CalAIM Data Sharing Authorization Guidance

March 2022

Table of Contents

1. Guidance Background and Overview

(1) CalAIM Background

In 2022, the California Department of Health Care Services (DHCS) launched California Advancing and Innovating Medi-Cal (CalAIM) to transform and strengthen Medi-Cal; offering Californians a more equitable, coordinated, and person-centered to help people maximize their health and life trajectory. CalAIM will integrate Medi-Cal Enrollees' care coordination and case management across physical health, behavioral health, and social service providers. This model focuses on the need for integrated care for Enrollees at various stages of risk and needs, while also providing care to Enrollees with the highest risk through Enhanced Care Management (ECM) and Community Supports. CalAIM builds upon the county-based Whole Person Care (WPC) pilots and plan-based Health Home Program (HHP) that use whole-person care approaches to address underlying social drivers of health (SDOH). CalAIM envisions enhanced coordination, integration, and information exchange among managed care plans (MCPs); physical, behavioral, community-based, and social service providers; and county agencies.

(2) Guidance Overview

CalAIM requires the exchange of information about Medi-Cal Enrollees, including an array of administrative, clinical, social, and human service information across sectors. This exchange must occur in compliance with federal and state privacy laws, regulations, and other data sharing rules.

This document is intended to provide guidance that supports data sharing between MCPs, health care providers, community-based social and human service providers, local health jurisdictions, and county and other public agencies that provide services and manage care under CalAIM (collectively referred to as "CalAIM Participants").[1] This

[1] This guidance document reflects the provisions of AB 133, which revised state laws regarding disclosures among different organizations seeking to coordinate the care and provide services to Medi-Cal Enrollees under CalAIM and required DHCS to issue guidance related to the law. While disclosures to individual Medi-Cal Enrollees are not the focus of this document, CalAIM Participants should remember that sharing information with Medi-Cal Enrollees can be a critical element of quality care, and nothing in this document limits existing legal obligations to keep Medi-Cal Enrollees informed and share information with Enrollees.

document also includes a description of processes and scenarios that illustrate how data may be shared to support the provision of ECM and Community Supports services.

ECM and Community Supports are interdisciplinary approaches to care that address whole person needs for Medi-Cal Managed Care Enrollees through systematic coordination of services and comprehensive care management that is community-based, high-touch, and person-centered. There are important legal protections regarding the sharing of personal information and the purpose of the guidance is to support data exchange partners in navigating this complex environment with the objective of creating a robust culture of data sharing to coordinate person-centered care. This advisory document does not impose any new obligations on CalAIM Participants; instead, it is intended to help CalAIM Participants better understand existing obligations related to data sharing. DHCS may issue future guidance which may impose obligations on CalAIM Participants and other organizations subject to the information sharing provisions of AB 133.

The next sections of this guidance address recent state legislation that fosters the disclosure of information under CalAIM and DHCS' interpretation of such legislation. The final section provides Data Sharing Use Cases, or scenario-based guidance describing how various data types (e.g., housing, justice) may be shared by stakeholders in support of CalAIM goals. Data Sharing Use Cases are presented to help support stakeholder understanding of data sharing requirements.

DHCS is also providing a repository of sample data sharing forms and agreements[1] that have been used by WPC and HHP stakeholders, such as counties and health plans, for the exchange of various forms of personally identifiable information (PII) to improve the coordination of care.

While this guidance document focuses on data sharing under CalAIM, a portion of this guidance also addresses new changes to the California Penal Code that address disclosures intended to ensure that prison, jail and youth correctional inmates have access to behavioral health treatment in the community post-release, disclosures which may or may not occur under CalAIM. ***DHCS emphasizes that the guidance contained in this document is not intended to be and should not be construed as legal advice.***

(3) Privacy Law Overview

Many federal and state privacy laws may apply to the disclosure of information under CalAIM. At the federal level, the primary health privacy law is the privacy rule adopted

under the Health Insurance Portability and Accountability Act (HIPAA).[2] HIPAA applies to protected health information (PHI), which typically means individually identifiable health information that is created or received by a "covered entity" such as a health care provider or a health plan. HIPAA permits the disclosure of PHI for treatment or care coordination purposes in many circumstances. In some cases, HIPAA prohibits PHI from being shared unless the patient who is the subject of that PHI signs a form that authorizes such disclosure. In addition, the federal substance use disorder (SUD) confidentiality regulation, 42 C.F.R. Part 2, applies to some, but not all, categories of SUD information. When it applies, 42 C.F.R. Part 2 is often stricter than HIPAA, in part because the regulation does not permit disclosures of information for treatment or care coordination purposes without patient consent.

Federal law is a privacy floor; HIPAA and 42 C.F.R. Part 2 always need to be followed if they are applicable. California, like most other states, has enacted health privacy laws that exceed HIPAA standards in some cases. The California Confidentiality of Medical Information Act (CMIA) is similar in many ways to HIPAA. The CMIA, however, imposes some requirements that go beyond HIPAA, such as additional restrictions related to authorization forms. California also has an SUD confidentiality law, Health and Safety Code Section 11845.5, which mirrors 42 C.F.R. Part 2 in many respects but applies to a broader class of providers. Other California health privacy laws include Welfare and Institutions Code Section 5328, which restricts the disclosure of information held by some health care providers that provide services to those with mental health or developmental needs.

In addition to laws that restrict the disclosure of information, other laws mandate the disclosure of information. The federal interoperability rule requires health plans and hospitals to share information in certain circumstances, and the federal information blocking rule prohibits health care providers from engaging in "information blocking," which is the unreasonable withholding of certain categories of health information.

2. Data Sharing Provisions in AB 133

The successful implementation of CalAIM depends on the sharing of information about Medi-Cal Enrollees between various organizations and individuals responsible for improving the quality of care. Organizations and individuals who may share information on Medi-Cal Enrollees under CalAIM will include MCPs, health care providers, home

[1] Repository of Data Sharing Forms and Agreements, DHCS.
[2] Health Insurance Portability & Accountability Act, DHCS.

and community-based service (HCBS) providers, community-based social and human service providers, county and other public agencies, providers of both ECM and Community Supports, patients, families, and caregivers, among others. A common understanding of when disclosure of information about Medi-Cal Enrollees is permissible – and when privacy laws and principles would prohibit or limit such disclosures – is critical to CalAIM and the health of Medi-Cal Enrollees who will receive care under the program.

Recognizing the importance of information sharing, the California State Legislature included provisions related to information disclosures necessary to implement applicable CalAIM initiatives authorized in the health omnibus trailer bill legislation for the 2021-2022 California Budget (AB 133; Chapter 143 of Statutes of 2021), which was signed into law by Governor Gavin Newsom on July 27, 2021. AB 133 added Section 14184.102 to the Welfare and Institutions Code, including the following language at subdivision (j) related to information sharing to implement CalAIM:

> *"(j) Notwithstanding any other state or local law, including, but not limited to, Section 5328 of this code and Sections 11812 and 11845.5 of the Health and Safety Code, the sharing of health, social services, housing, and criminal justice information, records, and other data with and among the department [of health care services], other state departments, including the State Department of Public Health and the State Department of Social Services, Medi-Cal managed care plans, Medi-Cal Behavioral Health Delivery Systems, counties, health care providers, social services organizations, care coordination and case management teams, and other authorized provider or plan entities, and contractors of all of those entities, shall be permitted to the extent necessary to implement applicable*
>
> *CalAIM components described in this article and the CalAIM Terms and Conditions, and to the extent consistent with federal law. The department [of health care services] shall issue guidance identifying permissible data sharing arrangements to implement CalAIM."*

AB 133 also revised Section 4011.11 of the Penal Code to add subdivision (h). Paragraphs (4) and (5) of subdivision (h) reads as follows:

> *"(4) (A) The department shall develop the data elements required to implement this section, in consultation with interested stakeholders that include representatives of counties, county sheriffs, county probation agencies, and whole*

person care pilot lead entities with experience working with incarcerated individuals.

"(B) Notwithstanding any other law, the department, counties, county sheriffs, and county probation agencies shall share the information and data necessary to facilitate the enrollment of inmates in health insurance affordability programs on or before their date of release and to appropriately suspend and unsuspend Medi-Cal coverage for beneficiaries.

"(5) (A) No sooner than January 1, 2023, the State Department of Health Care Services, in consultation with counties, Medi-Cal managed care plans, and Medi-Cal Behavioral Health Delivery Systems, shall develop and implement a mandatory process by which county jails and county juvenile facilities coordinate with Medi-Cal managed care plans and Medi-Cal Behavioral Health Delivery Systems to facilitate continued behavioral health treatment in the community for county jail inmates and juvenile inmates that were receiving behavioral health services prior to their release.

"(B) Notwithstanding any other law, including, but not limited to, Sections 11812 and 11845.5 of the Health and Safety Code and Section 5328 of the Welfare and Institutions Code, the sharing of health information, records, and other data with and among counties, Medi-Cal managed care plans, Medi-Cal Behavioral Health Delivery Systems, and other authorized providers or plan entities shall be permitted to the extent necessary to implement this paragraph. The department shall issue guidance identifying permissible data sharing arrangements.

"(C) For purposes of this paragraph, the following definitions shall apply:

- *(i) "Medi-Cal Behavioral Health Delivery System" shall have the same meaning as set forth in subdivision (i) of Section 14184.101 of the Welfare and Institutions Code.*
- *(ii) "Medi-Cal managed care plan" shall have the same meaning as set forth in subdivision (j) of Section 14184.101 of the Welfare and Institutions Code."*

This document is being issued for the purpose of initially fulfilling DHCS's obligations under the AB 133 to issue guidance identifying permissible data sharing arrangements, both under CalAIM and for the coordination of inmates' post-release behavioral health care.

3. Supplemental Guidance

(1) Guidance of Welfare and Institutions Code Section 14184.102(j)

Welfare and Institutions Code Section 14184.102(j) permits CalAIM Participants to disclose personally identifiable information – including protected health information – among one another so long as such disclosure is: (1) necessary to implement CalAIM components or the CalAIM terms and conditions; and (2) consistent with federal law. This means that other provisions of state law that restrict the disclosure of such information are not applicable so long as Participants disclose information for purposes or providing services under CalAIM and abide by federal law. This waiver of state law applies not only to the provisions explicitly named in Section 14184.102(j) – that is, Sections 11812 and 11845.5 of the Health and Safety Code and Section 5328 of the Welfare and Institutions Code (the Lanterman-Petris-Short Act's privacy provision) – but any other state and local laws that may otherwise restrict the disclosure of information if they were applied to CalAIM, to the extent consistent and permissible under federal law. Such laws include, but are not limited to, Civil Code Section 56 et seq. (the Confidentiality of Medical Information Act), Health and Safety Code Section 120985 (regarding HIV test results), Welfare and Institutions Code 10850 (governing public social service records), and state and local laws that may prevent the disclosure of inmates' release dates and other inmate information relevant to providing services under CalAIM. However, this limited waiver of state law should not be interpreted as applying to other state laws that protect the rights of Medi-Cal Enrollees. For example, anti-discrimination laws remain fully in effect, as do laws that provide Medi-Cal Enrollees with rights regarding how they may access their own information and request confidentiality of such information.

CalAIM Participants include not only the types of persons specifically set forth in Section 14184.102(j), but any CalAIM Participant sharing data under CalAIM. In addition, 14184.102(j) permits disclosures to "contractors" of CalAIM Participants. These include, but are not limited to, business associates that facilitate the exchange of PII. Therefore, CalAIM Participants may exchange PII through health information exchanges, community information exchanges, and other entities that permit the sharing of PII in accordance with federal law.[3]

[3] If a community information exchange or other intermediary provides Medi-Cal reimbursable services, such organization may also be a CalAIM Participant.

We note that even if other state and local laws are made inapplicable by virtue of Section 14184.102(j), CalAIM Participants remain fully responsible for complying with federal privacy laws, and many such laws may apply to disclosures that occur under CalAIM. Such laws may include, but are not necessarily limited to, the privacy and security rules under HIPAA, the federal substance use disorder regulations at 42 C.F.R. Part 2, CMS statutes, regulations and guidance limiting the disclosure of Medicaid records for purposes directly related to Medicaid administration, and United States Department of Agriculture statutes, regulations, and guidance limiting disclosures under the Supplemental Nutrition Assistance Program (SNAP, known in California as CalFresh); the Special Supplemental Nutrition Program for Women, Infants, and Children (WIC) program; and other programs. When information may be shared under HIPAA and other federal law or policies, entities often are permitted to share only the minimum information necessary to accomplish the purpose of the disclosure. However, HIPAA's minimum necessary standard does not apply in cases where the disclosure is made to a health care provider for treatment purposes or where the disclosure occurs pursuant to a HIPAA-compliant authorization, among other exceptions to such standard.

Importantly, federal requirements related to the use and disclosure of Medi-Cal data– and DHCS guidance interpreting those federal requirements – remain in effect.[4] This means that counties remain responsible for entering into written agreements with their contractors that have access to Medi-Cal PII in accordance with DHCS guidance.[5] Similarly, MCPs must abide by the applicable terms of their contracts with DHCS relating to ensuring their contractors and vendors properly safeguard Medi-Cal data.

(2) Guidance of Penal Code Section 4011.11(h)(4)(B) and (5)

AB 133 amended Penal Code Section 4011.11 to add subdivision (h) to promote the provision of services to those exiting jails and youth correctional facilities. Paragraphs (1) through (4) of subdivision (h) requires that county jail and youth correctional facility inmates are provided assistance in enrolling in health insurance affordability programs, such as Medi-Cal. Paragraph (5) of subdivision (h) is intended to ensure that jail inmates and youth correctional inmates have access to behavioral health treatment in the community post-release.

Penal Code Section 4011.11(h)(4)(B) applies to data sharing that occurs for purposes of health insurance affordability program enrollment, and Penal Code Section

[4] Social Security Act Section 1902(a)(7); 42 C.F.R. Section 431.300 et seq.; All County Welfare Directors Letter (ACWDL) #19-16.
[5] All County Welfare Directors Letter (ACWDL) #19-16.

4011.11(h)(5)(B) applies to data sharing that occurs for the provision of behavioral health services post-release. That is, a limited waiver of state law is permitted for purposes of both assisting jail and youth correctional inmates with applying for health insurance affordability programs (which may include applying for those programs while incarcerated or after release) and ensuring those inmates have access to behavioral health services post-release. The two goals are interconnected, since obtaining health insurance is often critical to obtaining continued access to behavioral health services.

Under Penal Code Section 4011.11(h)(4)(B), a disclosure of personally identifiable information is permitted if the disclosure: (1) is reasonably necessary to facilitate a county jail or youth correctional inmate's enrollment in a health insurance affordability program; (2) occurs between various county agencies (inclusive of county jails, youth correctional facilities, county health departments, and county law enforcement agencies), or between a county agency and DHCS; and (3) complies with federal law. Similarly, under Penal Code Section 4011.11(h)(5)(B), a disclosure of personally identifiable information is permitted if the disclosure: (1) is reasonably necessary to facilitate a county jail or youth correctional inmate's behavioral health treatment post-release; (2) occurs between various county agencies (inclusive of county jails and youth correctional facilities, county health departments and county law enforcement agencies), DHCS, Medi-Cal managed care plans, Medi-Cal behavioral health delivery systems, health care providers, or other persons involved behavioral health treatment; and (3) complies with federal law. Under both provisions, disclosures may be made while the individual is incarcerated, or they may be made post-release. Personally identifiable information disclosed may consist of "health information," but it may also include other data intended to serve the purposes of these disclosures.[6] Organizations have the discretion to determine the appropriate means of exchange, which, as with the case of disclosures under CalAIM, may include the exchange of information through contractors such as health information exchanges or community information exchanges.

Penal Code Section 4011.11(h)(4)(B) and (5) apply to county jails and county youth correctional facilities. The law does not apply directly to state prisons. Nevertheless, individuals exiting state prisons often need to enroll in health insurance affordability programs and receive behavioral health services post-release. The Department is working to coordinate with applicable agencies on the exchange of information to improve the care provided to former inmates of state prisons.

[6] Data that may be shared under the conditions of Penal Code Section 4011.11(h)(4)(B) may include the inmate's incarceration date, release data, and identifying demographic information.

As is the case with Welfare and Institutions Code Section 14184.102(j), Penal Code Section 4011.11(h)(4)(B) and (5)(B) have no impact on federal law requirements. Organizations disclosing information under subdivision (h) remain fully responsible for complying with applicable federal privacy laws. Similarly, Penal Code Section 4011.11(h)(4)(B) and (5)(B) have no impact on other state laws that protect individual rights, such as anti-discrimination laws. However, unlike Welfare and Institutions Code Section 14184.102(j), disclosures that occur under Penal Code Section 4011.11(h)(4)(B) and (5)(B) are not limited to those that occur under CalAIM.

(3) Policies and Procedures That Conflict with Necessary Data Sharing

Penal Code Section 4011.11(h)(4)(B) states that DHCS, counties, county sheriffs, and county probation agencies shall share information necessary to facilitate enrollment of inmates in health insurance affordability programs on or before their date of release and to appropriately suspend and unsuspend Medi-Cal Coverage. Similarly, Penal Code Section 4011.11(h)(5)(A) states that the facilitation of continued behavioral health treatment is a "mandatory process." Therefore, the exchange of information is required if such disclosure is necessary to facilitate enrollment in health insurance affordability programs, or continued behavioral health treatment post-release occurs between persons described in the applicable statutory provision, and complies with federal law. Counties – including county health agencies, county law enforcement agencies, county probation departments, and jails and youth correctional facilities operated by Counties – as well as Medi-Cal managed care plans, Medi-Cal behavioral health delivery systems, health care providers, and other persons or organizations involved in health insurance affordability enrollment and/or behavioral health treatment may not withhold information based on their own policies, procedures, or preferences if those are more restrictive than the requirements under Penal Code Section 4011.11(h)(4) or (5) or federal law. Organizations therefore may need to review their own policies and procedures to ensure they are not unnecessarily restrictive. Nevertheless, organizations may withhold information if the individual who is the subject of that information requests that their information not be shared or if applicable federal law requires such individual's authorization and the individual has not provided it.[7]

[7] MCPs subject to AB 1184 shall abide by requirements related to "confidential communication requests" under that law. We note that "confidential communications requests" involve communications between a plan and an enrollee, not communications between two organizations coordinating the care of an enrollee of such plan.

No statute specifically mandates the disclosure of personally identifiable information under CalAIM. However, the sharing of information among CalAIM Participants,

consistent with state and federal law, is necessary for the successful implementation of CalAIM. Therefore, we encourage CalAIM Participants to examine their policies and procedures, as well as any other data sharing practices and standard contractual terms, to ensure that they are not unnecessarily restrictive. While we expect CalAIM Participants to maintain safeguards to reasonably protect the privacy and security of PII, certain practices may thwart the goals of CalAIM if they are not dictated by applicable law or best practices. We note that CalAIM Participants that meet the definition of a "health care provider" under 42 U.S.C. Section 300jj are subject to the federal information blocking rule, which took effect on April 5, 2021, and the refusal to disclose electronic health information in response to the request of another CalAIM Participant could conflict with the information blocking rule in cases where such refusal is not based on legal requirements or does not otherwise fit within an information blocking exception.[8]

(4) Use of Electronic Signatures

Because federal requirements remain applicable to disclosures under both Welfare and Institutions Code Section 14184.102(j) and Penal Code Section 4011.11(h)(4)(B) and (5)(B), there may be circumstances under which an individual's authorization is required for the disclosure of information under the CalAIM or for purposes of connecting an individual with health insurance or mental health services following release from jail. In such a case, Welfare and Institutions Code Section 14184.102(j) and Penal Code Section 4011.11(h)(4)(B) and (5)(B) allow CalAIM Participants and others who are

[8] In general, information blocking is a practice by a health IT developer of certified health IT, health information network, health information exchange, or health care provider (collectively referred to as "actors") that, except as required by law or specified by the Secretary of Health and Human Services as a reasonable and necessary activity, is likely to interfere with access, exchange, or use of electronic health information (EHI). The federal information blocking rule describes categories with specific conditions that must be met for an actor to fit within an information blocking exception. In addition to meeting the definition of a "health care provider," it is also possible that some CalAIM participants could fall within the definition of a health information network/health information exchange or health IT developer. Legal counsel should review considerations related to information blocking.

acting under the scope of those laws to use electronic signatures on authorization forms, assuming such signature otherwise complies with federal law..

Both federal and California law allow the use of electronic signatures that meet certain standards. HIPAA permits the use of electronic signatures so long as their use complies

with otherwise applicable law such as the Electronic Signatures in Global and National Commerce (E-Sign) Act,[9] and California's Uniform Electronic Transactions Act (UETA) permits the use of electronic signatures in many circumstances. *See* Civil Code Section 1633.7. Historically, there has been an important exception to the permissibility of electronic signatures: if an authorization is required under the CMIA, then the UETA's presumption that electronic signatures are valid has not applied. Civil Code Section 1633.3(c). However, the new provisions in AB 133 change this framework. If a disclosure occurs in compliance with Welfare and Institutions Code Section 14184.102(j) or Penal Code Section 4011.11(h)(4)(B) or (5)(B), then other state laws such as the CMIA no longer limit such disclosure. Since the CMIA's authorization form requirements are no longer applicable, the CMIA exception to California's UETA is no longer applicable either. Therefore CalAIM Participants may recognize authorization forms executed by electronic signatures, so long as participants follow federal and UETA requirements governing the use of electronic signatures.[10] Under those laws, oral recordings may meet federal requirements for electronic signatures in some circumstances, but unrecorded verbal statements do not qualify as electronic signatures.[11]

(5) Applicability of 42 C.F.R. Part 2

Because CalAIM Participants will be providing services to Enrollees with SUDs, 42 C.F.R. Part 2 will apply to some of the information exchanged under CalAIM. 42 C.F.R. Part 2 often requires consent for disclosure of information in circumstances where

---

[9] How do HIPAA authorizations apply to an electronic health information exchange environment?, United States Department of Health and Human Services Office of Civil Rights.
[10] Recognition of electronic signatures is also consistent with AB 2520 which, enacted in 2020, permits health care providers to honor requests for disclosure of records based on electronic signatures.
[11] This guidance addresses the applicability of electronic signatures to authorizations that permit the disclosure of PII. Nothing in this guidance changes prior guidance related to the use of electronic signatures for Medi-Cal applications or renewals. See ACWDL 19-17 and MEDIL 21-38.

HIPAA does not; therefore, CalAIM Participants will need to assess what information is subject to 42 C.F.R. Part 2. DHCS cannot provide legal advice as to which particular data sets are subject to 42 C.F.R. Part 2 and which are not. However, below we highlight key aspects of 42 C.F.R. Part 2 and guidance from the Substance Abuse and Mental Health Services Administration (SAMHSA), the federal agency which has implemented that regulation.

42 C.F.R. Part 2 does not apply to all SUD information. The regulation only applies to information that has been obtained by a Part 2 provider, sometimes called a "Part 2 program," and which would identify an individual as having or having had an SUD.[12] A Part 2 provider is a federally assisted program "who holds itself out as providing, and provides, substance use disorder diagnosis, treatment, or referral for treatment."[13] SAMHSA has explained that a provider may "hold itself out" as providing SUD services if it, among other activities, obtains a state license specifically to provide SUD services, advertises SUD services, has a certification in addiction medicine, or post statements on its website about SUD services provided.[14]

In guidance, SAMHSA has said the following providers, among others, meet the definition of a Part 2 provider:

- A SAMHSA-certified Opioid Treatment Program that advertises its SUD services.
- A physician at a community mental health center who is identified as the center's leading SUD practitioner and who primarily treats patients with SUDs.

In contrast, SAMHSA has said the following providers are not subject to 42 C.F.R. Part 2:

- A psychiatrist who provides mental health services to patients with SUDs.
- A physician who treats a diverse group of patients and occasionally provides medication assisted treatment with buprenorphine to treat opioid dependency.

---

[12] 42 C.F.R. Section 2.12(a)(1).
[13] The regulation also applies to "(2) An identified unit within a general medical facility that holds itself out as providing, and provides, substance use disorder diagnosis, treatment, or referral for treatment; or (3) Medical personnel or other staff in a general medical facility whose primary function is the provision of substance use disorder diagnosis, treatment, or referral for treatment and who are identified as such providers." 42 C.F.R. Section 2.11.
[14] Applying the Substance Abuse Confidentiality Regulations, SAMHSA

- "[E]mergency room personnel who refer a patient to the intensive care unit for an apparent overdose, unless the primary function of such personnel is the provision of substance use disorder diagnosis, treatment, or referral for treatment and they are identified as providing such services or the emergency room has promoted itself to the community as a provider of such services."[15]

While CalAIM Participants are likely to be "federally assisted" by virtue of receiving Medi-Cal funds, many CalAIM Participants who obtain SUD information will not be subject to 42 C.F.R. Part 2 because they do not "hold themselves out" as providing SUD services as described above. SAMHSA has explained that if an organization is not subject to 42 C.F.R. Part 2, then information that such organization collects from a Screening, Brief Intervention and Referral to Treatment (SBIRT) is not subject to 42 C.F.R. Part 2, even if that information identifies individuals as having an SUD.[16] Therefore, member information files developed by MCPs that identify certain Medi-Cal Enrollees as having an SUD may not be subject to 42 C.F.R. Part 2 if the lists are based on screenings, assessments or other data sources that were generated by organizations that are not subject to 42 C.F.R. Part 2. In contrast, if an Enrollee's SUD status on a member information file is based on information provided by a Part 2 provider – which could occur, for example, if the information came from a claim or medical record provided by an opioid treatment program – then such entry on the file would be subject to 42 C.F.R. Part 2.

In addition, 42 C.F.R. Part 2 does apply to recipients of SUD information from Part 2 providers in some circumstances. However, the regulation's restrictions on disclosures typically apply to recipients of SUD information only if the disclosing party has notified the recipient that the information is subject to 42 C.F.R. Part 2, *except* in cases where the recipient is a third-party payer.[17] CalAIM Participants should discuss with their legal counsel as to when it is appropriate to conclude that SUD information received from another source is not subject to 42 C.F.R. Part 2.

In cases where an organization determines that the SUD information it has received from another source is subject to 42 C.F.R. Part 2, that organization may still be able to use and disclose such information in certain circumstances. 42 C.F.R. Section 2.33 permits organizations that receive records subject to 42 C.F.R. Part 2 in accordance

---

[15] Disclosure of Substance Use Disorder Patient Records, Does Part 2 Apply to Me?, SAMHSA; 42 C.F.R. Section 2.12(e)(1).
[16] Applying the Substance Abuse Confidentiality Regulations, SAMHSA.
[17] 42 C.F.R. Section 2.12(d)(2)(i).

with an individual's consent (described as "lawful holders") to redisclose such information to their contractors for payment or health care operations purposes, so long as they follow certain safeguards such as contractually requiring the contractor to abide by 42 C.F.R. Part 2. For example, the regulation permits such lawful holders to disclose information subject to 42 C.F.R. Part 2 to contractors assisting with care coordination and care management.

(6) Additional Information and Resources on Authorization Form Requirements

DHCS is in the process of developing a model data sharing authorization form and intends to make it available in mid-2022. The form will be designed to comply with applicable legal requirements, including the necessary elements under HIPAA and 42 C.F.R. Part 2. DHCS intends that the form be a resource to CalAIM Participants and does not intend at this time to mandate its use.

In addition, CalAIM participants may use their own authorization forms that comply with applicable law. Authorization forms may be administered by MCPs, providers, or other CalAIM Participants, who will be responsible for ensuring that the authorization forms comply with applicable law. If a disclosure of PII is being made consistent with CalAIM guidance on data sharing that DHCS issues, then the authorization should be permissible under state law pursuant to Welfare and Institutions Code Section 14184.102(j), but the form will still need to comply with federal standards regarding what must be included in an authorization form. Similarly, if a disclosure of PII is reasonably necessary to facilitate a county jail or youth correctional inmate's enrollment in a health insurance affordability program or to facilitate post-release behavioral health treatment, and such disclosure occurs between the organizations described in Penal Code Section 4011.11(h)(4) or (5), as applicable, then it is consistent with state law pursuant to Penal Code Section 4011.11(h)(4)(B) or (5)(B), as applicable, and any further authorization form requirements are dictated by federal legal requirements. The following resources may assist organizations in meeting authorization form requirements under applicable law.

1. The California Office of Health Information Integrity (CalOHII) issued several volumes of State Health Information Guidance (SHIG)[18] that provide important information about authorization form requirements under applicable law. The discussion of authorization form legal requirements appears in Appendix 2 of these documents.

[18] State Health Information Guidance (SHIG), State of California Office of Health Information.

2. Organizations often need to obtain a signed authorization form from the Enrollee (or, in some cases, the Enrollee's Personal Representative) because the requirements under 42 C.F.R. Part 2 require such a form. In addition to the authorization form requirements that appear in the regulation itself (42 C.F.R. Section 2.31), SAMHSA has issued guidance on Part 2 authorization form requirements in a document titled: "Applying the Substance Abuse Confidentiality Regulations to Health Information Exchange."[19] Section 3221 of the Coronavirus Aid, Relief, and Economic Security Act (CARES Act) modified the statute that is the basis for 42 C.F.R. Part 2 that may impact the requirements of a Part 2 authorization form, although SAMHSA has not yet issued proposed amendments to the Part 2 regulations to implement Section 3221.

3. HIPAA and 42 C.F.R. Part 2 require certain components in authorization forms to be compliant. For example, specifics regarding the data being shared, the respective parties to the sharing, the potential uses of the data, and an expiration and right to revocation are required. There are certain common misconceptions about authorization form requirements, such as specific time limits for an expiration of an authorization, so all components should be reviewed by legal counsel. We note that both HIPAA and 42 C.F.R. Part 2 provide some flexibility as to who may obtain consent; that is, the organization that discloses the PII does not need to have obtained consent directly from the Enrollee but may rely on a valid authorization form provided by another party. Best practices also include soliciting consumer feedback and exhibiting cultural competency (i.e., appropriate language) and/or health literacy, as well as consumer engagement with potential electronic consent options (e.g., "I Agree" click button, oral recording etc.)

4. CalOHII supported an extensive stakeholder engagement process and in collaboration with DHCS, developed a draft Universal Authorization for Release of Information form. The intent of the form was to help create a single, standardize data exchange process and form in the state that could help enable patient consent management. While the form has not been publicly released, DHCS is considering whether and how a version of the form could be piloted across several initiatives, including CalAIM.

[19] FAQ: Applying the Substance Use Confidentiality Regulations to Health Information Exchange (HIE), SAMHSA.

4. Data Sharing Authorization Use Cases

(1) Use Cases Background

Under Section 14184.200(j), DHCS must issue guidance that identifies permissible data sharing arrangements in CalAIM. The following Use Case scenarios are intended to assist CalAIM Participants in understanding the circumstances under which PII, including PHI subject to HIPAA, may be disclosed under CalAIM. ***This guidance is not intended to be legal advice, and it should not be construed as legal advice. DHCS cannot provide an authoritative interpretation of federal privacy laws that are determinative of whether PII may be disclosed.*** CalAIM Participants should confer with their legal counsel to ensure that their information sharing practices comply with applicable law.

These use cases are examples of circumstances where information sharing may be permitted. CalAIM Participants may be able to exchange PII in situations that are not addressed by any of these use cases. CalAIM Participants should not interpret these use cases as being the only categories of permissible information sharing under CalAIM. A disclosure may comply with applicable law even if it does not fit within one of the following use cases.

The Use Cases only address laws that are applicable to the disclosure of PII. They do not address restrictions that may exist in policies or procedures or in contracts. For example, the United States Department of Housing and Urban Development (HUD) has said that data in a Homeless Management Information System[20] (HMIS) may be disclosed without an Enrollee's written consent for purposes of coordinating care in cases where the homeless organization makes clear in its privacy notice that it may do so, but many Continuums of Care in California that operate an HMIS have adopted policies that require written consent even when disclosures are made for care coordination purposes. Similarly, some health information exchanges in California may have adopted policies that limit disclosures of PHI even in circumstances where such disclosures are permitted by HIPAA.

CalAIM Participants are responsible for understanding what requirements may exist outside law and regulation, and when they should be followed. As noted in the Data Sharing Provisions in the AB 133 section above, there may be circumstances under which following a policy that is unnecessarily restrictive may conflict with other

[20] Homeless Management Information System, HUD Exchange.

obligations imposed on CalAIM Participants, such as the need to comply with the information blocking rule.

In addition, CalAIM Participants have the discretion to determine the means of exchange of PII. As noted above, AB 133 permits CalAIM Participants to disclose PII through contractors, so long as they do so in compliance with federal law and for purposes of implementing CalAIM. Such contractors may include health information exchanges, community information exchanges, and other intermediaries that facilitate the exchange of PII.

(2) Assumptions

Information in the Use Cases is subject to the following assumptions. If one or more of these assumptions are not true, CalAIM Participants may still be permitted to disclose PII in accordance with applicable law, but the analysis in the Use Cases would be inapplicable. Information in the use cases and their following analyses are subject to the following assumptions:

- The Medi-Cal Enrollees who are the subjects of the information exchange are adults age 18 or older. Any information about enrollment status, including Family Planning, Access, Care, and Treatment (PACT) enrollment, do not include disclosures about minors. Additional use cases related to minors will be forthcoming in separate guidance.
- If an Enrollee provides authorization for disclosure of the Enrollee's information, that Enrollee has the legal capacity to provide such consent. If another person (such as a friend or family Enrollee) provides authorization on behalf of that Enrollee, then that other person has the legal authority to provide such consent, that is, such a person is a Personal Representative of the Enrollee.
- Participants are disclosing PII in order to coordinate the care of Medi-Cal Enrollees in CalAIM or otherwise implement CalAIM components; therefore, the limited waiver of state law under Welfare and Institutions Code Section 14184.100(j) applies.
- If jail release dates or other criminal justice information is requested to be shared, then the requester does not have direct access to a criminal justice information system, meaning that the requester is unable to access a system containing detailed criminal histories of Enrollees.
- Any criminal justice information provided by jails may include release dates, incarceration dates, and limited demographic information such as name, date of birth, sex, and race, but does not consist of the full criminal history of an Enrollee or a criminal identification and information (CII) number.

- Providers sharing information under CalAIM are not subject to: (1) the Violence Against Women Act (VAWA) or similar federal laws limiting the disclosure of information related to domestic violence providers; or (2) the Family Educational Rights and Privacy Act (FERPA). VAWA and FERPA often require an individual's consent for disclosures, even in cases where such consent is not required under HIPAA.
- Psychotherapy notes, as defined under HIPAA, are not disclosed.[21]
- Any disclosures that occur are made in compliance with all applicable security requirements, including the requirements of the HIPAA security rule, if applicable.
- Any data sharing entities exchanging PII have undergone all legally required privacy and security training, including HIPAA training, if applicable.
- Housing providers may be subject to HMIS requirements because they use an HMIS to share or receive information, but no other housing data privacy laws are applicable.
- If protected health information is being disclosed, the CalAIM Participant abides by HIPAA's minimum necessary standard, when applicable.[22]
- Social Security numbers are not disclosed.
- Medically tailored meal providers may be subject to HIPAA – either because they are HIPAA covered entities or because they act as business associates of HIPAA covered entities – but they are not subject to United States Department of Agriculture data privacy rules because they do not accept funding from the USDA to provide such meals. If a medically tailored meal provider is acting as a business associate of a covered entity, its business associate agreement permits the business associate to disclose the PHI it holds for care coordination purposes.

[21] Under HIPAA, "psychotherapy notes" are "notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record." 45 C.F.R. Section 164.501.

[22] Under HIPAA, the minimum necessary standard means that "[w]hen using or disclosing protected health information or when requesting protected health information from another covered entity or business associate, a covered entity or business associate must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request." 45 C.F.R. Section 164.502(b). This standard does not always apply. For example, the standard does not apply if the information is being shared with a health care provider for treatment purposes.

(3) Definitions

The following definitions apply to the terms used in the Use Cases. These definitions are intended to assist with the use case analysis, but they may differ with how organizations use these terms in other contexts. For example, the definition of "community-based organization" excludes HIPAA covered entities to illustrate how HIPAA rules differ for non-covered entities.

- **Asthma remediation provider:** a provider that undertakes modifications to an Enrollee's home to mitigate environmental triggers that exacerbate asthma conditions.
- **Behavioral health (BH) provider (non-Part 2):** a health care provider that provides mental health or substance use disorder services, or services for Enrollees with developmental disabilities, that is not subject to 42 C.F.R Part 2. This may include providers that provide some SUD services but do not "hold themselves out" as providing such services, such as hospital emergency rooms and mental health counselors who may treat Enrollees with substance use disorders.
- **Community-based organization (CBO):** Non-Covered Entities that are based in the community (i.e., non-governmental), provide a range of social and human services, and are not health care providers. CBOs include asthma remediation providers, housing providers, and medically tailored meal providers that are neither health care providers nor covered entities.
- **Community Supports provider:** a provider of Community Supports, which may be a community-based organization or a health care provider.
- **Covered entity:** a health care provider, health plan, or health care clearinghouse that is subject to HIPAA.
- **Demographic information:** basic patient information such as name (including any previous name), date of birth, address, phone number, email address, race, ethnicity, sex, sexual orientation, gender identity and preferred language(s).
- **ECM provider:** a health care provider that is responsible for the coordination or management of an Enrollee's care under CalAIM.
- **Enrollee Transition List:** a file provided by DHCS to MCPs that contain WPC enrollment information for ECM and Community Supports Enrollee outreach.
- **General health care provider:** a health care provider that is not a behavioral health provider or a Part 2 provider.
- **General health information:** protected health information that is subject to HIPAA and the California Confidentiality of Medical Information Act but no other health care privacy laws.

- **Health care provider:** as defined under HIPAA, a person or organization that furnishes, bills, or is paid for health care in the normal course of business.
- **HIV information:** protected health information that identifies a person as having or not having HIV or AIDS, including HIV test results, but not including HIV information held by a state or local public health agency.
- **Housing provider:** an organization that records, uses or processes PII to help provide housing to individuals, including housing navigation and transition services.
- **Local agency**: a county, city, or tribal agency that operates a social service program and which is not a health care provider or a covered entity. Local agencies include agencies that administer the Special Supplemental Nutrition Program for Women, Infants, and Children (WIC).
- **Medically tailored meal provider:** a provider that provides medically tailored meals to Enrollees. Medically tailored meal providers may or may not be HIPAA covered entities.
- **Medi-Cal redetermination date:** the effective date of an Enrollee's last determination of eligibility for Medi-Cal.
- **Part 2 provider:** a health care provider that provides substance use disorder services and is subject to 42 C.F.R. Part 2. To be considered a Part 2 provider, providers must hold themselves out as providing, and provide, diagnosis, treatment, or referral for a treatment for an SUD. A provider "holds itself out" as providing SUD care if the provider engages in any activity that would lead another person to reasonably conclude that the individual or organization provides substance use disorder diagnosis, treatment, or referral for treatment.
- **Personal Representative**: an individual authorized to make medical decisions on behalf of an Enrollee. For example, a parent or guardian is considered the Personal Representative of a minor in many circumstances.
- **Provider:**[23] any individual or entity that is engaged in the delivery of services – or ordering or referring for those services – to Enrollees under the Medi-Cal program, and is licensed, certified, or contracted to do so. Providers include health care providers, community-based organizations, and county health systems.

[23] The definition of "provider" differs from similar terms defined under other laws and regulations. For example, it is not the same as the definition of "health care provider" under HIPAA.

(4) Use Cases

In each use case and associated data flow, whether the Enrollee has signed a data authorization form may impact the scope of data that may be shared. For purposes of this guidance, it is assumed that the authorization form complies with all applicable law. All authorization forms should be reviewed with legal counsel before implementing.

In the following diagrams, information marked in green may be able to be disclosed in compliance with applicable law. Information marked in red denotes a significant likelihood that disclosure would violate one or more laws. ***DHCS emphasizes that a definitive interpretation of applicable law cannot be made, and CalAIM Participants should rely on their attorneys to decide when PII can be disclosed***.

Table 1: Use Case List and Descriptions

Use Cases	Description	Data Flow
1. ECM Enrollee identification, review, and authorization for ECM and Community Supports	MCPs identify ECM populations by compiling and analyzing administrative, physical, behavioral, dental and social service data and information received from DHCS, counties, Providers, Enrollee, and others	• 1-1: DHCS sends claims/encounter data to MCPs • 1-2: Providers, CBOs, and jails/prisons send records with Enrollee information to MCP
2. ECM assignment and Enrollee engagement	MCPs assign Enrollees to an ECM Provider based on their previous provider relationships, health needs, and known preferences, and ECM Providers use available information to reach out to and engage with Enrollees qualifying for the ECM benefit.	• 2-1: MCP sends assignment files to ECM Providers • 2-2: ECM Provider reports Enrollee engagement activity back to MCP
3. Care coordination and referral management	Providers support care coordination and care transitions for engaged Enrollees, including supporting referrals across the MCP's community, county, social services and Community Supports Provider networks.	• 3-1: Provider sends referral and other information to medical, behavioral, or Community Supports Provider • 3-2: Medical, behavioral or Community Supports Provider informs

Use Cases	Description	Data Flow
		referring Provider of receipt of services
4. Billing and encounter reporting practices	Providers submit claims/invoices to MCPs for services rendered, and MCPs report complete and accurate encounters of all services provided to DHCS.	• 4-1: Provider sends claims to MCPs • 4-2: MCPs sends encounters to DHCS

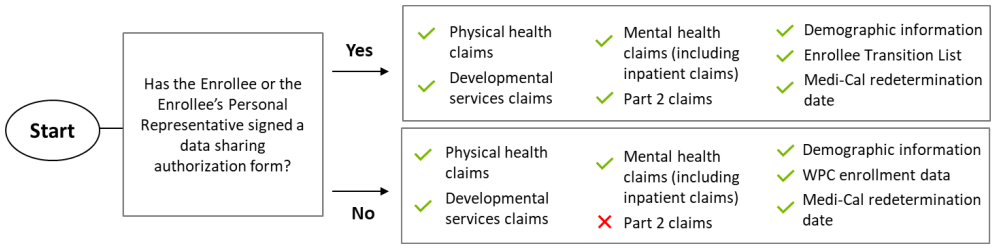
1. ECM Enrollee Identification, Review, and Authorization for ECM and Community Supports

MCPs are responsible for identifying high-cost, high-needs Enrollees eligible for the ECM benefit by compiling and analyzing information from Enrollees and their families, DHCS, counties, Providers, CBOs, jails/prisons and others. MCPs are expected to identify Enrollees for ECM through a combination of data sources, including enrollment and Medi-Cal encounter data they receive from DHCS and generate and manage themselves; other administrative, clinical, behavioral, dental, social service, and care needs; and assessment information they can securely access through partnerships with county agencies, health care providers, providers (e.g., housing, medically tailored meals), and health information organizations (HIOs). MCPs are also required to assess requests for the ECM benefit from providers, Enrollees, and Enrollee caretakers.

Use Case 1-1:

Data Exchange: Claims, encounter, and Enrollee Transition List data
Function: Enrollee identification for ECM and Community Supports services
Originating Entity: DHCS
Receiving Entity: MCP

Use Case 1-1 Visualization



Legal Rationale

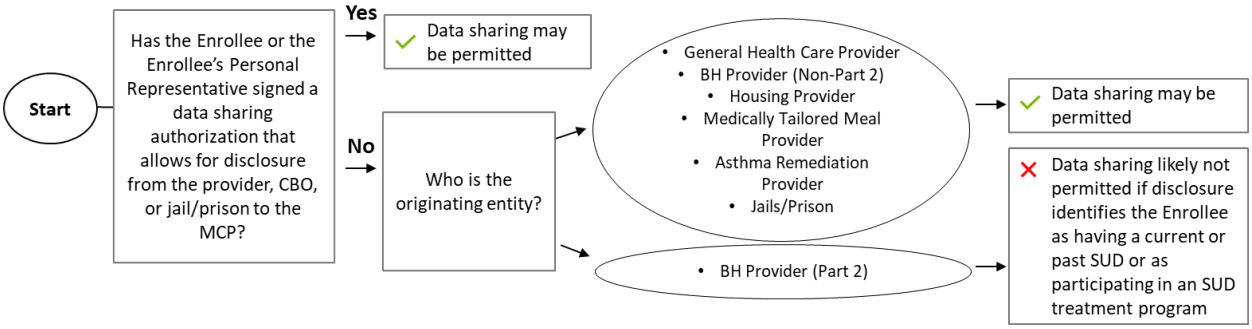
Physical health, mental health, and developmental services claims/encounters, as well as demographic information, Enrollee Transition Lists, and Medi-Cal redetermination dates, potentially may be shared in accordance with HIPAA since the disclosure is being made for a health care operations purpose – care management and care coordination – of the entity receiving the information; both DHCS and the MCP have a relationship with the Enrollees whose data is being disclosed; and the disclosure pertains to such relationships.

Further, the disclosure potentially may occur in accordance with Social Security Act Section 1902(a)(7) since the disclosure is being made for a Medi-Cal administration purpose. Part 2 records would need to be removed from claims/encounter data files originating from another MCP unless the Enrollee has signed an authorization form compliant with 42 C.F.R. Part 2.

Use Case 1-2:

Data Exchange: Records with Enrollee information
Function: Enrollee identification for ECM and Community Supports services
Originating Entity: Providers, CBOs, and jails/prisons[24]
Receiving Entity: MCP

Use Case 1-2 Dataflow



Legal Rationale

Records with Enrollee information potentially may be disclosed from an entity to an MCP if the entity is a:

- General health care provider or a behavioral health provider not subject to 42 C.F.R. Part 2 since, under HIPAA, the disclosure is being made in order to permit the MCP to engage in a health care operations purpose (care coordination), both the health care or behavioral health provider and MCP have a relationship with the Enrollees whose data is being disclosed, and the disclosure pertains to such a relationship;
- Medically tailored meal provider; if such provider is subject to HIPAA, then it may disclose its information in compliance with HIPAA for the reasons stated above;
- Housing provider as federal HMIS requirements permit disclosures without written consent for purposes of care coordination and the MCP is seeking information in order to better coordinate care; and
- Jail/prison (with regards housing location, incarceration date, release dates, and limited demographic information) since federal law does not prohibit disclosures of this information.

Behavioral health providers subject to 42 C.F.R. Part 2 may not disclose information to an MCP without authorization since there are no applicable Part 2 consent exceptions.

[24] Analysis assumes jails and prisons do not share criminal identification and information (CII) numbers.

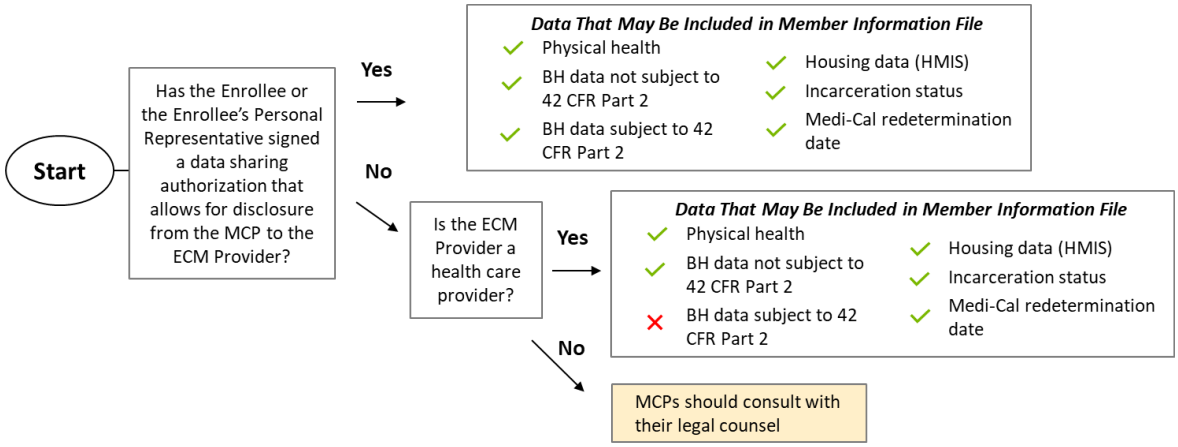
2. ECM Assignment and Enrollee Engagement

Once Enrollees are identified and authorized for the ECM benefit, MCPs identify the providers each Enrollee has engaged with and determine the most appropriate provider for ECM assignment based on that Enrollee's physical health, behavioral health, and social needs, including cultural and linguistic competency. After assignment is confirmed, MCPs are required to share Enrollee Assignment Files with ECM providers. ECM Providers then use available information to reach out to and engage with Enrollees qualifying for the ECM benefit.

Use Case 2-1:

Data Exchange: Enrollee Information File
Function: Enrollee engagement for ECM services
Originating Entity: MCP
Receiving Entity: ECM Provider

Use Case 2-1 Visualization



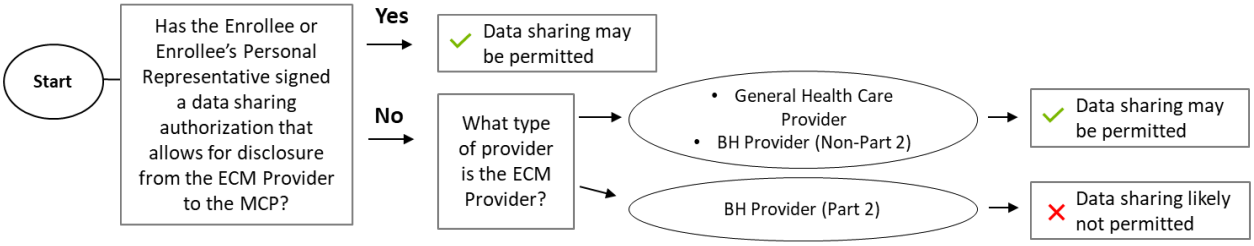
Legal Rationale

When the Enrollee has not signed an authorization that allows for disclosure from the MCP to the ECM Provider, data—including physical health and behavioral health information not subject to 42 C.F.R. Part 2, housing history, incarceration status, Medi-Cal redetermination dates, and demographic data—potentially may be disclosed from the MCP to the ECM Provider under HIPAA if the ECM provider is a health care provider, since the disclosure is being made for a treatment purpose to a health care provider. If the ECM Provider is not a health care provider under HIPAA and the Enrollee has not consented to disclosure, the treatment exception under HIPAA may not apply. HIPAA does permit a health plan to disclose PHI for care coordination purposes to organizations that are not HIPAA covered entities if those organizations act as a business associate of the health plan. MCPs, in consultation with their legal counsel, should consider whether it is appropriate to enter into business associate agreements with their ECM providers that are not covered entities.

Use Case 2-2:

Data Exchange: Enrollee engagement information such as contact information, outreach counts, and clinical characteristics such as diagnoses, screenings, or procedures
Function: Enrollee engagement for ECM services
Originating Entity: ECM Provider
Receiving Entity: MCP

Use Case 2-2 Visualization



Legal Rationale

When the Enrollee has not signed an authorization that allows for disclosure, ECM Providers that are general health care providers or behavioral health providers not subject to 42 C.F.R. Part 2 potentially may disclose Enrollee engagement information to their MCPs since covered entities may disclose PHI to health plans if both parties have a relationship with the Enrollee, the disclosure pertains to such relationship, and the MCP is seeking the data for a health care operations purpose (to coordinate care). ECM Providers that are behavioral health providers subject to 42 C.F.R. Part 2 may not disclose Enrollee engagement information since disclosure is not allowed for health care operations purposes without consent.

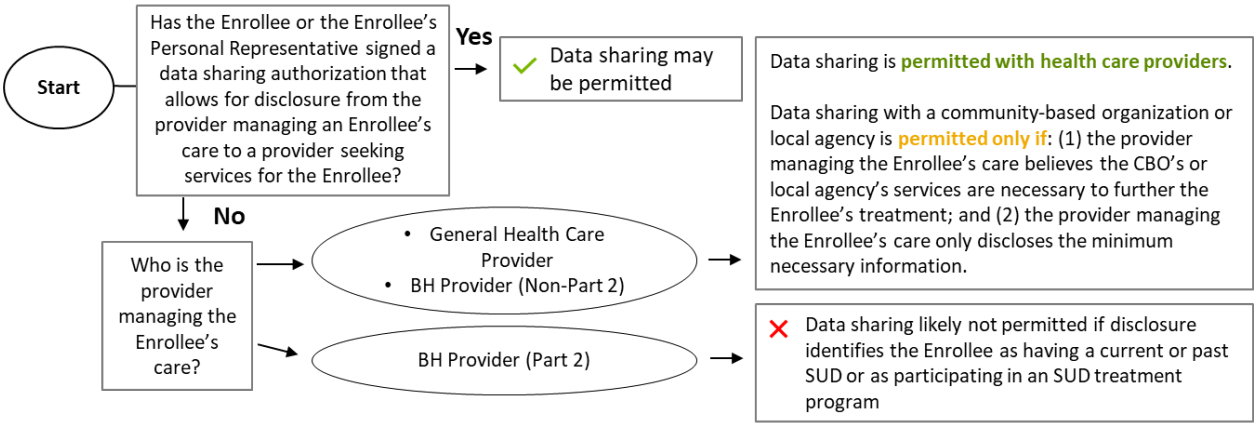
3. Care Coordination and Referral Management

Providers, including ECM Providers, support care coordination and care transitions for Enrollees. Providers engage and connect Enrollees to appropriate providers, services, and resources as needed to make referrals, coordinate care, and support care transitions across MCPs, community-based social and human service providers, and county and other public agencies and Community Supports Provider networks.

Use Case 3-1:

Data Exchange: Information such as diagnoses, care plan, and goals
Function: Care coordination and referral management
Originating Entity: Provider responsible for managing an Enrollee's care
Receiving Entity: Provider seeking information to determine whether such provider may provide services to the Enrollee and/or provide services to the Enrollee

Use Case 3-1 Visualization



Legal Rationale

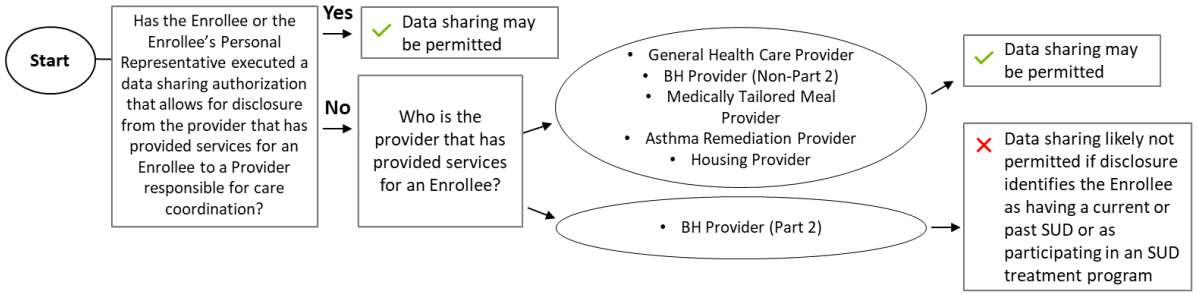
When the Enrollee has not signed an authorization that allows for disclosure, Providers that are general health care providers or behavioral health providers not subject to 42 C.F.R. Part 2 potentially may disclose information to health care providers since covered entities may disclose PHI to health care providers for treatment purposes. If the recipient is a community-based organization that is not a HIPAA covered entity, under guidance issued by the Office for Civil Rights then disclosure is only permitted if the disclosing health care provider believes that the disclosure helps advance the Enrollee's treatment and the minimum necessary information is disclosed.[25] Providers that are behavioral health providers subject to 42 C.F.R. Part 2 may not disclose information since disclosure is not allowed for care coordination purposes without consent.

[25] HIPAA FAQ, HHS.

Use Case 3-2:

Data Exchange: Confirmation of services such as encounter information, including screenings, diagnoses, services rendered, and procedures
Function: Care coordination and referral management
Originating Entity: Provider that has provided services to an Enrollee and/or has received a referral to provide services to an Enrollee
Receiving Entity: Provider that is responsible for coordinating the Enrollee's care

Use Case 3-2 Visualization



Legal Rationale

When the Enrollee has not signed an authorization that allows for disclosure, data sharing regarding confirmation of services potentially may be permitted from a provider to another provider responsible for coordinating the Enrollee's care if the provider that is sharing information is a:

- General health provider or behavioral health provider not subject to 42 C.F.R. Part 2 since covered entities may disclose PHI for care coordination purposes;
- Medically tailored meal provider; if such provider is subject to HIPAA than it may disclose its information in compliance with HIPAA for care coordination purposes; or
- Housing provider since federal HMIS requirements permit disclosures without consent for purposes of payment

A behavioral health provider subject to 42 C.F.R. Part 2 may not disclose Enrollee information to another provider for care coordination purposes without authorization.

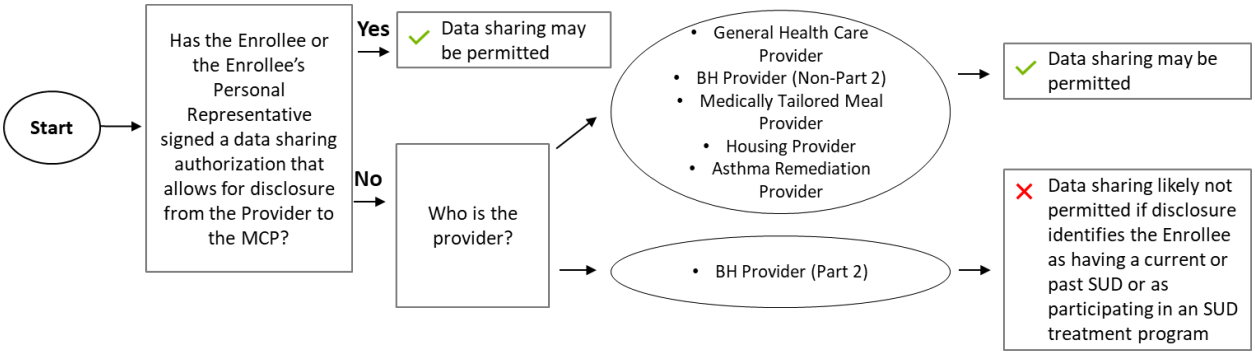
4.Billing and Encounter Reporting Practices

Providers submit claims/invoices to MCPs for services rendered. MCPs report complete and accurate encounters of services to DHCS, including supplemental reports that DHCS may use to verify encounter data completeness.

Use Case 4-1:

Data Exchange: Claims information
Function: Billing for payment of services
Originating Entity: Provider
Receiving Entity: MCP

Use Case 4-1 Visualization



Legal Rationale

Claims information potentially may be disclosed from a provider to an MCP if the provider is a:

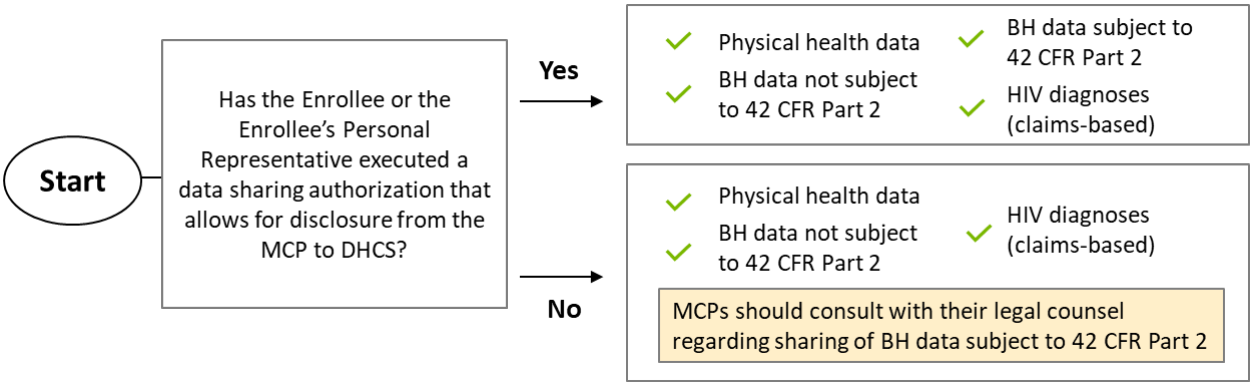
- General health provider or behavioral health provider not subject to 42 C.F.R. Part 2 since covered entities may disclose PHI to a health plan for payment purposes;
- Medically tailored meal provider; if such provider is subject to HIPAA, then it may disclose its information in compliance with HIPAA for the reasons stated above; and
- Housing providers since federal HMIS requirements permit disclosures without written consent for purposes of payment

Behavioral health provider subject to 42 C.F.R. Part 2 may not submit invoices to the MCP without consent; there is no exception under 42 C.F.R. Part 2 that permits disclosures for payment purposes without authorization.

Use Case 4-2:

Data Exchange: Encounter information
Function: Encounter reporting
Originating Entity: MCP
Receiving Entity: DHCS

Use Case 4-2 Visualization



Legal Rationale

Encounter data containing general health information, behavioral health information not subject to 42 C.F.R. Part 2, HIV information, or demographic data potentially may be disclosed to DHCS under HIPAA since such disclosure is required by law. Part 2 records could be included in claims/encounter data files if the Enrollee has signed an authorization form compliant with 42 C.F.R. Part 2 that permits disclosure to DHCS.[26] If the authorization form did not reference disclosures to DHCS, Part 2 records could be included if the disclosure met with the "audit and evaluation" exception at 42 C.F.R. Section 2.53 or complied with Section 3221 of the CARES Act; MCPs should discuss such disclosures with their legal counsel.

[26] In many cases, an authorization form that permits disclosure from the Part 2 Provider to the MCP would also permit disclosure to DHCS, since the MCP is a contractor of DHCS.