects individually identifiable health information created by most health care providers and health care service plans, while California's Insurance Information and Privacy Protection Act (**IIPPA**) protects individually identifiable health information created by health insurers,[33] and federal regulations, known as **42 C.F.R. Part 2**,[34] protect the confidentiality and control the disclosure of some substance use service information. These laws may apply in addition to FERPA or HIPAA. The "Limitations of this Guidance" section in the Introduction highlights a few other important laws that may be applicable.

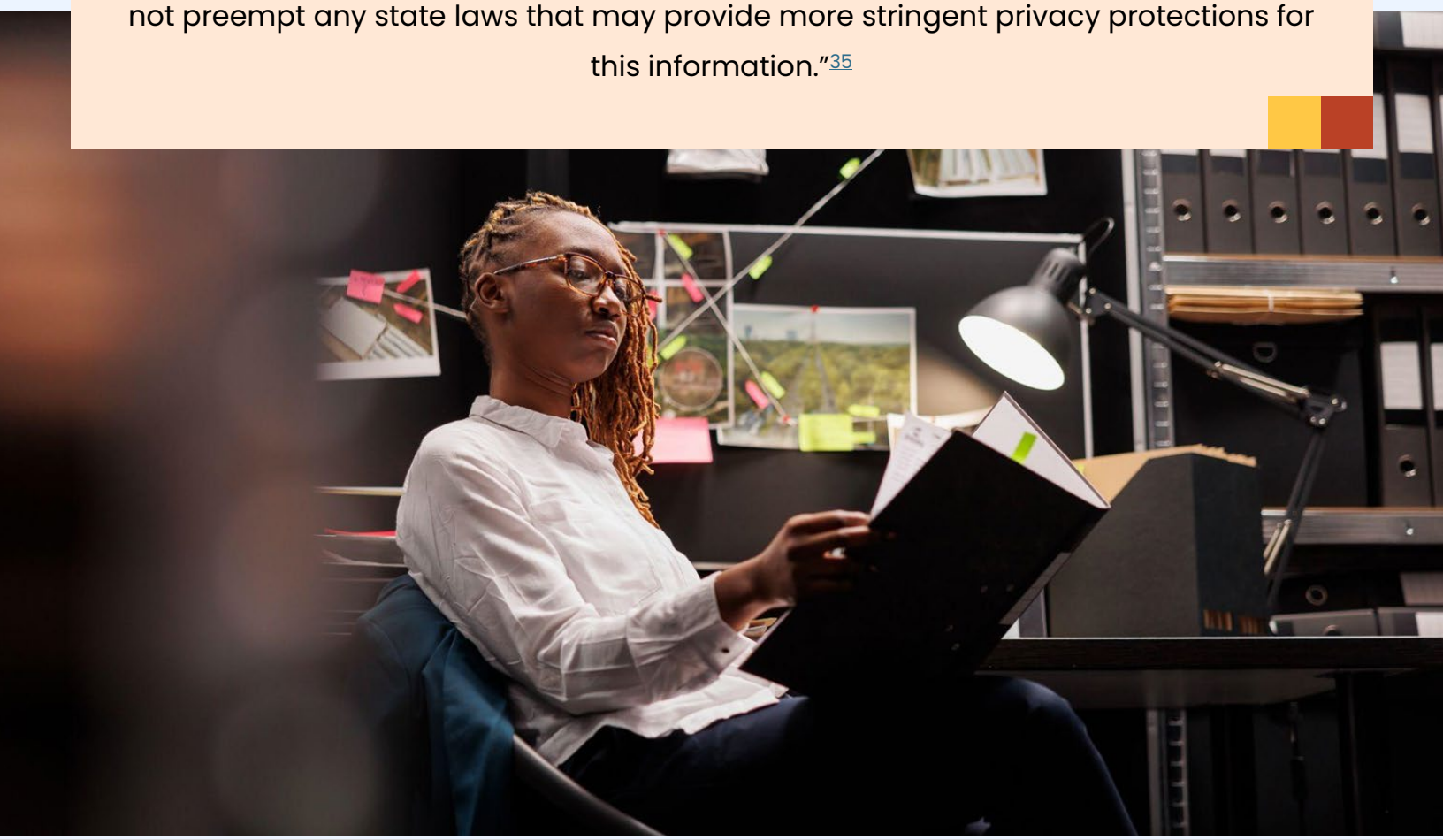


What happens if state law or guidance applies in addition to FERPA or HIPAA?

- ***When state law and FERPA apply:*** Educational agencies must comply with both FERPA and state law when possible. ED has said that many FERPA exceptions that allow information sharing without a written ROI are optional, meaning that educational institutions can choose to apply them or not.

  For example, the "school official" exception to FERPA allows, but does not require, educational agencies to share information with school officials in the same network who have a **"legitimate educational interest"** in the information, without a written release. ED guidance urges educational agencies to consider state law in applying permissive exceptions like the "school official" exception:

> [M]any states have privacy laws that protect the confidentiality of medical and counseling records. FERPA's permissive exceptions to the requirement of consent do not preempt any state laws that may provide more stringent privacy protections for this information."[35]



If there is a conflict between FERPA and state law, FERPA usually takes precedence. However, if an educational agency believes there is an actual conflict between obligations under state law and its ability to comply with FERPA, the educational agency must notify ED's Family Policy Compliance Office.[36] Such situations should be brought to your legal counsel.

- ***When State Law and HIPAA apply:*** When state law offers stronger confidentiality protections than HIPAA, providers must usually follow state law. [37]
- ***The CalAIM program:*** The California Department of Health Care Services (DHCS) has published guidance on **CalAIM data-sharing** that summarizes many federal and state health confidentiality laws and addresses Assembly Bill 133, which limits the application of certain state privacy laws so that information can be shared more easily to coordinate care within CalAIM.[38]
- ***Other Regulations and Professional Guidance:*** Licensed health professionals might also need to follow ethical codes and licensing requirements, which sometimes impose stricter confidentiality standards than HIPAA, FERPA, or state law. Providers should consult legal counsel if they have questions or concerns about conflicts. Additionally, there are other laws governing how schools and health care providers share student and health information electronically that must also be considered.

The U.S. ED has offered legal and best practice guidance on when to seek consent for the release of health information in an education record subject to FERPA protection.

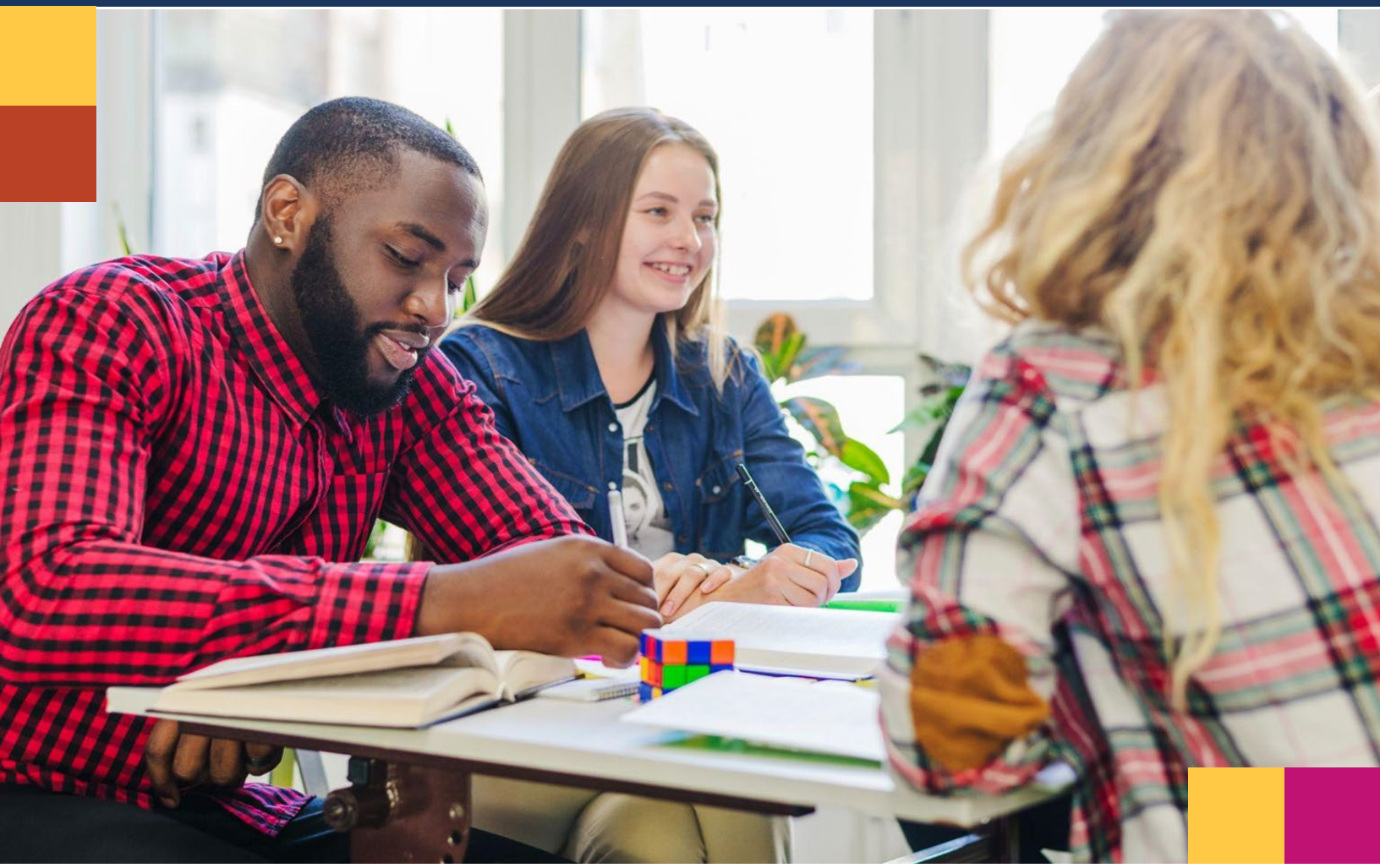
Legal guidance: In both 2008 and 2015, ED issued guidance, in conjunction with the U.S. Department of Health and Human Services (HHS), addressing how FERPA and HIPAA apply.[39]

Best Practice Guidance: In 2016, ED issued "significant guidance" to school officials in institutions of higher learning on best practices related to disclosure of medical information in education records, specifically where FERPA may allow disclosure without needing an ROI. Although this guidance was aimed at officials in institutions of higher learning, it may be of interest to school officials in other education agencies that offer health services. The guidance says:

> When institutions choose to disclose PII [personally identifiable information] from education records, including medical records, without consent, they should always take care to consider the impact of such sharing, and only should disclose the minimum amount of PII necessary for the intended purpose."[40]

In instances when schools or providers need to obtain consent to release information subject to HIPAA or FERPA protections, they must use compliant ROI forms.

The specific ROI forms you need and their contents will depend on whether FERPA, HIPAA, or other laws apply. Legal counsel should always be involved when developing these tools. DHCS has developed the Authorization to Share Confidential Member Information (ASCMI) Form, which health care organizations, schools, CBOs, counties and other entities can utilize to obtain consent to release information protected under HIPAA, FERPA, 42 C.F.R. Part 2, and other data sharing privacy laws.



FERPA and HIPAA Privacy Rule Comparison Chart

In many ways, FERPA and HIPAA are similar. However, there are some important differences that directly impact how, when, and with whom information may be shared, as well as administrative policies and practices that partners must implement. The following chart provides a basic overview of key differences between FERPA and HIPAA, describes a few of the ways that they might dictate implementation, and directs you to further resources. This chart is ***not*** a full summary of those laws, and there may be other federal and state laws that apply to your situation which are beyond the scope of this document. Do not rely on this chart alone to make decisions and consult with counsel as needed. See **A Primer on Sharing School Health Information in California** for citations and more guidance on answering the questions in the chart. [41]

Common Questions	FERPA	HIPAA Privacy Rule
Does the law usually require a signed release to disclose protected information?	Yes[42]	Yes[43]
Who signs the release/authorization?	"Parent" must sign for a minor student. If student is 18 or older or is attending a postsecondary institution, student signs. FERPA defines "parent" to include a parent, guardian, or person acting in the role of parent. See also local educational agency (LEA) policy for definitions.	"Personal representative" signs in most cases. For more detail, see 45 C.F.R. § 164.502(g)(3) and applicable California law, such as Civ. Code § 56.11.
What information is required to be included in the release?	Must specify the records that may be disclosed, the purpose of the disclosure, and the party or class of parties to whom the disclosure may be made. See 34 C.F.R. § 99.30 for more details.	Must specify the information being disclosed, the purpose of the disclosure, the recipients of the disclosure, and an expiration date. For more detail, see 45 C.F.R. § 164.508. In California, releases also may need to comply with applicable California law, such as Civ. Code § 56.11.
Does the law allow disclosures without needing a signed release?	Yes, in limited circumstances.[44]	Yes, in limited circumstances. (See e.g. 45 C.F.R. § 164.502 .)

Common Questions	FERPA	HIPAA Privacy Rule
Does the law allow disclosures of health information to *teachers and other school staff* for referral or care coordination, without a signed release?	Yes, if the school staff person is in the same educational agency and has a "legitimate educational interest" in the information as defined in school policy. See also "best practice guidance" from the U.S. ED cited in the section above.) The information disclosed must be limited to the information that meets that legitimate educational interest.	Yes, if school staff are *health care providers* and the release is for treatment, referral, and care coordination purposes. [45, 46]
Does the law allow disclosures of health information to other health providers for referral or care coordination, without a signed release?	Yes, if the provider is a "school official" in the same educational agency and has a "legitimate educational interest" in the information, as defined by school policy. The information disclosed must be limited to the information that meets that legitimate educational interest. If the provider is not a "school official," a signed release is needed to disclose the health information to that provider. [47]	Yes, with other health care providers for treatment, referral, and care coordination purposes.
Does the law allow disclosures in emergencies in order to prevent danger or harm?	Yes, as outlined in 34 C.F.R. § 99.36.[48]	Yes

Common Questions	FERPA	HIPAA Privacy Rule
Does the law allow disclosures in order to submit a reimbursement claim that includes information from the protected record to an insurer without a written release?	No, unless the insurer is acting as a "school official" with "legitimate educational interest" in the information as defined by school policy and has a contract with the LEA that subjects the insurer to the confidentiality and disclosure requirements of FERPA.	A written release is not required but may be recommended by legal counsel.
Are there administrative requirements?	Yes, including but not limited to: • Annual notices of rights to families • Required local policies • Document retention requirements • Documenting access to records • Required forms • Document security requirements (See e.g. 34 C.F.R. §§ 99.7, 99.30, 99.32)	Yes, including but not limited to: • Notice of Privacy Practice to patients • Document retention requirements • Documenting access to records • Required forms • Document security requirements (See e.g. 45 C.F.R. § 164.508, Civ. Code § 56.11, Civ. Code § 791.29) [49]

This chart was adapted with permission from Gudeman, HIPAA, or FERPA? A Primer on Information Sharing, 2nd Edition, National Center for Youth Law, 2018. See Primer for citations and for more information and guidance on answering the questions in the chart. It was adapted and updated by Gudeman and Estes, co-authors of this Toolkit, in July 2024.

Application of HIPAA & FERPA: Case Examples

This section of the Toolkit presents case examples that show how FERPA and HIPAA can apply in four different school-behavioral health network designs. After reading this section, you should have a clearer understanding of how network design structures can impact when and how FERPA or HIPAA apply to the documents and information that are created and managed.

Understand "Network Design"

As a reminder, this Toolkit uses the term **"network design"** to refer to how services are provided and funded in a school-behavioral health partnership, including: who provides the services, who funds the services, what services are offered, and who has operational and administrative control over service delivery. These factors help determine when FERPA, HIPAA, and other confidentiality and disclosure laws apply.

In this way, your network design(s) shapes the confidentiality, information sharing, and administrative policies and practices that you and your partners follow. This includes record-keeping rules, as well as who must sign consent forms, ROI forms, and billing paperwork. In large, complex school-behavioral health ecosystems, several network designs might be working at once. This may mean that there are different rules for confidentiality and information sharing in the same ecosystem.

Network designs can fall along a continuum (as depicted in the visual below labeled **Figure 1: Network Design Continuum)**, ranging from health services fully provided and funded by an educational agency (e.g., school or county office of education) to health services fully provided by an independent health care provider (e.g., Federally Qualified Health Center or county health agency) and billed through insurance or paid for through other funding.

Network Designs and Case Examples

The following section describes **four hypothetical programs** with different network designs across this continuum and offers **case examples of students receiving services in each**. The examples are offered to illustrate how FERPA and HIPAA can apply differently depending on network design and how this in turn can impact confidentiality and information sharing.

Hypothetical Network Designs in Case Examples

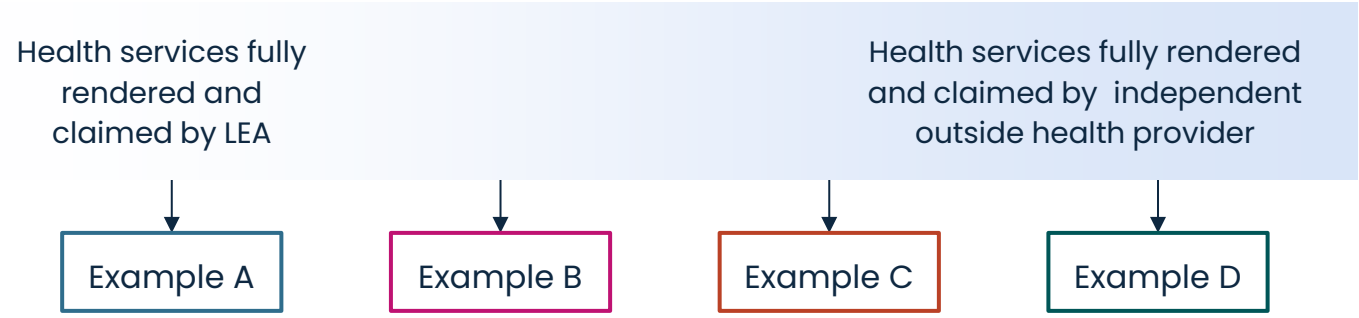


Figure 1: Network Design Continuum

Note: The following hypothetical network designs are intentionally simplified to illustrate application of the law. They are not intended to reflect existing networks or programs and do not address application of any laws other than FERPA and HIPAA. Real-world scenarios are more complicated than can be presented in this Toolkit. Toolkit users should work with their legal counsel to map their own network design(s), and apply FERPA, HIPAA, and other laws to their local context.

A

Network Design A: Staff employed by a County Office of Education (COE) deliver services to students on school campuses, fully funded by the COE. The COE bills eligible services to insurance where possible.

B

Network Design B: Staff employed by a school district deliver services to students on campus, fully funded by the district. The district bills eligible services to insurance where possible.

C

Network Design C: Staff from an independent health care provider deliver services to students on campus, on behalf of a school district (contracted). The district funds the services and bills eligible services to insurance where possible.

D

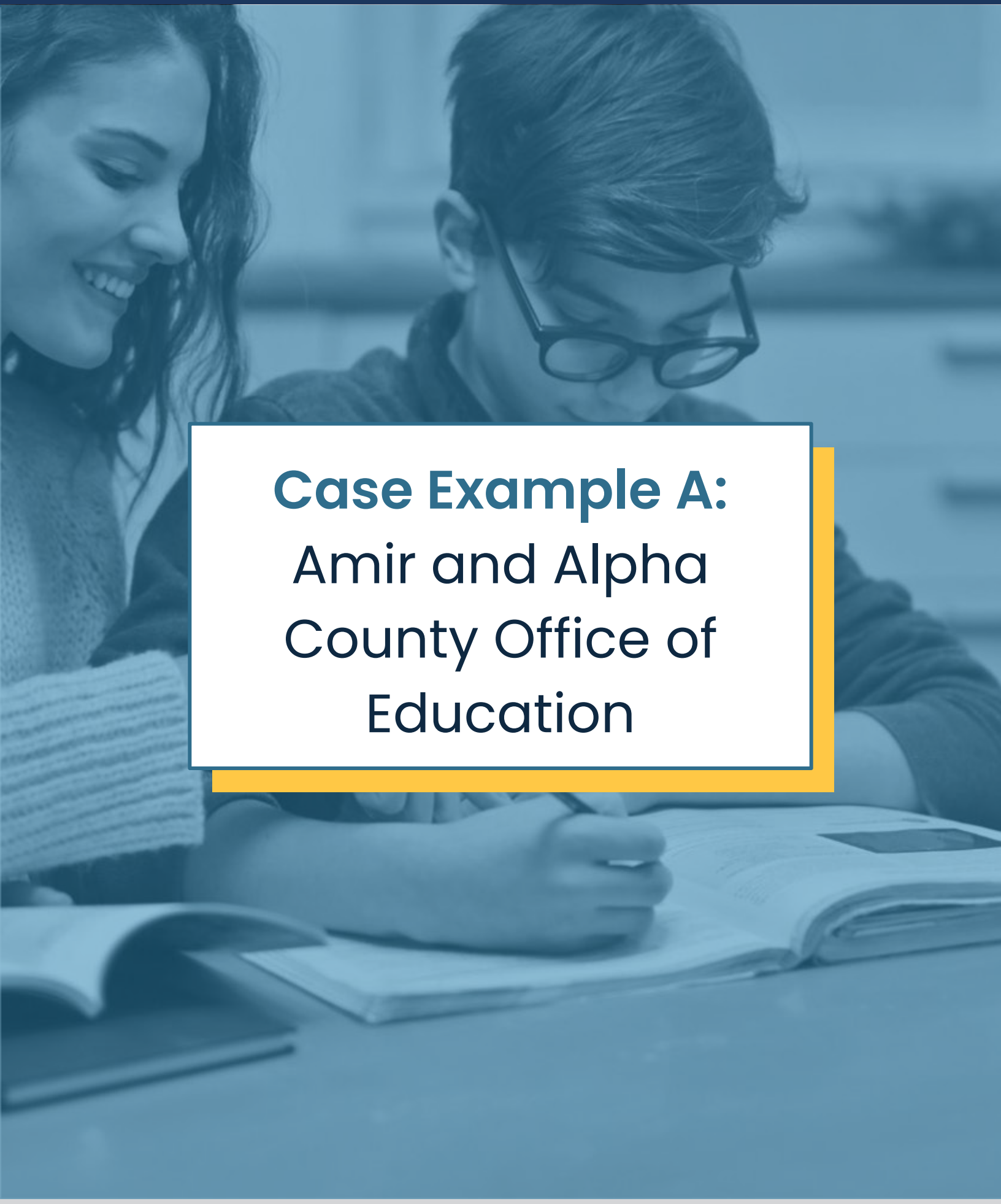
Network Design D: Staff employed by a Medi-Cal provider contracted with the county Specialty Mental Health Services (SMHS) Program deliver services to students off campus. The provider funds and bills insurance where possible.

How To Read The Case Examples

Each case example begins with a brief overview introducing the student, involved providers, and the key aspects of the hypothetical network design. The case presents a chronological sequence of actions by school staff, providers, parents/guardians, and students in delivering and granting permission to bill for behavioral health services.

Each step includes an analysis of

1. Whether HIPAA or FERPA may apply;
2. Whether a consent to share data is needed for that particular aspect of data sharing or collection.



Case Example A: Amir and Alpha County Office of Education

Context and Network Design

Who

At Apple Elementary, 10-year-old Amir has been referred by the school nurse to a licensed therapist employed by the Alpha COE for on-campus psychotherapy.

Staff

Alpha COE directly employs a licensed therapist and psychologist who deliver services to Alpha COE school district students on school campuses.

Services

Services include psychotherapy and Multi-Tiered Systems of Support (MTSS)[50] Tier 1-level prevention services such as psychosocial health education and mental health first aid.

Reimbursement

If services rendered are eligible for reimbursement, Alpha COE's LEA Billing Coordinator will submit the necessary information from students' educational records to their Third Party Biller (TPB) to complete claims paperwork.

Contracts/MOUs:

- Legal counsel for Alpha COE and its schools, including Apple Elementary, develop contracts between Alpha COE and the schools. These outline the responsibilities of Alpha COE staff when they enter school campuses and provide services. They also address issues such as reimbursement and confidentiality.
- Alpha COE and their TPB Vendor complete their own contract as well as the **"tri-party" Data Use Agreement (DUA)**[51] provided by California DHCS, which outlines confidentiality and data sharing requirements. The DUA with DHCS establishes a HIPAA business associate relationship for purposes of data use and information exchange.

FERPA or HIPAA?

In this network design case example, data exchange is **primarily governed by FERPA protections.**

The providers are Alpha COE employees with no additional affiliations. Alpha COE is not subcontracted by another health entity to provide these services, such as a County SMHS program, and Alpha COE maintains administrative control over all services, employs all providers, and funds the services. This means that **any information from education records that education staff *share to make referrals and coordinate care, or create insurance claims*, is subject to FERPA disclosure regulations.** This also means that ***information created by these employees* (e.g., school-employed therapists, psychologists) about services delivered to students that are entered into education records are subject to FERPA disclosure regulations.**

HIPAA Note: Alpha COE's TPB is also responsible for complying with HIPAA .

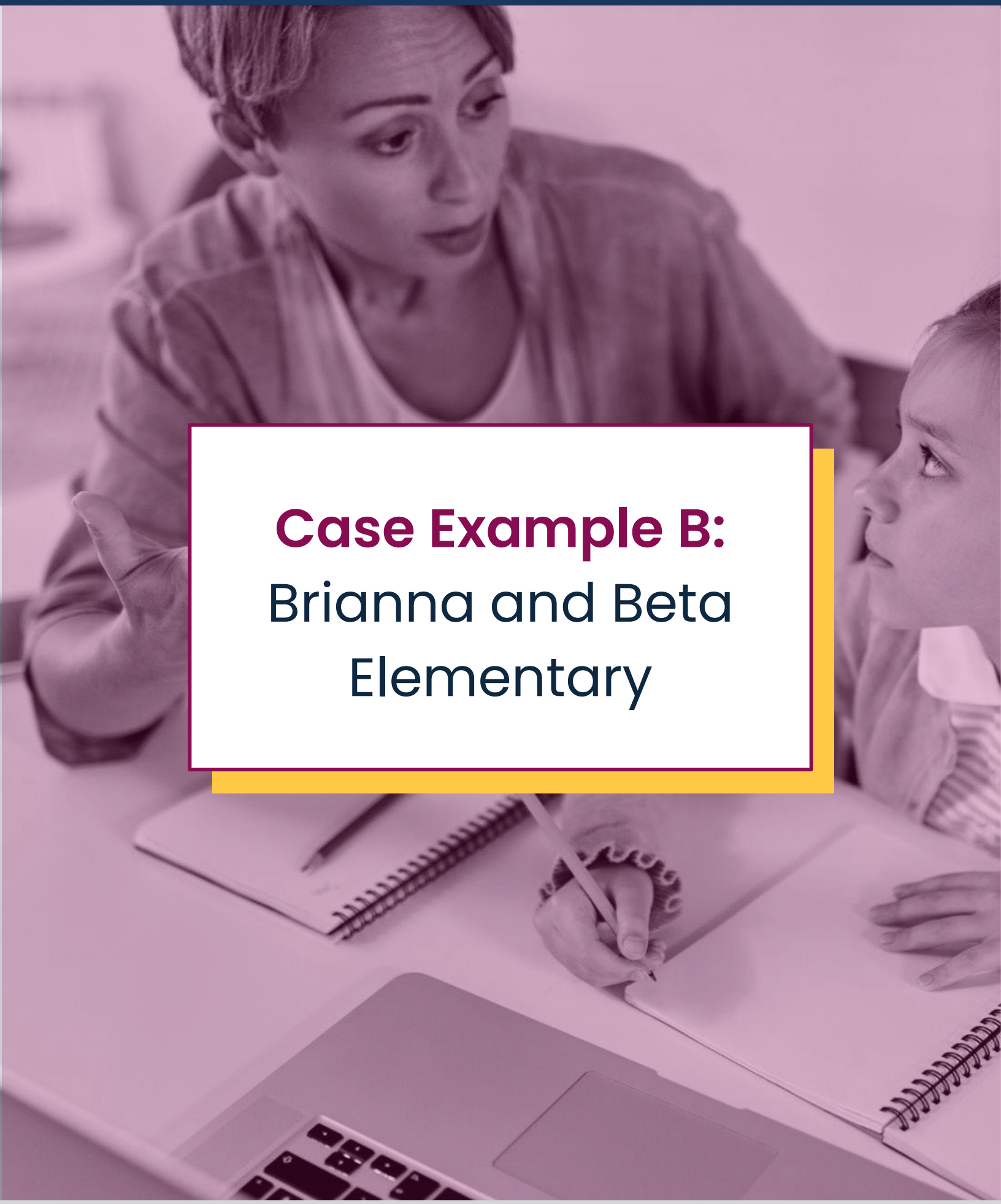
Steps	**1. Referral** 
Roles and Data Share	**Roles:** School nurse and Alpha COE Therapist **Data Shared:** Referral data
Description	11-year-old Amir, a student at Apple Elementary, is referred by the school nurse to a licensed marriage and family therapist (LMFT) hired employed by Alpha COE to receive psychotherapy. The school nurse shares Amir's date of birth, parent information, and class schedule with the therapist in accordance with the information-sharing policy in place.
Which Laws May Apply?	FERPA
May an ROI be Necessary? Why or Why Not?	**An ROI may not be necessary.** This is because all information being shared in a referral is subject to FERPA disclosure regulations. FERPA allows "school officials" in the same educational system to share education records with one another without an ROI if they have a "legitimate educational interest" in the information. ***Note:*** While a formal ROI may not be required in this example, the nurse may consider informing the family that information will be shared with the therapist. This builds both accountability and trust.

Steps	**2. Intake** 
Roles and Data Share	**Roles:** Alpha COE therapist and Amir's legal guardian **Data Shared:** No data is shared in this step
Description	At intake, the therapist explains to Amir and his legal guardian the scope of services and confidentiality, including confidentiality protections and the limits of confidentiality under FERPA. Amir's guardian consents to services. At the same time, Amir's guardian is asked to sign a FERPA-compliant ROI authorizing Alpha COE to use individually identifiable information from Amir's education record to seek reimbursement. This ROI explains the records that may be disclosed, the purpose, and to whom the disclosure is being made.
Which Laws May Apply?	FERPA may apply to the therapist, school, and Alpha COE.
May an ROI be Necessary? Why or Why Not?	**A FERPA-compliant ROI may be necessary to share individually identifiable information with the TPB and DHCS to submit a reimbursement claim.** An ROI may be necessary because there is no exception in FERPA that allows Alpha COE to share individually identifiable information from education records (e.g., special education information, service summary, student name, student date of birth) to bill without an ROI.

Steps	**3. Service Delivery and Care Coordination** 
Roles and Data Share	**Roles:** Alpha COE therapist and psychologist, Alpha Elementary nurse, and Amir's teacher **Data Shared:** Case summary information
Description	The therapist begins working with Amir and shares relevant summary information with the school psychologist (employed by Alpha COE) leading the school's wellness center to coordinate services and potentially refer Amir for more intensive support. The therapist also informs the Apple Elementary school nurse that Amir was connected to services. Amir's teacher also reaches out to his therapist to ask for specific details about his clinical diagnosis and family history
Which Laws May Apply?	FERPA
May an ROI be Necessary? Why or Why Not?	**The disclosures for referral and care coordination with the school psychologist and nurse may not require an ROI** according to the information-sharing policy in place. **Sharing a clinical diagnosis and family history with the teacher may require an additional FERPA-compliant ROI** because these details are outside the scope of legitimate educational interest. An alternative approach not requiring an additional ROI might be that the therapist confirms to the teacher that Amir is receiving services without divulging any additional details, such a diagnosis or management plan, provided that the teacher must be aware of Amir's receipt of services to perform their teaching duties (e.g., to coordinate Amir's school schedule).

Steps	**4. Claim Submission** 
Roles and Data Share	**Roles:** Alpha COE's Billing Coordinator, the TPB, and Medi-Cal **Data Shared**: Individually identifiable information from Amir's education record
Description	Alpha COE's Billing Coordinator submits individually identifiable information from Amir's education record to the TPB to request reimbursement for services. The TPB then communicates with Medi-Cal.
Which Laws May Apply?	FERPA
May an ROI be Necessary? Why or Why Not?	Since Alpha COE staff already obtained a FERPA-compliant ROI for billing purposes in step 2, **the billing coordinator may not need an additional ROI to share information with the TPB**. If a FERPA-compliant ROI had not been obtained, Alpha COE staff may need to obtain it from Amir's legal guardian. **The TPB must have a business associate agreement with DHCS** that requires it to abide by HIPAA regulations.

Steps	**5. Reimbursement**
Roles and Data Share	**Roles:** Medi-Cal **Data Shared:** No data is shared in this step
Description	Medi-Cal sends reimbursements on claims submitted
Which Laws May Apply?	**N/A**
May an ROI be Necessary? Why or Why Not?	**N/A**



Case Example B: Brianna and Beta Elementary

Context and Network Design

Who

At Beta Elementary, 7-year-old Brianna is participating in psychosocial health education provided by Beta-employed health providers.

Staff

Beta Elementary maintains "eligible"[44] professionals to offer several services at the school. Staff are Beta Elementary employees with no other agency affiliation and deliver services to students on school campuses.

Services

Staff offer several MTSS Tier 1-level prevention services, such as psychosocial health education and mental health first aid.

Reimbursement

Many of the services offered are eligible for reimbursement in the CYBHI Fee Schedule Program through a Third-Party Administrator, Carelon Behavioral Health.

Contracts/MOUs:

- Beta Elementary has entered a provider participation agreement (PPA)[53] with DHCS, which enrolls them in the CYBHI Fee Schedule Program's provider network and Medi-Cal program.
- Beta Elementary and Carelon have entered a DUA[54] as required by DHCS in which the parties agree to abide by HIPAA Security Rules that are related to maintenance and transmittal of CYBHI data, HIPAA (where applicable), and any other applicable confidentiality laws regarding the privacy and disclosure of CYBHI data.

How:

- **Referral to Services:** Teachers and other school staff make warm handoffs to Beta Elementary providers to connect students to services. Those providers use information from students' education records for referrals.
- **Care Coordination:** Beta Elementary providers use information from students' education records (e.g., assessment results, general health information) for care coordination with other Beta Elementary staff.

FERPA or HIPAA?

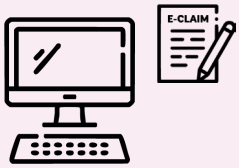
In this network design case example, data exchange is primarily governed by FERPA protections.

The providers are Beta Elementary employees with no additional affiliations. Beta Elementary is not providing services as a subcontractor to another health organization, such as a managed care plan. As such, **records about services delivered to students created by these providers are subject to FERPA**, not HIPAA. This is because the LEA maintains control over the administration of services on its campuses, the students who are served, the employees, and the financing of all services.

HIPAA Note: Carelon is subject to and must comply with HIPAA as a business associate of the state. Once records are received by Carelon from Beta Elementary, the records are covered by HIPAA and not FERPA.

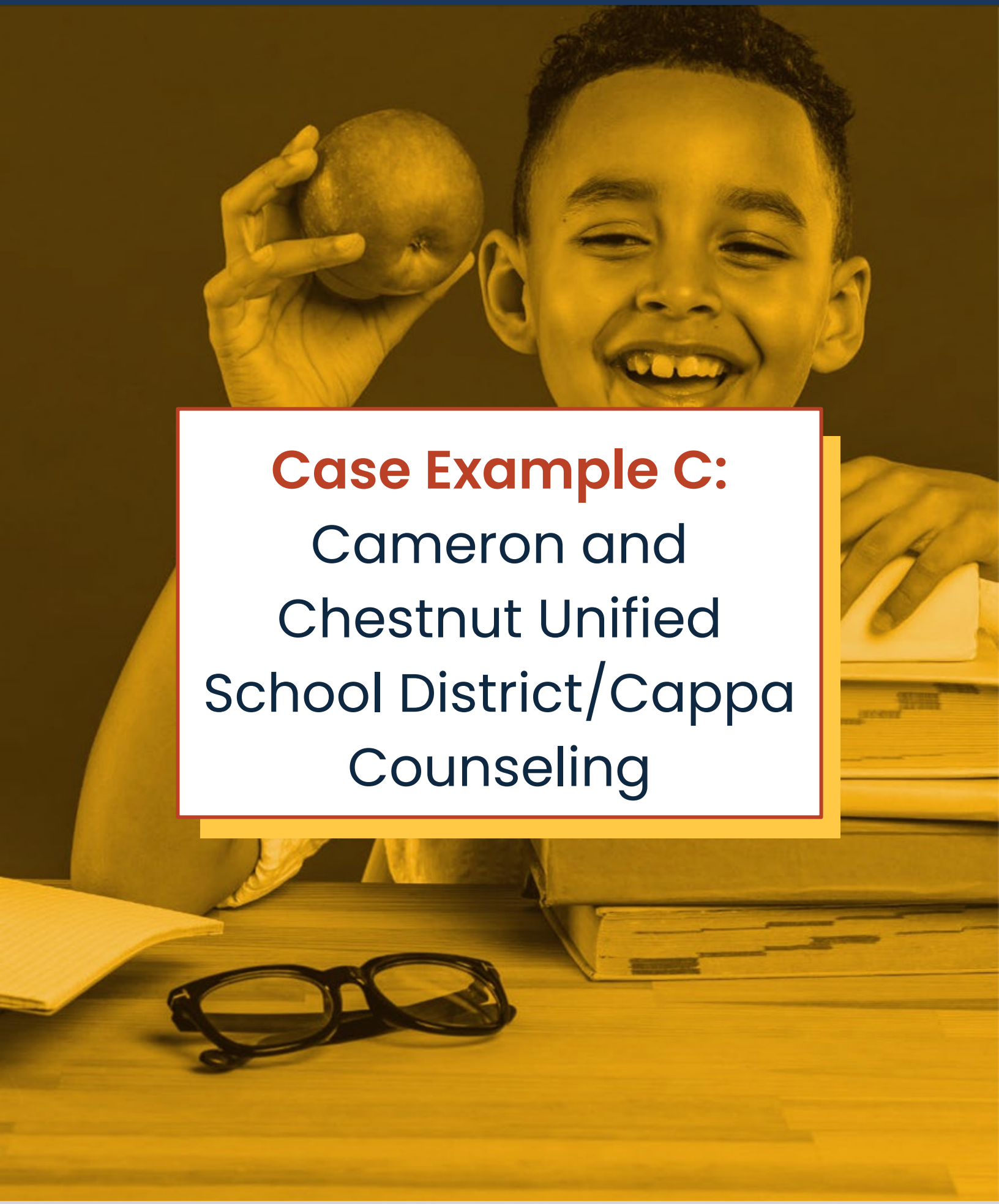
**This scenario is a special case because Carelon plays a specific role in CYBHI*

Steps	**1. Referral and Intake** 
Actors/ Data Shared	**Roles:** Brianna's parents and Beta Elementary staff and providers **Data Shared:** No data is being shared in this step
Description	7-year-old Brianna attends second grade at Beta Elementary. Brianna's parents are interested in having Brianna participate in psychosocial health education provided on campus by Beta Elementary staff, and give consent to "treatment," or participation in this program. Beta Elementary providers ask Brianna's parents to sign a HIPAA- and FERPA-compliant ROI, authorizing Beta Elementary to share relevant individually identifiable information with Carelon and DHCS to seek reimbursement for services provided from Brianna's family's insurer.
Which Laws May Apply?	FERPA
May an be ROI Necessary? Why or Why Not?	**A FERPA-Compliant ROI may be necessary** to share individually identifiable information collected or created by school staff (e.g., service summary) with Carelon and DHCS to seek reimbursement. An ROI may be necessary because there is no exception in FERPA that allows Beta Elementary to disclose individually identifiable information from education records to an outside entity for reimbursement purposes without an ROI. **Note: A HIPAA-compliant ROI may not be necessary in this case example** because HIPAA allows DHCS and insurers to disclose PHI for "payment" and "health care operations" without requiring a written ROI. However, Beta Elementary legal counsel decided to use a HIPAA-compliant ROI as a best practice and to facilitate insurance reimbursement and communications with Carelon and insurers.

Steps	**2. Claim Submission** 
Actors/ Data Shared	**Roles:** Beta Elementary and Carelon **Data Shared:** Individually identifiable information from Brianna's education record
Description	Beta Elementary submits a claim to Carelon via an electronic records system.
Which Laws May Apply?	FERPA
May an be ROI Necessary? Why or Why Not?	**An ROI may not be necessary,** because the HIPAA- and FERPA-compliant ROI signed in Step 1 included language authorizing Beta Elementary to disclose and receive information necessary to seek reimbursement from DHCS and insurers through Carelon.

Steps	**3. Claim Forwarding** 
Actors/ Data Shared	**Roles:** Carelon and the insurer **Data Shared:** Claim information
Description	Carelon identifies the appropriate insurer and forwards the appropriate information. The insurer then reviews the claim.
Which Laws May Apply?	The business associate agreement, PPA, DUA, and HIPAA
May an be ROI Necessary? Why or Why Not?	**An ROI may not be necessary,** because the business associate agreement, PPA, and DUA establish parameters around data exchange for claims and remittance. In Step 1, Brianna's parents also signed a HIPAA-compliant ROI authorizing communication for reimbursement purposes.

Steps	**4. Reimbursement** 
Actors/ Data Shared	**Roles:** The insurer, Carelon, and Beta Elementary **Data Shared:** No data is being shared in this step
Description	The insurer provides claims funding to Carelon, and Carelon remits the claims funding to Beta Elementary.
Which Laws May Apply?	N/A
May an be ROI Necessary? Why or Why Not?	N/A



Case Example C:

Cameron and Chestnut Unified School District/Cappa Counseling

Context and Network Design

Who

14-year-old Cameron and other middle and high school students in Chestnut Unified School District.

Staff

Health care professionals from Cappa Counseling, a local CBO, provide services three days per week in Chestnut Unified School District on middle and high school campuses.

Services

Health care professionals from Cappa Counseling provide psychotherapy and group counseling.

Reimbursement

Cappa Counseling shares some service delivery information with Chestnut Unified (e.g., number of service sessions, diagnoses) so that Chestnut Unified staff may determine eligibility for reimbursement. When services are eligible for reimbursement, Chestnut Unified's Billing Coordinator submits information to their TPB, which submits a claim for reimbursement that includes information from the student's educational record.

Contracts/MOUs:

Legal counsel for Chestnut Unified and Cappa Counseling have a contract in place outlining their roles in service delivery and reimbursement. Chestnut Unified reimburses Cappa Counseling for campus services, and Cappa staff, acting as school officials on campus, must comply with FERPA regulations. Chestnut Unified, their TPB, and payers have additional agreements **establishing the TPB as a HIPAA business associate for the purposes of data use and information exchange. To draft business associate agreements, consult with your legal counsel.**

How:

- **Referral to Services:** Chestnut Unified school staff, including school counselors and nurses, make warm referrals to the Cappa Counseling staff on site to connect students to services using individually identifiable information from education records.
- **Care Coordination:** Chestnut Unified staff may reach out to Cappa Counseling providers to request their participation in care coordination and/or for general information about the needs of specific students.

FERPA or HIPAA?

In this network design case example, data exchange is primarily governed by FERPA protections.

Because of the agreement Cappa Counseling has entered with Chestnut Unified, Cappa Counseling is considered a "school official" for purposes of service delivery on Chestnut Unified campuses and most documentation on services delivered to students on school campuses created by Cappa staff is subject to FERPA, not HIPAA. This includes individually identifiable information from education records that Chestnut Unified school staff use for referrals to Cappa Counseling or to coordinate care between Chestnut Unified and Cappa Counseling and any information from education records that Chestnut Unified staff use to create reimbursement requests (e.g., date of birth).

HIPAA Note: For billing purposes, Chestnut Unified and their TPB must comply with HIPAA when transferring insurance claims and remittance information.

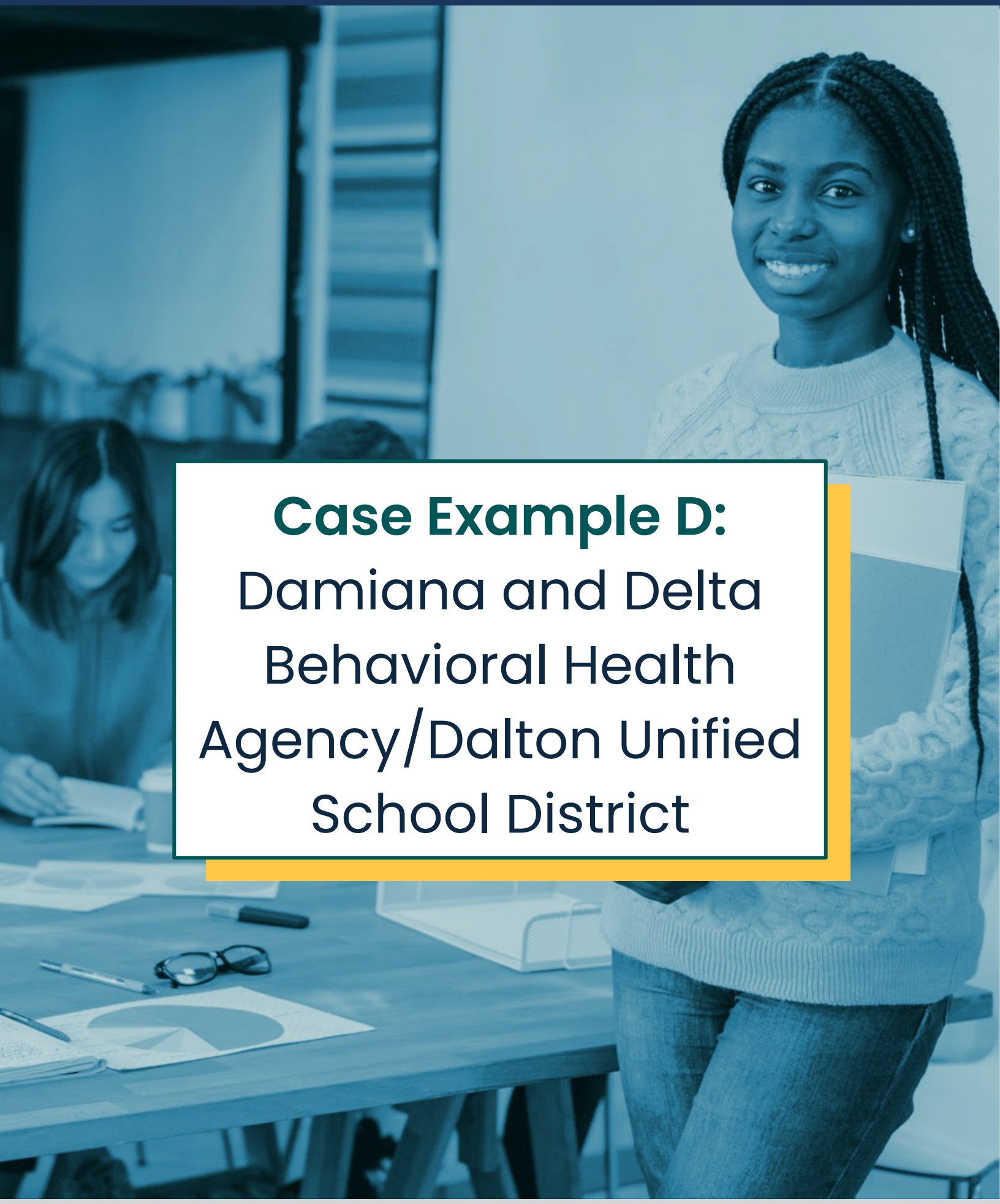
Steps	**1. Referral** 
Roles and Data Share	**Roles:** Cameron's parents and teacher, and the Cappa counselor **Data Shared:** Cameron's school schedule and parent information
Description	14-year-old Cameron is a student at Chestnut Unified High School. Their teacher refers them to the Cappa Counseling counselor on campus after Cameron's parents request a therapy referral following a family loss. Cameron's teacher shares Cameron's information, including their school schedule and parent information, with the Cappa counselor.
Which Laws May Apply?	FERPA
May an ROI be Necessary? Why or Why Not?	**An ROI may not be needed for this referral.** In this situation, Cappa Counseling is considered a "school official." FERPA allows "school officials" in the same educational system with a "legitimate educational interest" to share education records with one another without an ROI.

Steps	**2. Intake** 
Roles and Data Share	**Roles:** Cameron, his parents, and the Cappa Counseling Licensed Clinical Social Worker (LCSW) **Data Shared:** No data is shared in this step
Description	Cameron and their parents meet with the Cappa Counseling LCSW therapist for an intake at school. The LCSW explains the scope of services and confidentiality, including confidentiality protections and their limits under FERPA. Cameron's parents consent to services. Cameron's parents are asked to sign a FERPA-compliant ROI authorizing Chestnut Unified to use individually identifiable information from Cameron's education record to seek reimbursement through Chestnut Unified's TPB.
Which Laws May Apply?	FERPA
May an ROI be Necessary? Why or Why Not?	**A FERPA-compliant ROI may be necessary to share individually identifiable information with Chestnut Unified' s TPB and DHCS to submit a reimbursement claim.** An ROI may be necessary because there is no exception in FERPA that allows Chestnut Unified to share individually identifiable information from education records for billing without an ROI.

Steps	**3. Service Delivery and Care Coordination** 
Roles and Data Share	**Roles:** The LCSW, Cappa Unified Counselor, and Cameron's teacher **Data Shared:** Case summary information
Description	The LCSW provides services to Cameron and shares relevant summary information with the Chestnut Unified counselor who leads the student support team. The Chestnut Unified counselor tells Cameron's teacher that they are receiving services and asks the teacher to reach out if Cameron is struggling, without disclosing any additional information.
Which Laws May Apply?	FERPA
May an ROI be Necessary? Why or Why Not?	**Chestnut Unified and Cappa may not need an ROI for their staff to coordinate care** because they are part of the same educational system, as noted in step 1. Note: legal counsel decided to require an ROI as described in step 2 to provide families and students with an understanding about who comprises the student's care team for transparency purposes.

Steps	**4. Claim Submission** 
Roles and Data Share	**Roles:** Chestnut Unified's Billing Coordinator, the TPB, and Medi-Cal **Data Shared:** Individually identifiable information from Cameron's education record
Description	Chestnut Unified's Billing Coordinator submits individually identifiable information from Cameron's education record to the TPB to request reimbursement for services via the TPB's electronic records system. The TPB then communicates with Medi-Cal.
Which Laws May Apply?	FERPA and HIPAA
May an ROI be Necessary? Why or Why Not?	**In Step 2, a FERPA-compliant ROI was obtained, which allows Chestnut Unified to share information with the TPB for billing.** **HIPAA Note:** Once the information is submitted to the TPB via their electronic records system, it is governed by HIPAA. The TPB has a business associate agreement with DHCS in which it committed to abide by HIPAA regulations.

Steps	**5. Reimbursement** 
Roles and Data Share	**Roles:** Medi-Cal **Data Shared:** No data is being shared in this step
Description	Medi-Cal sends reimbursements on claims submitted.
Which Laws May Apply?	N/A
May an ROI be Necessary? Why or Why Not?	N/A



Case Example D: Damiana and Delta Behavioral Health Agency/Dalton Unified School District

Context and Network Design

Who

14-year-old Damiana and other middle and high school students in Dalton Unified School District.

Staff

Health care professionals are employed by Delta Behavioral Health Agency, a Medi-Cal enrolled provider contracted as a network provider with the county SMHS program to provide specialty mental health services off campus.

Services

A range of mental health services including individual psychotherapy.

Reimbursement

Delta Behavioral Health staff share authorization requests and reimbursement claims with the county SMHS program using information housed in their own records to complete the claims paperwork.

Contracts/MOUs:

All of Delta's behavioral health services are provided independently and off campus, so there is no contract in place with Dalton Unified. However, there is a contract in place between Delta and county SMHS programs outlining roles and responsibilities related to providing specialty mental health services, including HIPAA compliance.

How

Referral to Services and Care Coordination: Dalton Unified school staff provide students and families with information about Delta Behavioral Health as a service option, but they do not share any individually identifiable student information with Delta directly, unless consented to by the parents or guardians for the purposes of care coordination at school.

FERPA or HIPAA?

In this case example, both HIPAA and FERPA apply.

Delta Behavioral Health is a HIPAA-covered entity. There is no formal arrangement or relationship between Dalton Unified and Delta, and Delta is not acting as a "school official" in relation to Dalton Unified. Therefore, individually identifiable patient information from services delivered by Delta staff is subject to HIPAA. Both the county SMHS program and Delta must comply with HIPAA with respect to ePHI.

Individual identifiable information in Dalton Unified records is subject to FERPA. This means that Dalton Unified staff must honor FERPA disclosure rules if sharing individually identifiable student information (e.g., school schedule, academic performance, attendance) from education records to coordinate care with Delta providers.

Steps	**1. Referral** 
Roles and Data Share	**Roles:** Damiana's parents and the school counselor **Data Shared:** No data is being shared in this step
Description	The parents of 14-year-old Damiana, a student at Dalton High School, reach out to the school counselor to request a referral for therapy. The school counselor provides information about Delta Behavioral Health.
Which Laws May Apply?	FERPA, if applicable
May an ROI be Necessary? Why or Why Not?	Delta is not acting as a "school official," so a FERPA-compliant ROI may be needed if school staff share any individually identifiable information from education records with Delta. However, **an ROI may not be necessary if Dalton Unified staff are not sharing individually identifiable information with Delta.** In this case, Dalton Unified staff provides information about Delta to Damiana's parents rather than sharing her information directly with Delta.

Steps	**2. Intake** 
Roles and Data Share	**Roles:** Damiana and their parents, and a Delta Behavioral Health psychologist **Data Shared:** No data is being shared in this step
Description	Damiana and their parents meet with a licensed psychologist at Delta Behavioral Health. The psychologist explains the scope of services they offer, as well as confidentiality protections and limitations under HIPAA and California law. Damiana and their parents are asked to sign a HIPAA-compliant ROI that authorizes Delta to deliver services and seek reimbursement through Medi-Cal. The psychologist then provides services to Damiana.
Which Laws May Apply?	HIPAA
May an ROI be Necessary? Why or Why Not?	Individually identifiable patient information created by Delta is subject to HIPAA, which **allows disclosure of PHI for TPO purposes without requiring a written ROI.** Note: Delta's legal counsel decided to use an ROI as a best practice and to facilitate Delta's ability to communicate with the county SMHS program.

Steps	**3. Service Delivery and Care Coordination** 
Roles and Data Share	**Roles:** Damiana's parents, the Dalton High School counselor, and the school staff **Data Shared:** Case summary information
Description	Damiana's parents inform the Dalton High School counselor that Damiana is receiving services from a Delta Behavioral Health psychologist. The Dalton High School counselor asks if they can coordinate with the Delta psychologist to help school staff better support Damiana. After they express support, Damiana and their parents complete both a FERPA-compliant ROI and a HIPAA-compliant ROI.
Which Laws Apply?	HIPAA & FERPA
Is an ROI Necessary? Why or Why Not?	Delta is not operating as a "school official," so a FERPA-compliant ROI may be needed when Dalton Unified staff want to share individually identifiable information from education records with Delta for ongoing care coordination. **Delta Behavioral Health's legal counsel requires a HIPAA-compliant ROI** authorizing Delta staff to share information with Dalton, because this information may be exposed to non-provider staff and may be placed in the school education record. The roles and responsibilities outlined in this ROI may be different than those in ROI signed in step 2.

Steps	**4. Claim Submission** 
Roles and Data Share	**Roles:** Delta Behavioral Health and the county plan **Data Shared:** Service authorization and claims information
Description	Delta determines that the services delivered to Damiana is eligible for reimbursement under Medi-Cal. Delta submits service authorization and claims information to the county plan through an electronic records system.
Which Laws Apply?	HIPAA
Is an ROI Necessary? Why or Why Not?	The HIPAA-compliant ROI signed in Step 2 included language authorizing Delta to disclose information necessary to seek reimbursement. It is likely that **no other ROI is necessary.**

Steps	**5. Claim Receipt** 
Roles and Data Share	**Roles:** Medi-Cal **Data Shared:** No data is being shared in this step
Description	Once the county Medi-Cal plan receives the claim, the information becomes part of the plan's records and remains subject to HIPAA protections.
Which Laws Apply?	HIPAA
Is an ROI Necessary? Why or Why Not?	The county Medi-Cal plan is a HIPAA-covered entity and must honor HIPAA privacy and disclosure requirements for claims information once received. **No information is being exchanged in this step and therefore an ROI may not be needed.**

Steps	**6. Reimbursement** 
Roles and Data Share	**Roles:** Medi-Cal and Delta Behavioral Health **Data Shared:** No data is being shared in this step
Description	The Medi-Cal plan reimburses Delta.
Which Laws Apply?	N/A
Is an ROI Necessary? Why or Why Not?	N/A

Confidentiality and Information Sharing Tools

This section of the Toolkit covers some of the key tools needed to manage confidentiality and disclosure of information in different network designs, the contents of which will depend on whether FERPA, HIPAA, or other laws apply. Legal counsel should always be involved when developing these tools.

Key tools include but are not limited to:

01 **Releases of Information (ROIs):** These are often necessary to support information exchange for service delivery, billing, and/or reimbursement. ROIs help manage the sharing of student information as shown in the case examples.

02 **Agreements (Contracts, MOUs):** These are sometimes needed to execute service delivery, billing, and reimbursement processes. Agreements outline legal obligations and establish the vision and intended outcomes of your network design(s).

03 **Information Notices:** Both FERPA and HIPAA require certain disclosures and notices . As a best practice, consider developing guidance that is family-friendly.

04 **Guidance on Information Sharing:** Once agreements are in place regarding network design and legal counsel has helped map confidentiality and disclosure rules, policy and practice guidance can help "translate" legal requirements into real-world scenarios and help staff with implementation.

05 **Staff Training:** After confidentiality and disclosure processes are established, staff training is essential to ensure they know what to document, how to discuss confidentiality and its limits with families, how to complete referrals, and when to consult with legal counsel.

06 **Messaging for Families:** Clear, accessible communication tools help families understand the services provided, their rights, and how their information may and may not be used. In addition to family and youth information notices, consider distributing handouts or other materials to explain confidentiality and information sharing in simple terms.

Releases of Information (ROI)

When developing ROI(s), you should discuss each of the questions below with your legal counsel(s).

Type of Forms:[55]

1. Is a FERPA ROI necessary for referral, service delivery, billing, and/or reimbursement?
    a. If yes, it must meet the requirements for a FERPA-compliant ROI.[56]
2. Is a HIPAA ROI necessary for referral, service delivery, billing, and/or reimbursement?
    a. If yes, it must meet the requirements for a HIPAA-compliant ROI.
3. Must the ROI satisfy other confidentiality laws or regulations (e.g., Confidentiality of Medical Information Act (CMIA), the Insurance Information and Privacy Protection Act (IIPPA), 42 C.F.R. Part 2)?
    a. If yes, consider each law's requirements. For example, the CMIA and the IIPPA have their own requirements for compliant releases, and an ROI may need to meet the requirements of CMIA or the IIPPA, as well as HIPAA and/or 42 C.F.R. Part 2.

Content of Forms:

4. Given your current and/or future network design(s), what information-sharing scenarios need to be described and included in your ROIs? For example, do disclosures to the state TPA and/or insurers for billing and/or disclosures from an LEA to providers for referral and care coordination need to be included?
    a. What information should be collected? What timeline needs to be included?

Process and Procedure:

4. Given the confidentiality laws implicated, who must or may sign the ROI?
5. If both a FERPA-compliant and HIPAA-compliant ROI are necessary for billing, will there be situations in which the signature of more than one person will be necessary?
6. How will legally compliant ROIs be obtained? Is this something to address in agreements between partners?
7. What is the mechanism for an authorization to be withdrawn?

Sample Forms: The document linked below is just a sample. As such, *it must be customized to your specific context, in partnership with your legal counsel.*

- A sample ROI consent form from DHCS can be found here: ASCMI-CalAIM[57]

The Authorization to Share Confidential Medi-Cal Information (ASCMI) Form is a voluntary standardized consent form developed by DHCS. While a new version is under development, the pilot version is currently available for use. DHCS intends to publish and maintain the ASCMI form, which is intended for providers to obtain consent from Medi-Cal; members for the sharing of certain sensitive HSSI, as well as to inform individuals of their privacy rights and the process to express their consent preferences for data disclosures. Once the finalized ASCMI form is released, LEAs, providers, TPBs/TPAs, and insurers are strongly encouraged to adopt the form.

Agreements

Different agreements may be needed to manage referrals, service delivery, billing, and reimbursement processes. Although just a small subset, examples of the agreements that may be deemed necessary by legal counsel include those between:

01
Health Care Provider and LEA

02
Billing entity (Provider/LEA) and DHCS

03
TPA /TPB and billing entity (Provider/LEA)

04
TPA and Insurers (if applicable)

These agreements often include data-sharing provisions and/or will be supplemented by DUAs. When developing agreements, it is important to discuss the following questions with legal counsel:

1. What role does each agency play? For example, what services, equipment, and commitments is each agency offering?
2. Which agency is ultimately responsible for delivering services?
3. Which agency (if any) will seek reimbursement from insurance or other funding sources?
4. Is a provider acting as a contracting "school official" of an educational agency?
5. Is a partner acting as a contracting "business associate" of a HIPAA-covered entity?
6. What confidentiality laws apply to student or patient information for referral, service delivery, billing, and reimbursement in your network design?
7. What records will be created throughout, and why are they needed??
8. Who will have access to the records, and what is the reason for that access? How will they access records?
9. Where will records be maintained and how? Do applicable laws impose storage and security requirements that must be considered (e.g., HIPAA Security Rule)?

10. What additional confidentiality rules (e.g., CMIA, IIPPA, 42 CFR Part 2, etc.) apply given the services offered?
11. What are the required and allowed (but optional) confidentiality and disclosure practices? What are the best practices, keeping your shared goals and guiding principles[58] in mind?

Information Notices

Both FERPA and HIPAA require that certain disclosures and notices be created and shared. When developing and disseminating these notices, work with legal counsel to determine the specifics, including:

- **LEA Annual Notices:** LEAs are required to distribute these to parents/guardians annually. Review whether the updates are needed with your legal counsel.
- **Information Packets:** Legal counsel should review what forms or information to include in these packets, such as ROIs, other forms and protocols, and/or service overviews.
- **HIPAA Annual Notice of Privacy Practice:** HIPAA-covered entities must give certain privacy notices to patients. Legal counsel can advise when and how to distribute these notices, and what they should include.

Policy and Practice

Decisions made in agreements and forms should be turned into written policies to ensure consistent implementation. Some policies may not be legally required but may be considered best practices to help partners achieve shared goals within the ecosystem.

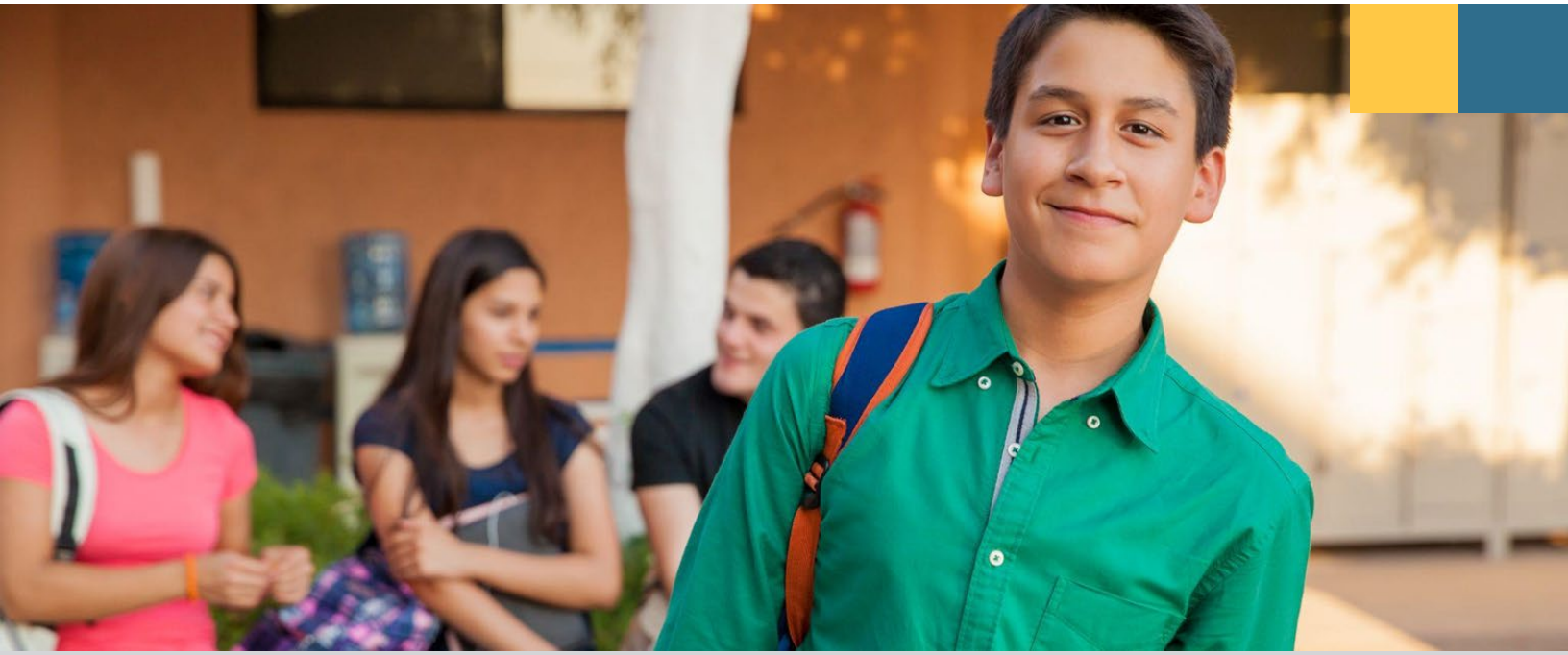
Staff Training

Once confidentiality and disclosure processes are established, all staff involved in service delivery, billing, and reimbursement should be trained on these procedures. Training ensures everyone understands their role and responsibilities within the ecosystem.

Where Do I Go From Here?

Building a collaborative system of behavioral health care for children, youth, and families in California takes time, dedication, and shared commitment between education and health partners. By focusing on shared goals, partners can ensure that families get the care they need while respecting their privacy and following confidentiality laws. As a leader in this effort, you have the ability to break down barriers and create more connected systems.

This Toolkit is designed to help you and your colleagues navigate the complexities of confidentiality and information-sharing. Although this work can feel overwhelming, there are concrete steps you can take to build, improve, or strengthen confidentiality practices.



Next Steps Checklist

- ◯ **Identify Key Champions:** Find individuals within your organization and partner organizations who are passionate about strengthening school-behavioral health partnerships and have the influence to drive change.
- ◯ **Connect with Partners:** Reach out to existing and potential partners in education, health care, and community organizations to discuss your approach to confidentiality and information sharing across systems. Consult information technology and legal counsel with experience regarding the confidentiality of school records, health records, and the like.
- ◯ **Review the Toolkit Together:** Schedule time with partners to go over this Toolkit, align on goals, and plan how to apply the guidance.
- ◯ **Develop Systems:** Assess your current processes for managing confidentiality and information sharing and consider how the case examples in this Toolkit might apply to your unique context. After reading these materials, and if you still have questions or concerns about sharing confidential information, please consult with your legal counsel.
- ◯ **Evaluate Tools:** Identify which tools from this Toolkit need to be refined or created to help achieve shared goals.
- ◯ **Create Sustained Collaboration:** Set up regular check-ins (e.g., quarterly meetings) to maintain momentum and ensure continued collaboration.

By taking these steps you can help build a more connected and effective system of care, ensuring that families get the support they need to thrive.

Appendix A

Guiding Principles for the Toolkit

Laws offer a baseline for compliance, but the values and principles below should also be used to guide decisions on confidentiality and information sharing in school-behavioral health partnerships.

Maintain Transparency: Inform families about confidentiality and its limits and explain the purpose of information sharing, ensuring that any forms are easy to understand and user-friendly.

Build Trust: Use plain language and center family experiences when building relationships across systems to build trust.

Allow for Autonomy: Always obtain consent for disclosures when possible and make provisions for situations in which a family may choose not to consent.

Integrate Across Sectors: Develop a shared vision, goals, accountability, and support across government, non-profit, health, education, advocacy, and others.

Center Children, Youth & Families: Craft strategies by, for, and with families, ensuring that their needs, voices, and perspectives are represented.

Focus on Equity: Advance outcomes for those facing the greatest systemic barriers to wellness and who are disproportionately impacted by behavioral health issues.

Practice Intentionality: Dedicate the time needed to make thoughtful decisions about confidentiality, consent, and information sharing.

Partner Together: Collaborate with partners to build systems that are easy to navigate, and where there is no wrong door to seek help.

Appendix B

Additional Key Resources

Additional resources about FERPA, HIPAA, and other privacy and confidentiality laws include, but are not limited to:

FERPA & HIPAA Joint Guidance on the Application of FERPA and HIPAA to Student Health Records (U.S. ED)

A California Guide for Sharing Student Health and Education Information (California School-Based Health Alliance)

HIPAA or FERPA? A Primer on Sharing School Health Information in California, 2nd Edition (National Center for Youth Law)

Other Confidentiality Laws and Guidance:

- 42 C.F.R Part 2
- HIPAA Security
- The 21st Century Cures Act
- (HITECH) Act related to protecting electronic health records (EHRs)
- SOPIPA
- Data Sharing Authorization Guidance (DSAG) 2.0 California Information Practices Act
- Other student information privacy protection laws, both federal and state (e.g., Ed. Code § 49060 et seq)

Appendix C

Protection & Storage of Electronic Information

This Toolkit and case examples focus exclusively on confidentiality (the HIPAA Privacy Rule) and not on security obligations for electronic data storage and transfer (the HIPAA Security Rule).

However, please note that **while FERPA and the HIPAA Privacy Rule will never apply at the same time, FERPA and the HIPAA Security Rule can.**

Even if a health care provider is considered a HIPAA-covered entity, the health information the provider creates won't be subject to the *HIPAA Privacy Rule* if that information is part of an education record subject to FERPA. However, the provider may still need to comply with other HIPAA requirements, such as the *HIPAA Security Rule.*

The 2008 Joint Guidance from the ED and HHS gives an example of a scenario in which FERPA and the HIPAA Security Rule both apply:

> [I]f a public high school employs a health care provider that bills Medicaid electronically for services provided to a student under the Individuals with Disabilities Education Act (IDEA), the school is a HIPAA covered entity and would be subject to the HIPAA requirements concerning transactions. However, if the school's provider maintains health information only in what are education records under FERPA, the school is not required to comply with the HIPAA Privacy Rule. Rather, the school would have to comply with FERPA's privacy requirements with respect to its education records."[59]

In this case, while the provider's records are subject to FERPA disclosure requirements generally, when the school bills Medicaid for services, the school must ensure that the information system it uses to maintain and transfer electronic health information meets the physical, technical, and administrative requirements of the HIPAA Security Rule.

For more information regarding the HIPAA Security Rule and other federal and state laws that set *administrative, physical, and technical requirements* for information technology and electronic data storage and communication, please review:

- HIPAA Security
- The 21st Century Cures Act
- (HITECH) Act related to protecting EHRs
- SOPIPA

For additional information about EHR systems and applicable state and federal laws, see the DHCS Privacy Office webpage[60], and consult legal counsel.

Operationalization Considerations

While this Toolkit suggests tools for building your own network designs, there are many other tools that may be needed but are not included here. This Toolkit is not meant to imply that no other tools are required.

Appendix D

Glossary

1. **Business Associate:** An individual or organization that performs certain functions or activities on behalf of, or provides services to, a covered entity that involves the use or disclosure of protected health information.
2. **Community-Based Organization (CBO):** Non-profit organizations that work at the local level to improve life for residents, often involved in providing health and social services.
3. **Claim:** Claims information may include Student Name, Birth Date, Physical Address, Phone Number, Email Address, Date of Service, Health Plan Beneficiary, Service Billing Code, Social Security #, Medical Record #, Diagnosis Code (if relevant), Medical Necessity
4. **Confidentiality of Medical Information Act (CMIA):** A California state law that protects the privacy of medical information held by health care providers and health care service plans.
5. **Confidential Communications Request:** A request made by a patient to a health plan or provider to send communications about health services to a specific location or in a specific manner to protect privacy.
6. **Consent Form:** A document used to obtain consent from a patient or their legal guardian before a health care provider can perform a specific action, such as treatment or the ROI.
7. **Covered Entity:** Under HIPAA, this refers to health plans, health care clearinghouses, and health care providers who transmit health information in electronic form related to certain transactions.
8. **Designated Providers and Practitioners List:** A list of providers and practitioners an LEA designates to render services on its behalf. In this context, employed, contracted, and affiliated practitioners may include individual designated practitioners (e.g., PPS credentialed provider, contracted RN) or broader designated entities (e.g., CBOs, FQHCs).

9. **Electronic Health Records (EHR):** Digital versions of patients' paper charts, containing their medical and treatment histories, used to streamline the sharing of information among health care providers.
10. **Family Educational Rights and Privacy Act (FERPA):** A federal law that regulates access and disclosure of students' education records. Applies to all schools that receive funds under an applicable program of the U.S. ED.
11. **Federally Qualified Health Center (FQHC):** A type of health care provider that receives federal funding to provide primary care services in underserved areas, often including mental health services.
12. **Health Insurance Portability and Accountability Act (HIPAA):** A federal law that protects the privacy of individually identifiable health information held by covered entities, such as health plans, health care clearinghouses, and health care providers.
13. **Insurance Information and Privacy Protection Act (IIPPA):** A California state law that protects the privacy of medical information held by insurers.
14. **Local Educational Agency (LEA):** Refers to a public board of education or other public authority within a state that maintains administrative control of public elementary or secondary schools.
15. **Local Education Agency Billing Option Program (LEA BOP):** LEA BOP reimburses LEA BOP Providers (school districts, county offices of education, charter schools, state special schools, community college districts, California State Universities, and University of California campuses) the federal share of the maximum allowable rate for approved health-related services provided by qualified health service practitioners to Medi-Cal eligible students.
16. **Medi-Cal:** California's Medicaid program providing health care services for low-income individuals, including many students in school-based health services.
17. **Memorandum of Understanding (MOU):** A formal agreement between two or more parties, often used to establish collaborative efforts between schools and health care providers.

18. **Multi-Tiered Systems of Support (MTSS):** An integrated, comprehensive framework that focuses on CCSS, core instruction, differentiated learning, student-centered learning, individualized student needs, and the alignment of systems necessary for all students' academic, behavioral, and social success (from CA Department of Education).
19. **Network Design:** The structure of service delivery and reimbursement within school-behavioral health partnerships, determining how and when FERPA, HIPAA, and other laws apply.
20. **Pupil Records / Education Records:** Records maintained by an educational institution that contain information directly related to a student and are protected under FERPA.
21. **Release of Information (ROI):** A document signed by a patient or their legal guardian authorizing the release of PHI to a specified entity or individual.
22. **School-Linked Behavioral Health Provider Network:** A network of health care providers affiliated with schools to offer integrated behavioral health services.
23. **School Official:** A person employed by an educational institution, such as teachers, counselors, or school nurses, who has a legitimate educational interest in accessing student records. A school official could also be a contractor, consultant, or volunteer, or other person that the educational institution uses to do work on its behalf, among other criteria.
24. **Third-Party Administrator (TPA):** The state TPA for the CYBHI Fee Schedule Program will serve as a claims clearinghouse and provider network management for fee schedule providers and payers.
25. **42 C.F.R. Part 2:** Federal regulations that govern the confidentiality of substance use disorder patient records, restricting the disclosure of such information without patient consent.

Appendix E

Guide for Providers: Communicating with Families about Privacy and Information Sharing in School-Based Mental Health Services

Release of Information Forms

In instances when individual consent is required **schools and providers must obtain consent to disclose data pursuant to the federal and state laws and ensure that they comply with the following at a minimum:**

- Use appropriate consent to disclose information forms that are compliant with federal and state standards to secure consent to share FERPA or HIPAA information when required. HIPAA and FERPA both specify a set of requirements for consent forms. In the event that they use their own consent forms, schools and providers should review with their counsel these requirements, including:
  - The student's name, and the names or other specific identification of the persons, or class of persons, authorized to make the disclosure;
  - A specific and meaningful description of the information that will be shared;
  - The names or class of the data recipients;
  - The purpose of the data sharing;
  - The right to revoke consent in writing; and
  - An expiration date (if needed).
- Schools and educational agencies must have an agreement in place with their network of providers to ensure appropriate consent forms are used. BHPs must also recognize electronic signatures and verbal consents if their use complies with applicable laws.[61,62]

Appendix F

Acknowledgements

This toolkit was developed by the State of California with input from youth, families, and subject matter experts representing health care providers, health plans, TK-12 education, and legal sectors, with special acknowledgment to Rebecca Gudeman and Elizabeth Estes. Administrative support was provided by Third Sector Capital Partners, Inc. under contract with CalHHS through the Children & Youth Behavioral Health Initiative.

References

1. More information about the California Children and Youth Behavioral Health Initiative (CYBHI) can be found here: https://cybhi.chhs.ca.gov/
2. More information about the CYBHI Fee Schedule program can be found here: https://www.dhcs.ca.gov/CYBHI/Pages/Fee-Schedule.aspx
3. More information about the Community Schools Partnership Program can be found here: https://www.cde.ca.gov/ci/gs/hs/ccspp.asp
4. This refresher section was excerpted with permission from Gudeman, HIPAA or FERPA? A Primer to School Information Sharing in California, 3rd edition, National Center for Youth Law, 2024 (forthcoming). It was reviewed and adapted by Gudeman and Estes, co-authors of this Toolkit, in July 2024.
5. Review Appendix B: Additional Key Resources
6. 34 C.F.R. § 99.1. ("CFR" means the Code of Federal Regulations.)
7. 34 C.F.R. § 99.3.
8. See Ca. Ed. Code § 49060 et seq.
9. 34 C.F.R. § 99.3.
10. 34 C.F.R. §§ 99.30, 99.31.
11. 34 C.F.R. § 99.31.
12. References to "insurers" in the Toolkit refers to health insurance companies, health maintenance organizations or HMOs, employer-sponsored health plans, and government programs that pay for health care, like Medicare, Medicaid, and military and veterans' health programs.
13. HIPAA covered entities in the context of schools can be private schools, schools that provide healthcare services to the public, and schools that conduct transactions electronically outside of the education record.
14. 45 C.F.R. §§ 160.102, 160.103.
15. 45 C.F.R. § 160.103.

References

16. See 45 C.F.R. § 164.302 et seq. Although it is important to understand whether, when, and how the HIPAA Security Rule applies, as well as all its technical requirements, when selecting health information systems and developing electronic data storage and exchange policies and practices, to ensure compliance with federal law, the Security Rule is outside the scope of this Toolkit.
17. 45 C.F.R. §164.502(a).
18. 45 C.F.R. §§ 164.502(a),164.512.
19. 45 C.F.R. §§ 164.502(a),164.506.
20. HHS, Security Rule, https://www.hhs.gov/hipaa/for-professionals/security/index.html
21. DHCS, CalAIM Data Sharing Authorization (Oct. 2023), https://www.dhcs.ca.gov/CalAIM/ECM/Documents/CalAIM-Data-Sharing-Authorization-Guidance.pdf
22. 45 C.F.R. §160.103.
23. ED, Who is a "school official" under FERPA? https://studentprivacy.ed.gov/faq/who-school-official-under-ferpa, accessed on July 6, 2024.
24. ED, Letter to University of New Mexico re: Applicability of FERPA to Health and Other State Reporting Requirements, Nov. 29, 2004, at 3, https://studentprivacy.ed.gov/resources/letter-university-new-mexico-re-applicability-ferpa-health-and-other-state-reporting, accessed July 8, 2024.
25. 34 CFR 99.31(a).
26. 45 C.F.R. § 160.103. These include legal, actuarial, transcription, accounting, consulting, management, accreditation, or financial services.
27. 45 C.F.R. §§ 164.502(a)(3)&(4), 164.504(e).
28. 45 C.F.R. § 164.504(e).
29. 45 C.F.R. § 160.103.
30. HHS, Transactions Overview, https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/Transactions/TransactionsOverview, accessed July 6, 2024.

References

31. "[E]ven though a school employs school nurses, physicians, psychologists, or other health care providers, the school is not generally a HIPAA covered entity because the providers do not engage in any of the covered transactions, such as billing a health plan electronically for their services. It is expected that most elementary and secondary schools fall into this category." Joint Guidance 2019, at 8.
32. 34 C.F.R. § 99.33.
33. Ca. Civ. Code § 56 et al.
34. Fact Sheet: SAMHSA 42 CFR Part 2 Revised Rule. Available at: https://www.hhs.gov/hipaa/for-professionals/regulatory-initiatives/fact-sheet-42-cfr-part-2-final-rule/index.html
35. ED, *Dear Colleague Letter to School Officials at Institutions of Higher Learning, August 2016,* https://studentprivacy.ed.gov/sites/default/files/resource_document/file/DCL_Medical%20Records_Final%20Signed_dated_9-2.pdf, accessed June 30, 2024.
36. 34 C.F.R. § 99.61.
37. 45 C.F.R. § 160.203(b).
38. DHCS, CalAIM Data Sharing Authorization (Oct. 2023), https://www.dhcs.ca.gov/CalAIM/ECM/Documents/CalAIM-Data-Sharing-Authorization-Guidance.pdf.
39. The most recent guidance can be found here: Joint Guidance on the Application of FERPA and HIPAA to Student Health Records (U.S. Department of Education)
40. ED, *Dear Colleague Letter to School Officials at Institutions of Higher Learning, August 2016,* https://studentprivacy.ed.gov/sites/default/files/resource_document/file/DCL_Medical%20Records_Final%20Signed_dated_9-2.pdf, accessed June 30, 2024.
41. National Center for Youth Law (2018), https://youthlaw.org/sites/default/files/attachments/2022-04/2018.10.23-HIPAAorFERPA-California.pdf

References

42. 34 C.F.R. § 99.30
43. 45 CFR § 164.508
44. 34 C.F.R. § 99.31
45. 45 C.F.R. § 164.506
46. Civ. Code § 56.10(c)(1))
47. 34 C.F.R. § 99.30
48. 34 C.F.R. § 99.36
49. DHCS. (2021) *Notice of privacy practices*. Retrieved from https://www.dhcs.ca.gov/formsandpubs/laws/priv/Pages/NoticeofPrivacyPractices.aspx
50. An integrated, comprehensive framework that focuses on CCSS, core instruction, differentiated learning, student-centered learning, individualized student needs, and the alignment of systems necessary for all students' academic, behavioral, and social success (from CA Department of Education).
51. DHCS, https://www.dhcs.ca.gov/provgovpart/Documents/ACLSS/LEABOP/Eligibility_Verification/DUA_REV_FY_15_18.pdf
52. See here for current list of eligible staff roles: https://www.dhcs.ca.gov/CYBHI/Documents/Fee-Schedule-Scope-of-Services-Rates-and-Codes.pdf
53. https://www.dhcs.ca.gov/CYBHI/Documents/EXAMPLE-CYBHI-Fee-Schedule-Provider-Participation-Agreement.pdf (Sample only)
54. https://www.carelonbehavioralhealth.com/content/dam/digital/carelon/cbh-assets/documents/ca/ca-tpa/data-use-agreement-two-party.pdf
55. Additional Resources | California School-Based Health Alliance.
56. 34 C.F.R. § 99.30(b)
57. DHCS, CalAIM ASCMI Pilot. https://www.dhcs.ca.gov/CalAIM/Pages/ASCMI-CalAIM.aspx
58. See Appendix A, Guiding Principles

References

59. Joint Guidance 2008. See HHS, *Does the HIPAA Privacy Rule apply to an elementary or secondary school?*, https://www.hhs.gov/hipaa/for-professionals/faq/513/does-hipaa-apply-to-an-elementary-school/index.html, accessed July 11, 2024.
60. CA DHCS. Privacy laws. Retrieved from https://www.dhcs.ca.gov/formsandpubs/laws/priv/Pages/default.aspx
61. Office of Civil Rights, HHS. How do HIPAA authorizations apply to an electronic health information exchange environment?
62. California's Uniform Electronic Transactions Act (UETA), Civ. Code, § 1633.7.


CalHHS
California Health & Human Services Agency