siren
Social Interventions Research & Evaluation Network

manatt

JULY 2020

Data Sharing and the Law: Overcoming Healthcare Sector Barriers to Sharing Data on Social Determinants

Alexander Dworkowitz, Partner
Manatt Health
Cindy Mann, Partner
Manatt Health

This paper was made possible through the generous support of the
Social Interventions Research & Evaluation Network and the Robert Wood Johnson Foundation.

About Manatt Health

Manatt Health integrates legal and consulting expertise to better serve the complex needs of clients across the healthcare system. Combining legal excellence, firsthand experience in shaping public policy, sophisticated strategy insight, and deep analytic capabilities, we provide uniquely valuable professional services to the full range of health industry players.

Our diverse team of more than 160 attorneys and consultants from Manatt, Phelps & Phillips, LLP, and its consulting subsidiary, Manatt Health Strategies, LLC, is passionate about helping our clients advance their business interests, fulfill their missions, and lead healthcare into the future. For more information, visit https://www.manatt.com/Health or contact:

Alexander Dworkowitz
Partner
Manatt Health
212.790.4605
ADworkowitz@manatt.com

Cindy Mann
Partner
Manatt Health
202.585.6572
CMann@manatt.com

About SIREN

The mission of the Social Interventions Research & Evaluation Network (SIREN) is to improve health and health equity by advancing high-quality research on healthcare sector strategies to improve social conditions. SIREN is supported by Kaiser Permanente and the Robert Wood Johnson Foundation and housed at the Center for Health and Community at the University of California, San Francisco. For more information, visit https://sirenetwork.ucsf.edu.

Data Sharing and the Law: Overcoming Healthcare Sector Barriers to Sharing Data on Social Determinants

Table of Contents

Introduction

Hospitals, health plans, and other organizations in the healthcare system increasingly recognize that the health of patients depends not only on medical interventions, but also on social ones. Under a social determinants of health (SDOH) model, care for patients may involve linking those patients to services that are not provided by healthcare providers. For instance, it is critical for an asthmatic child from a low-income family to have access to expert physicians, but replacing a moldy home carpet may be just as important. These types of coordinated efforts are critical to promoting health equity for vulnerable populations. Meaningfully integrating social risk screening and social interventions into healthcare delivery programs requires overcoming new challenges, including funding social services interventions and establishing linkages between healthcare providers and community-based organizations (CBOs). Since healthcare organizations' ability to engage the social services, education, and criminal justice sectors often requires the exchange of detailed information—including information that may be subject to federal and/or state privacy laws—an added challenge is the lack of an established framework that enables healthcare providers to disclose personal information to CBOs and other involved parties.

Data sharing can be challenging in part because the many privacy laws and regulations at issue were not written with an intersectoral SDOH model in mind. The privacy rule of the Health Insurance Portability and Accountability Act (HIPAA) envisions disclosures of protected health information (PHI) being made between "covered entities"—which are typically healthcare providers and health plans. Federal laws regulating Medicaid and the Supplemental Nutrition Assistance Program (SNAP), also known as food stamps, envision personal information being disclosed for purposes of operating those programs. And criminal history privacy laws typically assume that such information will be used for criminal justice purposes and for background checks, not to help a person find services such as housing.

Healthcare organizations interested in an SDOH model are looking for ways to implement their new approach consistent with patients' privacy rights and applicable law. Such organizations may not be aware of all the privacy laws that apply to their proposed data sharing efforts. Compounding this problem are other barriers. For instance, many of these laws were written long before electronic data sharing was even possible, include confusing and sometimes archaic language, and have not been clarified through guidance issued by administering agencies. Additionally, efforts to share data with CBOs may be hampered by the CBOs not having adequate or timely access to legal support. But these challenges often can be addressed, and in most circumstances personal information can be exchanged for purposes of promoting SDOH.

This paper is intended to address these legal concerns by shedding light on the circumstances in which healthcare organizations can exchange personal information outside the healthcare sector in compliance with federal and state law. It complements earlier work by focusing specifically on common barriers to the healthcare sector's involvement in these data sharing activities. Other reports in this area, such as those produced by Data Across Sectors for Health (DASH), the National Center for Complex Care, the Network for Public Health Law, the All In: Data for Community Health learning collaborative, and others, have weighed

in on related topics, including by offering advice and support on how to implement data sharing (e.g., about using data sharing agreements and patient consent forms) or by focusing on the exchange of data between healthcare and select other sectors.[1]

The paper focuses on four use cases that reflect real-life experiences of healthcare institutions implementing cross-sector initiatives and explains how statutes and regulations may be applied to those use cases.[2] The use cases are organized as follows:

- Each use case begins with an analysis of federal laws that are applicable to the disclosures set forth under the use case, explaining what information may be disclosed in compliance with those laws, what information may not be, and the areas in which there is ambiguity in the law.[3]
- The federal law analysis is followed by a discussion of the ways in which state laws impose requirements that extend beyond federal law. Laws from three states are examined:
  - California and New York, which generally are considered states with a high level of privacy regulation; and
  - Louisiana, which is considered a less heavily regulated state.

The use cases highlighted in the paper were selected based on input from organizations that are undertaking and supporting this work. Some of them address the impact of making disclosures through third-party platforms, such as health information exchanges. The use cases start with and focus on the healthcare sector's ability to share data with external partners. When applicable to the particular scenario, the analysis also addresses bidirectional information sharing.[4]

- Under the first use case, a clinician and a housing provider share information on a shared patient in order to help the patient find housing.
- The second use case involves disclosures between a school health program, healthcare providers, and state agencies to improve the quality of healthcare for a school's students and connect them with publicly funded meal programs.
- Under the third use case, a health services unit of a prison seeks to connect an inmate with healthcare providers and CBOs prior to the inmate's release from prison.
- The final use case involves a scenario in which a managed care organization seeks to obtain information on its members to assist the organization with enrolling interested members in SNAP.

Although the paper examines only four use cases, it provides a framework that can be used to approach similar data sharing questions under other scenarios. Any expansion to other use cases, however, will need to take into account other applicable privacy laws (such as protections for domestic violence victims under the Violence Against Women Act) that are not addressed here.

One of the key findings of the paper is that, despite the barriers posed by various privacy laws, sharing data across different sectors is possible. In all four use cases, disclosure of information is permitted in at least some circumstances, and disclosure is almost always permitted if the individual who is subject to the disclosure signs a written consent form allowing disclosure. Given the emphasis on written consents, data sharing often will depend on the feasibility of obtaining consent. In some use cases, it is fairly easy for the

parties to ask an individual to sign a consent form. But in use cases that require the disclosure of data on thousands of individuals, obtaining written consent may pose an important barrier to intended data sharing initiatives. Similarly, laws governing the content of consent forms can themselves create barriers to managing consents. The paper also highlights ambiguities in different privacy laws, which can contribute to different interpretations in legal requirements that hinder data sharing.

The paper concludes with action steps that healthcare organizations investing in models of care that involve intersectoral data sharing can take to address legal challenges posed by privacy laws. These action steps provide guidance on how to develop a data sharing model that respects privacy while also allowing for the coordination of services across many sectors. Nevertheless, the paper is not intended to be legal advice, and parties interested in increased data sharing should consult with legal counsel when appropriate.

The analysis is intended to give parties interested in data sharing across different sectors insight into applicable laws and how those may apply under different scenarios. However, this paper is not intended to be legal advice. This paper does not examine all potentially applicable privacy laws. For example, laws that protect the records of domestic violence or child abuse victims were not reviewed, nor laws that protect certain types of health information, such as records that contain genetic information. Moreover, even when applicable privacy laws may permit disclosure, there may be other reasons disclosure is prohibited. For example, one organization may have inadequate security for its information technology systems, and therefore another party may view sharing personal information with that organization as too risky. Further, there may be policies or contractual agreements that prohibit a disclosure even where applicable law allows it. We recommend that agencies planning to increase data sharing consult with legal counsel before doing so.

Analysis of Use Cases

Clinician Connecting Patient to Housing

Use Case Overview

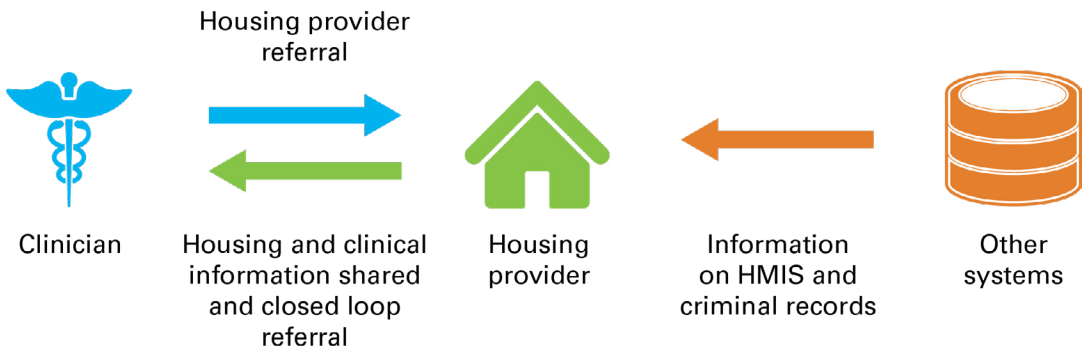
A healthcare clinician—whether a physician, a nurse practitioner, a social worker, or another licensed healthcare professional—treats an adult patient who has a serious mental illness and is homeless. The clinician identifies a housing program that can help find the patient housing. The clinician refers the patient to the housing program, either by recommending that the patient visit such program or by sending the patient's information directly to the housing program through a third-party electronic platform. The housing program is not a "covered entity" under HIPAA, nor is it a "Part 2 program" under 42 C.F.R. Part 2 ("Part 2")—the federal substance use disorder (SUD) confidentiality regulation—and so its employees have not been trained in following HIPAA.

The patient then visits the housing provider to obtain services. The housing provider seeks to obtain information from the clinician relevant to housing placement, including information on mental health and SUD treatment that the patient received through the clinician. The housing provider wants to supplement the health data with information from the local homeless management information system (HMIS) in order to understand what housing services the patient has received previously. Because certain types of housing are unavailable to individuals with particular categories of criminal convictions, the housing provider also seeks information on the patient's criminal background.

The clinician asks the housing provider to provide a "closed loop" referral. That is, the clinician asks to be informed about whether the patient has been successfully placed in housing, since such placement will impact future treatment. The clinician might also seek information about the nature of the housing and related services provided to the patient.

Note that while this use case focuses on disclosures between clinicians and housing providers, the analysis below would be largely the same if the exchange occurred between the clinician and another type of CBO, such as a food bank.

Figure 1. Connection to Housing Use Case Process Flow



Information Disclosures Allowed Under Federal Law

The clinician and the housing provider may use and disclose almost all of the patient's information as described in the use case in compliance with federal law, typically even if they do not have the patient's written consent to do so. This includes data on the clinician's services, physical and mental health diagnoses, and the housing provider's services. However, the substance use and criminal records are different. Part 2, the federal SUD confidentiality regulation, almost always requires written authorization for disclosure, so any SUD records covered by Part 2 could be provided only if the patient signed a written consent form.

Health Information From the Clinician to the Housing Provider[5]

The information that the clinician is sharing with the housing provider is considered PHI under HIPAA. Nevertheless, the clinician is allowed to disclose this information under federal law without written authorization in many circumstances. Regardless of whether the clinician discloses the patient's information through an electronic platform or via phone, email, fax, or another method, the information will be considered PHI because it identifies the patient as having received services from the clinician. The clinician is permitted to disclose the information to the housing provider if the patient signs a HIPAA-compliant authorization form.[6] But under federal law, the clinician also can disclose this information to the housing provider without obtaining the patient's written authorization if the clinician believes the housing is necessary for improving the patient's health, the clinician is not subject to the federal SUD confidentiality regulations at 42 C.F.R. Part 2, and the records do not include psychotherapy notes.[7] Although the housing provider is not a HIPAA-covered entity, HIPAA permits a clinician to disclose PHI to a noncovered entity if the disclosure relates to the treatment the clinician gave the patient.[8]

If the clinician is subject to the federal SUD confidentiality regulations at 42 C.F.R. Part 2, however (discussed below), and the information to be sent to the housing provider contains SUD information, then the clinician will need the patient's written consent in order to make the disclosure.

If the clinician is federally assisted in some manner (the clinician is federally assisted if, among other things, the clinician participates in Medicare or Medicaid), then the clinician will be subject to the federal SUD confidentiality regulations at 42 C.F.R. Part 2 if he or she "holds himself or herself out" as providing SUD services.[9] For example, if the clinician's website identifies the clinician as an expert in SUD treatment, then the clinician likely has held himself or herself out as a provider of SUD services and needs to comply with Part 2. If this is the case, the consent form that the patient signs must meet Part 2 requirements. While there is no requirement as to which party needs to present the form to the patient—it could be the clinician, the housing provider, or a third party—the authorization form requirements under Part 2 are somewhat stricter than the HIPAA requirements (although recent statutory changes may result in changes to these Part 2 requirements).[10] In particular, the authorization form would need to identify the housing provider by name unless the disclosure were made through a health information exchange or other third-party platform, and even then there is some ambiguity in federal law as to whether the name of the housing provider must be included on the form.[11] The patient also will need to sign a consent form in the event that the clinician seeks to disclose psychotherapy notes to the housing provider.[12]

HIPAA 101: HIPAA's privacy rule governs the disclosure of protected health information (PHI). PHI is information created or received by a healthcare provider, health plan, employer, or healthcare clearinghouse that relates to a health condition, the provision of healthcare, or payment for healthcare; to be considered PHI, information must identify an individual or there must be a way to use the information to identify an individual. Only "covered entities"—healthcare providers, health plans, and organizations that facilitate the exchange of information between providers and plans, known as "health care clearinghouses"—must comply with HIPAA, along with contractors of those groups, who are called "business associates."

Under HIPAA, PHI is confidential and cannot be used or disclosed unless a particular exception allowing use or disclosure applies. Three commonly used exceptions are disclosures for purposes of (1) treatment, (2) payment, and (3) "health care operations," a catchall category that includes quality improvement and data analytics related to care coordination. Typically, covered entities share PHI with one another under these exceptions.

For example, a hospital may share with a clinic PHI regarding patients who are treated by both providers, or a physician group may disclose PHI to a health plan in order to obtain payment from the plan. However, in guidance, the Office of Civil Rights (OCR) of the federal Department of Health and Human Services—the agency that enforces HIPAA—explained that the treatment exception may permit disclosures to noncovered entities such as CBOs in some cases: "[H]ealth care providers who believe that disclosures to certain social service entities are a necessary component of, or may help further, the individual's health or mental health care may disclose the minimum necessary PHI to such entities without the individual's authorization."[13]

Other Information Sought by the Housing Provider to Support Housing Placement

The housing provider may obtain information on the patient that other organizations have uploaded to HMIS. Federal guidance permits "covered homeless organizations"—which are providers of housing and other social services—to disclose data to other organizations through an HMIS in order to "provide or coordinate services to an individual."[14]

The housing provider may obtain criminal records about the patient, so long as the housing provider does not log on to the criminal justice agency's data system and the records do not contain "nonconviction data," which are records relating to a charge that was dismissed or for which the patient was ultimately acquitted, as well as arrest information if more than one year has passed since the date of arrest and there is no active prosecution.[15] Since the housing provider is not an employee of a criminal justice agency, the housing provider may not have "direct access" to a state or local criminal history database, meaning that the housing provider may not log in to and search for individual records in such database.[16] However, federal law permits the housing provider to obtain criminal records by other means. For example, some law enforcement agencies provide a public database of criminal records, and others may provide such records to an organization such as a housing provider upon request.

Closed-Loop Referral Back to the Clinician

The clinician may obtain a closed-loop referral from the housing provider that indicates that the patient received services from such provider and includes information about the nature of the services. Since the housing provider is not subject to HIPAA or Part 2, these federal laws do not restrict the manner in which such provider informs others of the services it provides. The housing provider is permitted to share these data through an HMIS since HMIS information may be disclosed for purposes of coordinating services.

State-Specific Limitations

In each of the three states surveyed, state law imposes limitations that extend beyond federal law and further limit how information may be exchanged between the clinician and the housing provider. For example, these laws may require the patient to sign an authorization form (i.e., provide written consent) where federal law does not require consent, may require the authorization form to meet additional requirements, or may prohibit the disclosure of certain information entirely.

As noted earlier, the following analysis sets forth only the areas **where state law is more stringent than federal law**. Since organizations operating in these states must follow both state and federal law, these restrictions are in addition to the federal restrictions described above.

California

- Under the California Confidentiality of Medical Information Act (CMIA), written authorization typically will be needed for the disclosure of health information from the clinician to the housing provider, but there is an important exception to this requirement if the clinician and housing provider are both part of a "homeless multidisciplinary team." The CMIA, California's healthcare privacy law, typically applies to the same type of information as HIPAA but differs from HIPAA in that disclosures for purposes of diagnosis or treatment can only be made to "providers of health care, health care service plans, contractors, or other health care professionals or facilities."[17] Since the housing provider does not fall within any of these categories, the CMIA requires written authorization for the disclosure from the clinician to the housing provider. Moreover, the CMIA imposes requirements for authorization forms that go beyond HIPAA: The forms must be in at least 14-point font and include a "specific date" on which the form expires.[18] The state's mental health and HIV laws also suggest that a disclosure of information subject to those laws cannot be made to the housing provider since it is not a licensed healthcare provider.[19] Importantly, however, California has adopted a limited waiver of state laws like the CMIA that require consent for disclosures **if the individual being treated is homeless or at risk of homelessness**. That waiver, however, is subject to several restrictions. These include that the clinician and housing provider must join a homeless multidisciplinary team,[20] take privacy awareness training, and sign a confidentiality statement.[21]
- In order to obtain HMIS information on the patient, the housing provider will need to be a participant in the local HMIS, and the patient will need to have signed the system's authorization form allowing disclosures to participants.[22] If the clinician seeks confirmation through HMIS that the housing services were provided, then the clinician will need to become a participant in the applicable HMIS.

- The housing provider may be able to obtain limited public information related to the patient's past arrests, which may include the charges brought against the patient.[23] The state also has a public sexual offender database.[24] But if this publicly available information is not sufficient, then the housing provider will be able to obtain sought-after records from the applicable law enforcement agencies only if the patient signs a written consent form and the law enforcement agencies agree to recognize such form, since unlike federal law, California law does not permit the disclosure of criminal records for purposes of coordinating care.[25]

Louisiana

- If the clinician is an employee of a clinic or another provider that is owned and operated by the Louisiana Department of Health, then the clinician needs the patient's written consent prior to disclosing PHI to the housing provider.[26] In such a case, the authorization form must include the name of the housing provider and must be signed by both the patient and a witness.[27] Written consent is also needed if the clinician is a licensed social worker.[28]
- In order to receive data from a particular HMIS, the housing provider will need to become a participant in that HMIS. Whether the patient needs to sign an authorization form depends on which HMIS is being accessed. For example, the New Orleans-area HMIS defers to federal policies as to whether written consent is needed, and therefore a patient's data may be disclosed to another HMIS participant for purposes of providing or coordinating services without written consent.[29] In contrast, in many other parts of the state, written consent is required.[30]
- As in California, limited information related to arrests is publicly available. This information includes a description of the individual and the charges brought against that person.[31] More-detailed criminal histories are maintained by the Louisiana Bureau of Criminal Identification and Information. Other than information held in sex offender registries, this more detailed information is not public and cannot be disclosed.[32]

New York

- The clinician is permitted to send health information to the housing provider, but only if the clinician informs the patient in advance that the patient is being referred to the housing provider and the patient does not object to the disclosure. The New York State Department of Health (NYS DOH) has interpreted New York State law as requiring a patient's consent for the disclosure of the patient's health information, even where such disclosure is being made for purposes of treatment or care coordination. However, NYS DOH also has said that consent need not be written but can be oral or even implied: "At a minimum, the patient must have knowledge that the patient's chosen health care provider is making the disclosure."[33] Therefore, if the clinician makes clear to the patient that the patient's information may be sent to the housing provider and the patient does not object, then the clinician may provide the information to the housing provider.
- While oral or implied consent is sufficient in many cases, if the clinician is employed by a clinic or facility that is subject to the state's mental health law, then the patient's written consent is needed for the clinician to disclose health information to the housing provider.[34]
- The housing provider may obtain HMIS information only if it is a participant in the applicable HMIS, and likewise the clinician may obtain a record of the housing provider's services through HMIS only if the clinician is an HMIS participant.[35] HMIS requirements, however, do differ by region in New York State.

Depending on the region, the patient may have to sign an HMIS authorization form in order for the housing provider to provide a closed-loop referral to the clinician. New York City's HMIS, for example, would allow disclosure of HMIS information so long as the patient was informed that the housing provider may disclose HMIS records, while the Albany HMIS would not allow disclosure unless the patient has signed a release.[36]

- The housing provider may obtain limited information about the patient's criminal convictions that is publicly available.[37] If the housing provider needs more detailed information than what is set forth on the state's public website, then the patient will need to provide such records directly to the housing provider, since New York law does not permit law enforcement agencies to disclose criminal records for purposes of coordinating care.[38]

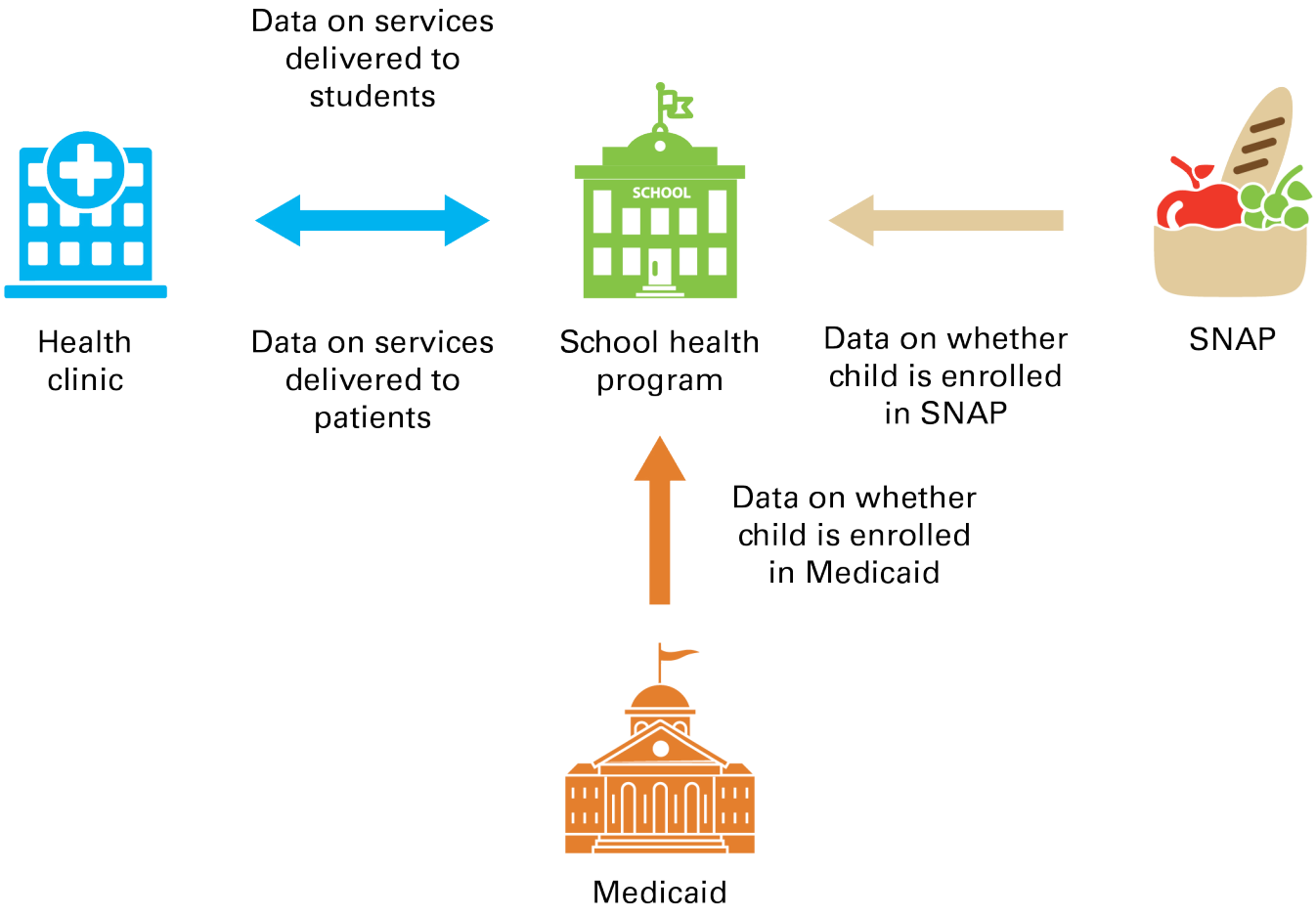
School Health

Use Case Overview[39]

A school health program in a public school provides various healthcare services, such as the administration of immunizations and mental health counseling, to its students. In an effort to improve the quality of care it provides, the school health program seeks health information from other providers, including federally qualified health centers and medical groups that may provide services to the same population. To better coordinate care, those other healthcare providers also seek information from the school health program on the services it provides. The school health program and these other healthcare providers might exchange information directly, or they might use a third-party platform such as a health information exchange.

Many students at the school are from low-income families, but some do not currently receive free or reduced-price breakfasts or lunches. Concerned that the lack of access to food is damaging to the health of its students, the school health program seeks information on whether these children are enrolled in SNAP and Medicaid to help determine whether the children should qualify for meal assistance. (Under federal law, children in households receiving SNAP automatically qualify for free school meals, and those enrolled in Medicaid may also qualify for free school meals if their family income is below 133% of the federal poverty level; those with higher income levels may still receive reduced-price meals.)

Figure 2. School Health Program Use Case Process Flow



Information Disclosures Allowed Under Federal Law

Health Information From Providers to the School Health Program

Since the school health program is a healthcare provider, regardless of whether such program is a "covered entity" under HIPAA outside providers may disclose PHI to the school health program without obtaining consent, either directly to the school health program or through a third-party platform. HIPAA permits disclosures of PHI to healthcare providers without consent for purposes of treatment.[40] If the provider is subject to Part 2, the federal SUD confidentiality regulation, then it will need to obtain the student's written consent for the disclosure of the Part 2 program's records to the school health program. The parent's consent is also required if the applicable state requires that the program obtain parental consent to the Part 2 program's services.[41] The authorization form will need to identify the school health program by name if the

Part 2 program discloses information directly to the school health program; if disclosure is made through a third-party platform, then the school health program will not need to be identified by name since it has a treating provider relationship with the students.[42]

School Health Records to Other Providers Treating Their Students

Though the external healthcare providers can send health records to the school health program, the school health program cannot as easily transfer records to the outside healthcare providers. This is because the school's health records are subject to the Family Educational Rights and Privacy Act (FERPA), the federal statute that applies to educational records of federally funded schools. Since the records are subject to FERPA, they are not covered by HIPAA.[43] The school health program can disclose its students' health records to other healthcare providers only in cases of emergency or with written, signed authorization from students' parents (or the students themselves if they are 18 or older).[44]

SNAP or Medicaid Information to the School Health Program for Purposes of Providing School Meals

Under federal law, the school district can obtain SNAP and Medicaid data on behalf of the school health program in order to enroll low-income students in programs providing free or reduced-price meals.

Federal law permits state SNAP agencies to disclose SNAP participation and income information to school districts that administer school breakfast/lunch programs for purposes of determining eligibility for these programs.[45] Similarly, since the enactment of the Healthy Hunger-Free Kids Act of 2010, Medicaid agencies are permitted to disclose Medicaid enrollment status and income levels to school districts in order to connect students with these meal programs.[46] While Medicaid data are subject to HIPAA, such disclosure is permitted under HIPAA so long as only the minimum necessary data are disclosed to the school district.[47] The Medicaid agency must enter into an agreement with the applicable state SNAP agency, and the U.S. Department of Agriculture (USDA), which administers SNAP, must approve such data sharing in order for it to occur.[48]

While these laws do not appear to permit an individual school health program to review SNAP or Medicaid eligibility and income data to determine eligibility for meal assistance, here the school health program can reach out to the local school district (or, if the school meal programs are directly administered by the state, to the applicable state agency), and that school district can check the child's eligibility for these programs on the school health program's behalf.

State-Specific Limitations

In contrast to the "connection of housing" use case, states do not impose limitations on the disclosures in this use case that are materially different from those imposed by federal law. This is in part because the federal school breakfast and lunch laws give school districts the right to obtain SNAP and Medicaid program data for purposes of enrolling their students in meal assistance, and therefore states do not have the discretion to legally prohibit such disclosures.[49] Similarly, FERPA already requires written parental consent for the disclosure of student health records to other healthcare providers, and therefore states do not have the flexibility to modify this requirement.[50]

Nevertheless, state laws do impose some additional restrictions about the exchange of information between school health programs and external healthcare providers. These are described below.

California

- In addition to the requirement to obtain a parent's consent before disclosing a student health record to an outside healthcare provider, the school health program must ensure that the providers who receive the students' information are notified that they may not re-disclose the information without the parent's consent. A copy of the consent also must be kept in the school's files.[51]

Louisiana

- As noted above, providers owned and operated by the Louisiana Department of Health generally need written consent before disclosing PHI, even if for treatment purposes. Here, the school health program can obtain PHI from a provider operated by the Louisiana Department of Health only if the student's parent has signed an authorization form (or the student signed the form, if the student consented to the applicable service), a witness signed the form, and the form names the school that is to receive the student's information.[52] Similarly, a social worker can disclose information to the school health program only with written consent.[53]
- School health programs are limited in the type of information they can require their students to provide. Schools may not require the collection of information on "[m]ental or psychological problems of the student or the student's family" or "[s]exual behavior or attitudes," among other types of information, although such information may be voluntarily disclosed by students or parents.[54] It is unclear whether this is intended to prohibit school mental health counselors from inquiring about these topics, or if it simply prevents schools from mandating that students provide information on these issues (by, for example, requiring students to fill out surveys on these topics).

New York

- If a healthcare provider seeks to disclose its patients' information to a school health program, a parent must be informed of the intended disclosure before the information is shared. As discussed in the first use case, New York State interprets its privacy laws as requiring at least "implicit" consent for the disclosure of PHI between providers even for treatment purposes.

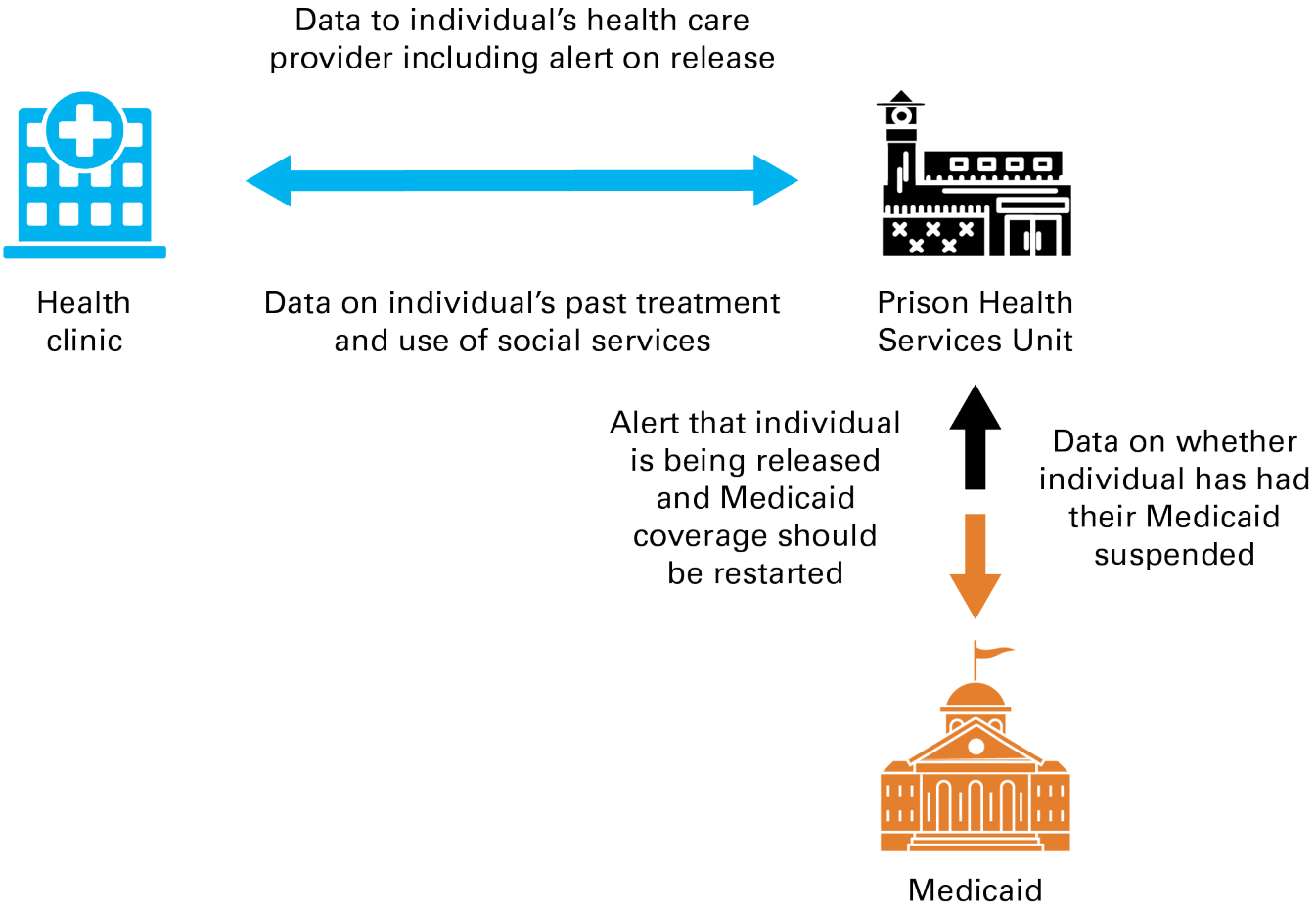
Prisoner Reentry

Use Case Overview

An individual receives healthcare services while an inmate in prison, which may be a federal, state, or local facility. The services are provided by the prison's health services unit, which is considered a healthcare provider and a covered entity under HIPAA but is not subject to Part 2, the federal SUD confidentiality regulation. Prior to the individual's release, the health services unit seeks to make connections with the healthcare providers and community-based organizations that provided services to the individual prior to their incarceration, and therefore seeks to connect to a third-party platform that contains such information. In trying to connect the individual with healthcare benefits post-release, the health services unit also seeks information from the state's Medicaid agency as to whether the individual's Medicaid status was suspended due to incarceration and therefore could be reactivated upon release.

After obtaining a list of providers and CBOs—such as a nutrition or housing program—that formerly cared for the individual, the health services unit plans to send an alert to such providers and CBOs to inform them of the date of the individual's release and to recommend that they connect with the individual. The health services unit also would like to notify the state's Medicaid agency to inform the state that the individual is about to be released and may be eligible for Medicaid upon release.

Figure 3. Prisoner Reentry Use Case Process Flow



Information Disclosures Allowed Under Federal Law

Health Information From Providers to the Health Services Unit

Healthcare providers generally are permitted to disclose PHI to the health services unit without the individual's written consent since the health services unit is seeking PHI for treatment purposes, although written consent is required if the disclosing provider is subject to the federal SUD confidentiality regulations at 42 C.F.R. Part 2. If written consent is required because one of the disclosing providers is subject to Part 2, such consent may be obtained by the health services unit itself, or the health services unit may rely on a

consent previously obtained by the Part 2 program so long as such consent applies to the health services unit. Since the disclosure will be made through a third-party platform, the authorization form may use a general designation; for instance, the form could indicate that disclosures may be made to any healthcare provider that provides treatment to the individual.

Medicaid Suspension Information to the Health Services Unit

The health services unit is allowed to obtain Medicaid suspension status information from the state Medicaid agency if the unit has contracted with the state Medicaid agency to assist in the administration of the Medicaid program. If there is no such contract and the applicable beneficiaries have not provided consent, federal law is unclear as to whether the health services unit is allowed to receive Medicaid suspension status information in order to facilitate inmates' enrollment in Medicaid post-release. On the one hand, federal law permits disclosure of Medicaid information for "purposes directly connected with" the administration of Medicaid, and such purposes include "establishing eligibility."[55] On the other hand, federal regulations mandate that Medicaid agencies obtain permission from a Medicaid beneficiary "whenever possible, before responding to a request for information from an outside source …."[56] This may mean that organizations that do not have a contract with the state Medicaid agency to assist with enrollment activities cannot obtain Medicaid beneficiary information for enrollment purposes, absent written consent.

Alert From Health Services Unit to Providers, CBOs, and the Medicaid Agency About Impending Release

The health services unit may send an alert about an impending release from prison to healthcare providers and the local Medicaid agency in compliance with HIPAA without obtaining the consent of the individual. Since the alerts in effect notify the recipient that the individual has received services from the health services unit, the alerts are a form of PHI, but they are being provided for the purposes of treatment, which does not require written authorization.[57] Similarly, the disclosure to the Medicaid agency is permitted because such disclosure is for purposes of payment under HIPAA, as the information will be used to determine eligibility for health benefits.[58] In making a disclosure to the Medicaid agency, the health services unit may disclose only the minimum PHI necessary to notify the agency of the need for an eligibility redetermination. Past diagnoses, treatment, and other information irrelevant to an eligibility determination should not be provided.[59]

These alerts can be disclosed in compliance with federal laws on criminal records. Federal regulations limit disclosures of nonconviction data and prohibit non-criminal justice agencies from having direct access to criminal record systems.[60] But in sending an alert of impending release to providers, CBOs, and a Medicaid agency, the health services unit would not be engaging in these prohibited disclosures. In short, federal law allows information on inmate release dates to be publicly disclosed.

While healthcare providers can receive these alerts in compliance with federal law, it is less clear whether CBOs, such as nutrition or housing programs, are allowed to receive these alerts under HIPAA without written consent. While guidance permits healthcare providers to disclose PHI to CBOs in the context of making a referral to a CBO, here the health services unit is not referring the individual for services but is simply notifying the CBO that the individual is being released.[61] Given this ambiguity, the health services unit may need to obtain the individual's written authorization prior to sending an alert to a CBO.

State-Specific Limitations

Laws in California, Louisiana, and New York applicable to disclosures under the prisoner reentry use cases are in harmony with federal law in several respects. For example, states must follow federal law in allowing disclosures of Medicaid information for purposes of administration of the Medicaid program.[62] Further, none of the three states extends criminal records laws—which generally limit the disclosure of criminal histories—to information about an inmate's impending release date, and the states or counties within them often make this information publicly available.[63] Louisiana has even implemented an initiative under which prisons notify the state Medicaid agency of the impending release of prisoners.[64]

However, healthcare privacy laws impact a few disclosures related to this use case. These are described below.

California

- The health services unit may not send an alert about the individual's impending release from prison to CBOs without the individual's written consent. While federal law is ambiguous on this point, California law is more clear in that disclosures for treatment purposes may be sent only to "providers of health care, health care service plans, contractors [generally independent practice associations or pharmacy benefit managers], or other health care professionals or facilities."[65] Since written consent is required under the CMIA, the consent form must also comply with the CMIA, meaning it must be written in at least 14-point font and specify an expiration date.

Louisiana

- If the health services unit is seeking records from a provider operated by the Louisiana Department of Health, then the health services unit needs the patient's written consent in order to obtain such records, and the authorization form must name the health services unit and be signed by a witness.[66] The health services unit also needs written consent if it seeks records held by a social worker.[67]

New York

- The health services unit may obtain the individual's records from their previous treating providers if the health services unit informs the individual that it plans to do so and the individual does not object. As noted above, NYS DOH requires a patient's consent for the disclosure of PHI, although such consent may be implicit or oral (written is also permitted). If the source of the health information is a facility regulated by New York's Office of Mental Health, then implied consent is not sufficient, and the health services unit will need to obtain the individual's written consent to obtain the necessary records.

Assistance in Obtaining Food Stamps

Use Case Overview

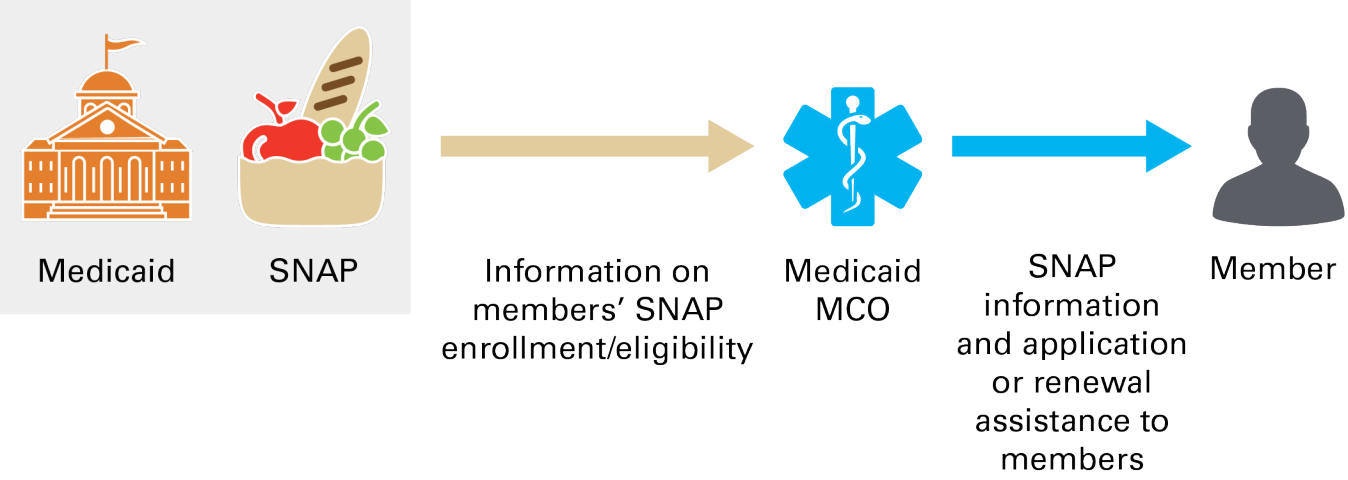
A Medicaid managed care organization (MCO) believes many of its low-income beneficiaries lack reliable access to food and that food insecurity is having a negative impact on member health. The MCO therefore seeks to facilitate SNAP enrollment for its members. The MCO hopes to get a list of members currently

enrolled in SNAP, as well as the renewal date for those who are enrolled in SNAP, so that the organization can assist with renewal applications. The MCO also wants to know which of its enrollees not currently enrolled in SNAP appear to meet the SNAP income requirements (income at or below 130% of the federal poverty level). The MCO asks the state SNAP agency and/or the state Medicaid agency for this information.

Once the MCO obtains this information, it contacts its members who are not enrolled in SNAP but who are likely eligible for the program in order to provide assistance with filing a SNAP application. For those who are currently enrolled in SNAP but whose SNAP benefits are subject to renewal in the near future, the MCO might remind the member about the need to renew their benefits and offer assistance with that process.

Although this use case focuses on Medicaid MCOs, the same analysis would follow if the organization seeking to facilitate enrollment in SNAP were a medical group, a hospital, an accountable care organization, or another healthcare organization that is responsible for the care of a group of patients.

Figure 4. Assistance in Obtaining Food Stamps Use Case Process Flow



Information Disclosures Allowed Under Federal Law

Disclosure of Medicaid Data to the MCO

The state Medicaid agency could share Medicaid data with a Medicaid MCO to help the MCO enroll individuals in SNAP if (1) the agency or the Centers for Medicare and Medicaid Services (CMS) determined that reducing food insecurity is directly related to the administration of Medicaid; and (2) the Medicaid agency or OCR concluded that disclosing the data to Medicaid MCOs was part of a "population-based activity relating to improving health."[68]

Two separate laws regulate the ability of state Medicaid agencies to share their data with MCOs: federal Medicaid privacy law and HIPAA. The first of those laws, federal Medicaid privacy law, permits states to disclose Medicaid data if the purpose of the disclosure is "directly connected" to the administration of Medicaid or enrollment in free or reduced-price school meal programs (not for enrollment in SNAP, which is a program separate from the school meal programs).[69] Disclosure to the MCO could be allowed if the state

Medicaid agency or CMS found that connecting the beneficiary to food covered by another federal program is directly connected with the administration of Medicaid.[70] However, there is no formal guidance from CMS on this question, and, in the absence of federal guidance, each state Medicaid agency would need to make its own determination.[71]

Assuming such a disclosure complied with federal Medicaid privacy law, arguably it would comply with the other key privacy law, HIPAA, although the relevant HIPAA rules are also somewhat ambiguous. A Medicaid agency may disclose its data to a Medicaid MCO for the MCO's "health care operations" purposes. "Health care operations" include "population-based activities relating to improving health or reducing health care costs, … care coordination, [and] contacting of health care providers and patients with information about treatment alternatives …."[72] An effort to enroll Medicaid recipients in SNAP could be viewed as a "population-based activity relating to improving health," but it is possible OCR could view enrollment in a non-healthcare program as too far afield from a healthcare service to qualify for this HIPAA exception.

Disclosure of SNAP Data to the MCO

The state SNAP agency could disclose SNAP data to the MCO if the parties signed an agreement under which the MCO agreed to adequately protect the data received.[73] Federal law permits state SNAP agencies to disclose their data for purposes directly connected with the administration of SNAP, and assisting individuals in enrolling with SNAP is related to the administration of the program.[74] Under USDA guidance, this means that MCO employees handling the SNAP data must be trained on security protocols and must sign a document stating they understand their responsibilities; in addition, the data may only be stored and exchanged using encrypted servers.[75]

State-Specific Limitations

None of the three states appears to restrict disclosures under this use case beyond the requirements imposed under federal law. California allows disclosures of both Medicaid information and SNAP information for purposes directly connected with the administration of the applicable programs.[76] Louisiana and New York do the same.[77] New York also permits the state to enter into contracts with private organizations to conduct SNAP outreach.[78]

Key Findings From the Analysis

Data Sharing Is Often Permitted

Some healthcare organizations interested in data exchange with the social service and criminal justice sectors believe that such disclosures are often prohibited. But in our analysis, **we found that in all four use cases, disclosures are permitted in at least some circumstances, and disclosures can almost always be made if the individual's written consent is obtained**. Existing law is more flexible than people commonly understand. While the laws at issue vary, they often allow disclosure when the parties are seeking to coordinate the care of an individual jointly under their care. And even when there is no law allowing such disclosures, there may be other means of finding needed information. For example, while the criminal records laws in the three states reviewed do not permit a criminal justice agency to share patients' criminal histories for purposes of coordinating care, the states make public limited criminal history information, which can be accessed via a website or a phone call.

The Challenge of Obtaining Written Consent Varies by Use Case

The most straightforward solution to many of the privacy regulations described is to ask the individual to sign a data sharing authorization form. But the practicality of obtaining consent can vary significantly depending on the use case. In the prisoner reentry use case, there are no significant logistical barriers to obtaining consent. Because the individual is in prison, there is no challenge to locating the individual, and the health services unit can ask if the individual is willing to sign a form that permits data disclosures. In contrast, obtaining written consent in the school health program use case to permit disclosures of school health records is more challenging, since typically it will be the parent who needs to sign an authorization form, and the school health program may not have regular contact with many parents. And in the SNAP use case, asking for consent is impractical. There, the MCO may need data on thousands of its members, and a state Medicaid agency or SNAP agency likely cannot reach out to so many individuals, particularly since these agencies rarely have face-to-face contact with their beneficiaries.[79]

Strict Authorization Form Requirements Complicate Efforts to Share Data

Assuming a party is able to obtain an individual's written consent, laws that regulate the content of authorization forms can limit the effectiveness of those authorization forms. The substance abuse disorder confidentiality regulation, 42 C.F.R. Part 2, typically requires the names of all potential recipients of the individual's information to appear on the face of the authorization form. While that requirement does not apply if disclosure is made through a third-party intermediary and the recipient has a treating provider relationship with the individual, such exception will not be of much value in some circumstances.[80] Louisiana similarly requires certain authorization forms to name all potential data recipients.

Other authorization form requirements can also make disclosures more difficult in practice. California's health privacy law requires the form to include a "specific date" on which the form expires; this suggests that if a form says it expires at the time of program disenrollment or at another event with an unknown date, it would violate the law.[81] A Louisiana regulation requires a witness to sign an authorization form if disclosures are initiated from a setting operated by the Louisiana Department of Health.

Ambiguity in Laws Can Stifle Data Exchange

While laws do not bar data disclosures in all situations, the laws often are difficult to interpret. The use case analyses above highlight several critical areas where the laws are ambiguous. For example:

- CMS has not clarified whether a Medicaid agency may disclose its data for purposes of assisting with enrollment in SNAP.
- It is unclear whether a CBO can be considered to have a "treating provider relationship" under Part 2 and therefore can receive Part 2 information under an authorization form that uses a general designation.
- New York's mental health law does not specify whether written consent is needed to disclose information subject to that law.

These areas where there is lack of clarity can be almost as problematic as a data sharing prohibition. Data sharing depends on the cooperation of at least two parties, and the parties need to be in agreement on what applicable law permits. If one party believes disclosure can be made in compliance with the law but the other party is more risk averse, then data exchange is unlikely to occur.

Ambiguity can be particularly problematic in regard to federal laws that address the privacy of benefit information or state healthcare laws. OCR focuses on privacy issues and therefore will provide guidance on what is permitted under HIPAA. But federal agencies that administer benefit programs such as Medicaid or SNAP devote most of their energies to the operational details of those programs, not privacy issues. Similarly, few state agencies have resources dedicated to privacy and interpretation of privacy law. In the final use case on food stamps, there is a plausible legal theory as to why a state Medicaid agency can share data with the MCO. But absent confirmation from CMS, state Medicaid agencies may be reluctant to share data in this instance.

State Laws Significantly Impact Only Some Data Sharing Use Cases

California, Louisiana, and New York all have state healthcare privacy laws that are more restrictive than HIPAA in certain circumstances. California does not permit disclosures to CBOs without written consent. Louisiana requires written consent if the information comes from a provider operated by the Louisiana Department of Health. And New York requires providers always to have their patients' consent, although in some circumstances their consent may be implied by their actions.

These restrictions significantly impact use cases where disclosure of information from healthcare providers is important. The "Connection to housing" use case, for example, envisions that the information a clinician shares with a housing provider may be subject to multiple state health privacy laws. Clinicians need to be cognizant of these laws to the extent they seek to share information with a housing provider or another type of CBO.

In contrast, state law did not play an important role in the "Assistance in obtaining food stamps" use case. This is because the states' Medicaid and SNAP privacy laws mirror the federal standard, which allows disclosures for purposes of administering these programs.

Conclusion

The analysis of the use cases above shows that disclosures of personal information between the healthcare system, the social service sector, schools, and the criminal justice system can be made in compliance with federal and state laws. There are many scenarios where data can be shared to help coordinate care, and oftentimes the parties can exchange information relatively easily without having to substantially modify their practices. Nevertheless, developing an effective data sharing model that helps improve quality of care and also complies with applicable law remains a challenge. Before parties can enter in a data sharing model, it is essential that they form relationships and build trust among each other and the communities they reach. Obtaining community buy-in through education and outreach efforts throughout the process contributes to the model's success. The following action steps can help parties navigate this challenge.

First, healthcare organizations seeking to exchange data need to work with their data sharing partners to develop a detailed model (e.g., a flowchart) for how they intend to disclose data. When it comes to privacy laws, details matter. As the use cases addressed in this paper indicate, legal requirements depend on not only the purpose of the disclosure but also the nature of the parties involved. Allowing disclosures from a primary care clinic that provides SUD care but is not subject to the federal SUD confidentiality regulation at 42 C.F.R. Part 2, for instance, is very different from allowing disclosures from a similar clinic that is subject to Part 2.

Second, the parties seeking to engage in data sharing should develop a common understanding of both federal and state laws applicable to data sharing and how those laws apply to the data model. The laws described in this paper provide a sample of many common privacy laws applicable to SDOH arrangements, but this paper does not include an exhaustive list of all privacy laws. As part of this process, the parties should develop common assumptions of what is and is not permitted in cases where the applicable law may be unclear. If the parties do not agree to such assumptions, one party may ultimately decline to implement the model out of concern that doing so implicates a risk of violating the law.

Third, if the parties determine that obtaining written consent is necessary, then the parties will need to develop an effective authorization form and consent management process. The form should be written broadly enough to apply to all the disclosures contemplated by the parties, but narrowly enough so it is still meaningful to the individuals being asked to sign it; translation of the form into other languages also needs to be considered. The parties will need to reach agreement on who will ask the individuals to sign the form and under what circumstances, and they will need a system for sharing that form once it is signed.

Fourth, the parties should employ workarounds to address legal restrictions. If a particular type of data cannot be disclosed, another type of data that suits the parties' needs may be available.[82] For example, while access to an individual's full criminal history may be impossible, elements of that criminal history may be publicly available. And if a party has direct contact with an individual, oftentimes the individual has the necessary information and is willing to provide it to the party upon request.

Fifth, the parties should consider ways to promote security that go beyond the minimum legal requirements. The increased interest in data sharing for purposes of improving health has been accompanied by a growth in hacking and data breaches, and therefore developing sufficient security protocols is essential (e.g., encrypting data in motion and at rest). But requirements beyond security protocols may be important as well.

For example, individuals may want the right to access their data, amend it when such data are incorrect, and obtain a record of disclosures. While HIPAA provides many of these rights, not all of the personal information exchanged in these scenarios is subject to HIPAA; other laws sometimes do not provide these same rights.

Sixth, the parties should consider how to maintain these data exchanges over the long term. Documenting the goals of the data exchange and the assumptions behind certain practices will help ensure that data exchange may continue after the leaders who pushed for such exchange move on to other priorities. Similarly, establishing regular communication between the parties involved in the exchange will increase the likelihood that the exchange will continue to address each organizations' needs and privacy and security concerns, which may change over time.

Finally, the findings in this report highlight potential policy targets for reform. Efforts to harmonize privacy laws can help promote data sharing. Common requirements for authorization forms can be particularly useful, since they can enable individuals to consent to the disclosure of many different types of data by signing one form rather than having to sign multiple forms. But even where it is infeasible for the federal government or a state to adopt new laws or regulations, federal and state agencies responsible for interpreting privacy laws have an important role to play. While government agencies are often reluctant to publicly commit to an interpretation of law, many agencies now recognize the opportunities in cross-sectoral data sharing—and the legal barriers that can thwart related initiatives. Parties hoping to share data to promote health and well-being should reach out to the applicable regulatory agencies to request input on what is permitted in cases where the law may be ambiguous.

The Network for Public Health Law (The Network) has created a free legal resource bibliography to promote data sharing across sectors that is available here: https://legalbib.communitycommons.org/.

[1] For example, see the following: Data Across Sectors for Health and The Network for Public Health Law, Data Sharing and the Law: Deep Dive on Consent (November 2018), http://dashconnect.org/wp-content/uploads/2018/11/Data-Sharing-and-the-Law-Deep-Dive-on-Consent.pdf; Data Across Sectors for Health, A Legal Approach to Sharing Health & Education Data (May 2018), http://dashconnect.org/wp-content/uploads/2018/05/DASH-Bright-Spot_Chicago.pdf; The National Center for Complex Health and Social Needs, Cross-Sector Collaboration for Data Sharing (webinar series), https://www.nationalcomplex.care/research-policy/resources/webinars/data-sharing/; Camden Coalition for Healthcare Providers and the National Center for Complex Health and Social Needs, Navigating Legal Parameters for Cross-Sector Data Collaboration (June 2018), https://www.nationalcomplex.care/wp-content/uploads/2018/08/Navigating-Legal-Parameters_.pdf; The Network for Public Health Law, Data Sharing Agreements (Jan. 18, 2020), https://www.networkforphl.org/news-insights/data-sharing-agreements/; All In: Data for Community Health, Webinar: Navigating Consent, https://dashconnect.org/2016/09/11/webinar-navigating-consent/. See also Cason Schmit, Kathleen Kelly, and Jennifer Bernstein, Cross Sector Data Sharing: Necessity, Challenge, and Hope, The Journal of Law, Medicine & Ethics (July 12, 2019), https://journals.sagepub.com/doi/full/10.1177/1073110519857325; The Build Health Challenge, Data Sharing Within Cross-Sector Collaborations: Challenges and Opportunities (July 2018), https://www.debeaumont.org/wp-content/uploads/2019/04/BUILDDataSharing.pdf; The Partnership for Public Health Law, Legal Issues Related to Sharing of Clinical Health Data with Public Health Agencies (April 2016), https://www.astho.org/Public-Policy/Public-Health-Law/Legal-Issues-Related-to-Sharing-Clinical-Health-Data-with-Public-Health-Agencies/.

[2] Denise Chrysler and Colin Boes (speakers), "Navigating Law to Share Data: Privacy and Security Fundamentals," 2019 Public Health Law Summit: Data Sharing to Improve Community Health, The Network for Public Health Law, October 3, 2019, available at https://events.networkforphl.org/2019-summit/schedule/.

[3] "Federal Privacy Laws," The Network for Public Health Law, available at https://www.networkforphl.org/resources/topics/health-information-and-data-sharing/federal-privacy-laws/.

[4] Denise Chrysler, "Checklist of Information Needed to Address Proposed Data Collection, Access and Sharing," The Network for Public Health Law, October 1, 2019, available at https://www.networkforphl.org/resources/checklist-of-information-needed-to-address-proposed-data-collection-access-and-sharing/.

[5] Colleen Healy Boufides, Denise Chrysler, Jennifer Bernstein, Kerri McGowan Lowrey, Peter D. Jacobson and Sallie Milam, "FAQ: COVID-19 and Health Data Privacy," The Network for Public Health Law, June 22, 2020, available at https://www.networkforphl.org/resources/faqs-covid-19-and-health-data-privacy/.

[6] The standards for a HIPAA authorization form as set forth at 45 C.F.R. § 164.508(c).

[7] 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. § 164.501. The prohibition on disclosing psychotherapy notes without a written authorization is rarely a significant barrier to information exchange, since summaries related to counseling sessions—such as diagnoses and medications—can be disclosed without written consent.

[8] 45 C.F.R. § 164.506(c)(1).

[9] 42 C.F.R. § 2.11.

[10] The Part 2 regulations regarding consent form requirements may be revised in light of the passage of the Coronavirus Aid, Relief, and Economic Security (CARES) Act. A provision of that act changes the statute underlying Part 2. While the statute still requires written consent, it allows recipients to redisclose Part 2 data without obtaining a subsequent consent form.

[11] 42 C.F.R. § 2.31(a)(4). A "general designation" of information recipients—rather than a list of all names of potential recipients—may be used if data is excluded through "an entity that facilitates the exchange of health information" and the recipient has "a treating provider relationship with the patient whose information is being disclosed." It is unclear whether a housing provider can have a "treating provider relationship" with a patient.

[12] 45 C.F.R. § 164.508(a)(2).

[13] Department of Health and Human Services Office of Civil Rights, Does HIPAA permit health care providers to share PHI about an individual with mental illness with a third party that is not a health care provider for continuity of care purposes?, available at https://www.hhs.gov/hipaa/for-professionals/faq/3008/does-hipaa-permit-health-care-providers-share-phi-individual-mental-illness-third-party-not-health-care-provider-continuity-care-purposes/index.html.

[14] 69 Fed. Reg. 45888, 45928 (July 30, 2004).

[15] 28 C.F.R. §§ 20.3(q), 20.21(b).

[16] 28 C.F.R. § 20.21(f)(4)(v).

[17] Cal. Civ. Code § 56.10(c)(1). A "contractor" is a medical group, independent practice association, pharmaceutical benefits manager, or medical service organization and is not a healthcare service plan or provider of healthcare. Cal. Civ. Code § 56.05(d).

[18] Cal. Civ. Code § 56.11.

[19] Under California mental health privacy law, disclosures for purposes of "provision of services" can only be made to "qualified professional persons." Cal. Welf. & Inst. Code § 5328(a)(1). Arguably, a housing provider lacking a healthcare license is not a "qualified professional person." Similarly, HIV test results may be shared without authorization only with "providers of health care." Cal. Health & Safety Code § 120985(a).

[20] A homeless multidisciplinary team is "any team of two or more persons who are trained in the identification and treatment of homeless adults and families, and who are qualified to provide a broad range of services related to homelessness." Team members may include mental health counselors, police officers, medical personnel, social service workers, and teachers, among others. Cal. Welf. & Inst. Code § 18999.8(b)(2).

[21] Cal. Welf. & Inst. Code §§ 18999.8, 18999.81. The statute regarding coordinating care for homeless individuals applies to all of California, while the statute regarding coordinating care for those "at risk of homelessness" applies only to Los Angeles, Orange, Riverside, San Bernardino, San Diego, Santa Clara, and Ventura counties.

[22] See, e.g., Los Angeles Homeless Services Authority, Greater Los Angeles Homeless Management Information System Privacy Notice, available at https://www.lahsa.org/documents?id=1114-hmis-privacy-notice.pdf&ref=hmis; San Francisco Department of Homelessness and Supportive Housing, Homelessness Response System, Authorization for Use or Disclosure of Information, available at https://onesf.clarityhs.help/hc/en-us/articles/360029904574-Department-of-Homelessness-and-Supportive-Housing-Privacy-Practice-and-Releases-of-Information. We did not review the policies of every HMIS in California; it is possible that some do not require written consent.

[23] Cal. Govt. Code § 6254(f)(1). This comports with federal law because the definition of "nonconviction data" excludes arrest records if the individual is being actively prosecuted. 20 C.F.R. § 20.3(q).

[24] California Department of Justice, California Megan's Law Website, available at https://www.meganslaw.ca.gov/mobile/Disclaimer.aspx.

[25] Cal. Penal Code §§ 11105, 13300.

[26] La. Admin. Code tit. 48, §§ 507, 509.

[27] La. Admin. Code tit. 48, § 507(A).

[28] La. Admin. Code tit. 46, § 115.

[29] UNITY of Greater New Orleans Continuum of Care (CoC) Housing & Service System: Coordinated Entry Policies and Procedures Handbook, at 20 (Feb. 28, 2019), available at https://unitygno.org/wp-content/uploads/2019/09/LA-503-Coordinated-Entry-Policies-and-Procedural-Handbook-APPROVED-February-2019-Revisions.pdf.

[30] See Louisiana Services Network Data Consortium Release of Information, available at https://static1.squarespace.com/static/5ad7424f7c9327973957a9dd/t/5d71570819b5fb0001abf6d3/1567708937308/LSNDC+Release+of+Information.pdf.

[31] La. Rev. Stat. Ann. § 44:3(A)(4).

[32] La. Rev. Stat. Ann. § 44:3(A)(7).

[33] New York State Department of Health, Guidance Documentation: Privacy and Data Sharing within DSRIP (June 5, 2017), available at https://hca-nys.org/wp-content/uploads/2017/06/FINAL_Privacy-and-Data-Sharing-within-DSRIP-June-5-2017-002.pdf.

[34] N.Y. Ment. Hyg. Law § 33.13(c)(7), (d). Consent is not needed if the recipient is a health plan, a health home, or an organization that coordinates healthcare services, but the housing provider does not fall into any of these categories. While the statute does not explicitly state that consent must be written, most providers in New York assume written consent is needed to disclose these records.

[35] NYC Coalition on the Continuum of Care, HMIS Policies and Procedures, § 6.7, available at https://www1.nyc.gov/assets/nycccoc/downloads/pdf/HMIS_PP_v5.0_2019-Appendices_Amended.pdf.

[36] *Id.*, § 6.6.2, available at https://www1.nyc.gov/assets/nycccoc/downloads/pdf/HMIS_PP_v5.0_2019-Appendices_Amended.pdf; Policies and operations of the CARES of NY, Inc. Regional Homeless Management Information System (CRHMIS), § 13.01.03, available at https://caresny.org/wp-content/uploads/2019/10/CRHMIS-PoliciesProceduresManual-2019.10.pdf.

[37] A list of convictions of inmates and former inmates is available in New York State's Inmate Population Information Search, available at http://nysdoccslookup.doccs.ny.gov/. See also N.Y. Correction Law § 9. In addition, New York State has a public sex offender registry. See New York State Division of Criminal Justice Services, Sex Offender Registry, available at https://www.ny.gov/services/search-sex-offender-registry.

[38] N.Y. Exec. Law § 845-b. Criminal history information may be disclosed only for limited purposes, such as related to the granting of a license.

[39] Kerri McGowan Lowrey, "Data Sharing Guidance for School Nurses," The Network for Public Health Law, January 23, 2020, available at https://www.networkforphl.org/resources/data-sharing-guidance-for-school-nurses/; Kerri McGowan Lowrey, "Data Privacy in School Nursing: Navigating the Complex Landscape of Data Privacy Laws (Part I)," The Network for Public Health Law, June 19, 2019, available at https://www.networkforphl.org/resources/data-privacy-in-school-nursing-navigating-the-complex-landscape-of-data-privacy-laws-part-i/; Kerri McGowan Lowrey, "Data Privacy in School Nursing: Navigating the Complex Landscape of Data Privacy Laws (Part II)," The Network for Public Health Law, January 23, 2020, available at https://www.networkforphl.org/resources/data-privacy-in-school-nursing-navigating-the-complex-landscape-of-data-privacy-laws-part-ii/.

[40] 45 C.F.R. § 164.506(c)(2). See also Department of Health and Human Services Office of Civil Rights, Does the HIPAA Privacy Rule allow a healthcare provider to disclose PHI about a student to a school nurse or physician?, available at https://www.hhs.gov/hipaa/for-professionals/faq/517/does-hipaa-allow-a-health-care-provider-to-disclose-information-to-a-school-nurse/index.html.

[41] 42 C.F.R. § 2.14.

[42] 42 C.F.R. § 2.31(a)(4)(iii)(B)(3).

[43] FERPA applies to health records maintained by schools that receive federal educational funds, and nearly all public schools receive such funds. If a school health record is subject to FERPA, it is not considered PHI under HIPAA. See Joint Guidance on the Application of the Family Educational Rights and Privacy Act (FERPA) and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) to Student Health Records Q6, available at https://www.hhs.gov/hipaa/for-professionals/faq/517/does-hipaa-allow-a-health-care-provider-to-disclose-information-to-a-school-nurse/index.html.

[44] 34 C.F.R. §§ 99.30(b), 99.31. The regulations do not specify whether a FERPA consent can be combined with a consent that allows disclosures of other types of information, such as Part 2 information. One consent form may allow disclosure to multiple recipients; the form must specify the records to be disclosed, state the purpose of the disclosure, and identify the recipient or class of recipients.

[45] 7 U.S.C. § 2020(e)(8)(F), (u); 42 U.S.C. § 1758(b)(3)(F)(i)(I); 7 C.F.R. § 272.1(c)(1)(viii). The law also permits disclosures to state agencies that administer meal programs.

[46] 42 U.S.C. §§ 1396a(a)(7)(B), 1758(b)(3)(F)(i)(IV).

[47] 42 C.F.R. §§ 164.502(b), 164.512(k)(6)(i).

[48] CMS, United States Department of Agriculture (USDA) Demonstration Project to Test Using Medicaid Enrollment to Qualify Children for Free and Reduced Price School Meals (Feb. 12, 2016), available at https://www.medicaid.gov/federal-policy-guidance/downloads/CIB-02-12-16.pdf.

[49] 42 U.S.C. § 1758(b)(3)(F)(i)(I). This differs from many other federal privacy laws such as HIPAA. Under HIPAA, for example, federal law permits disclosure without consent for purposes of treatment, but it does not give providers a right to obtain PHI for purposes of treatment, and therefore state law can be more stringent and mandate consent. In contrast, federal law here gives school districts the right to obtain SNAP data to verify eligibility for meal programs, so if a state law prohibited such disclosure, it would interfere with a right set forth under federal law.

[50] See, e.g., N.Y. Educ. Law § 2-d.

[51] Cal. Educ. Code § 49075(a).

[52] La. Admin. Code tit. 48, §§ 505(G), 507(A).

[53] La. Admin. Code tit. 46, § 115.

[54] La. Stat. § 17:3914(C)(1).

[55] 42 U.S.C. § 1396a(a)(7)(A); 42 C.F.R. § 431.302(a).

[56] 42 C.F.R. § 431.306(d).

[57] 45 C.F.R. § 164.506(c)(2).

[58] 45 C.F.R. §§ 164.501, 164.506(c)(3).

[59] 45 C.F.R. § 164.514(d)(3).

[60] 28 C.F.R. §§ 20.3(q); 20.21(b), (f)(4)(v).

[61] Department of Health and Human Services Office of Civil Rights, Does HIPAA permit health care providers to share PHI about an individual with mental illness with a third party that is not a health care provider for continuity of care purposes?, available at https://www.hhs.gov/hipaa/for-professionals/faq/3008/does-hipaa-permit-health-care-providers-share-phi-individual-mental-illness-third-party-not-health-care-provider-continuity-care-purposes/index.html.

[62] Cal. Welf. & Inst. Code § 14100.2; La. Admin. Code tit. 67, § 101(B)(15); N.Y. Soc. Servs. Law § 369(4).

[63] See San Diego County Sheriff's Department, Sheriff's Who Is in Jail, available at https://apps.sdsheriff.net/wij/wij.aspx; New York State Department of Corrections and Community Supervision, Inmate Population Information Search, available at http://nysdoccslookup.doccs.ny.gov/. Louisiana provides a phone number where callers can obtain an inmate's release date. See Louisiana Department of Public Safety & Corrections, Supporting Offenders & Their Families, available at https://doc.louisiana.gov/offender-programs-resources/offender-information/.

[64] The Louisiana Department of Health, Department of Health, and Department of Corrections team up to provide health care coverage for newly released offenders (March 1, 2017), available at http://ldh.la.gov/index.cfm/newsroom/detail/4170.

[65] Cal. Civ. Code § 56.10(c)(1).

[66] La. Admin. Code tit. 48, §§ 507, 509.

[67] La. Admin. Code tit. 46, § 115.

[68] 45 C.F.R. § 164.501.

[69] 42 U.S.C. §§ 1396a(a)(7).

[70] Generally, an organization that is involved in the administration of a Medicaid program must enter into a contract with the state Medicaid agency to adequately secure the data received. 42 C.F.R. § 431.306(g). Since the MCO already is contractually required to keep Medicaid beneficiary data secure, it is possible the state Medicaid agency may conclude that the existing contract is sufficient.

[71] In addition, if the disclosure included income information that originated from the Internal Revenue Service (IRS) or Social Security Administration (SSA), CMS or the state Medicaid agency would need to find that the disclosure to the MCO was consistent with its statutory obligation to safeguard the information received in accordance with IRS and SSA requirements. 42 C.F.R. § 431.305(b)(6).

[72] 45 C.F.R. § 164.501.

[73] "State and Implementing Agencies must establish a data exchange agreement before data can be shared." United States Department of Agriculture, FY2020 SNAP-ED Plan Guidance, at 27, https://snaped.fns.usda.gov/sites/default/files/documents/SNAP-Ed%20Plan%20Guidance%20FY%202020%20Complete.pdf. See also 7 C.F.R. § 272.1(c)(2).

[74] 7 U.S.C. § 2020(e)(8)(A); 7 C.F.R. § 272.1(c)(1)(i).

[75] United States Department of Agriculture, FY2020 SNAP-ED Plan Guidance, at 27, https://snaped.fns.usda.gov/sites/default/files/documents/SNAP-Ed%20Plan%20Guidance%20FY%202020%20Complete.pdf.

[76] Cal. Welf. & Inst. Code § 14100.2 (Medicaid); California Department of Social Services, Food Stamp Regulations § 63-201.311 (SNAP), available at https://www.cdss.ca.gov/inforesources/calfresh/regulations-and-policy-guidance. California's Information Practices Act permits state agencies to disclose personal information if the disclosure is compatible with a purpose for which the information is collected; arguably that standard would be met here. Cal. Civ. Code § 1798.24.

[77] La. Admin. Code tit. 67, §§ 101 (applying to both SNAP and Medicaid), 103, 1927 (SNAP only); 18 N.Y.C.R.R. § 387.2(j) (SNAP); N.Y. Soc. Servs. Law § 369(4) (Medicaid).

[78] N.Y. Soc. Servs. Law § 95-a(2).

[79] These agencies could attempt to obtain consent from their beneficiaries when they enroll in the applicable program.

[80] As noted earlier, the Part 2 regulations regarding consent form requirements may be revised in light of the passage of the CARES Act.

[81] Arguably, a form that expires at the earlier of a specific future date or a particular event might comply with this rule.

[82] "De-identification of Data," The Network for Public Health Law, available at https://www.networkforphl.org/resources/topics/health-information-and-data-sharing/de-identification-of-data/.

manatt

Albany
Boston
Chicago
Los Angeles
New York
Orange County
Palo Alto
Sacramento
San Francisco
Washington, D.C.