



**Congressional
Research Service**

Informing the legislative debate since 1914

Privacy Protections for Individuals with Substance Use Disorders: The Part 2 Final Rule in Brief

Amanda K. Sarata
Specialist in Health Policy

C. Stephen Redhead
Specialist in Health Policy

June 18, 2018

Congressional Research Service

7-5700

www.crs.gov

R44790

Summary

On January 18, 2017, the Secretary of Health and Human Services (HHS) published a final rule to amend the federal regulations known as “Part 2” that protect the privacy of patient records maintained by alcohol and drug treatment programs across the country. Part 2 was developed in the 1970s to allay the concerns of individuals with substance use disorders who were afraid to get treatment for fear that their medical information would be released, leading to discrimination and even prosecution.

Health care providers participating in new health care delivery models such as accountable care organizations (ACOs), which rely on sharing medical information to coordinate and integrate patient care, complain that Part 2 restricts their ability to access important medical data.

Disclosure of Part 2 Data

Disclosure of Part 2-covered data generally requires a patient’s written consent unless the type of disclosure falls under one of a handful of statutory exceptions. Consent is needed for a clinician to release patient information to another health care facility to improve the coordination of care. This requirement contrasts with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, which applies more broadly to medical information throughout the health care system, and which permits health care providers to share patient data with few restrictions.

Alcohol and drug treatment programs typically are subject to both Part 2 and the Privacy Rule unless there is a conflict between the two. In that case, the program must comply with the regulations that are more protective of privacy, which generally means following Part 2.

Changes in the Final Rule

The final rule was developed by the HHS Substance Abuse and Mental Health Services Administration (SAMHSA). According to SAMHSA, the changes in the final rule are intended primarily to facilitate the sharing of Part 2 data among providers participating in clinically integrated health care networks that include addiction treatment programs.

The final rule introduced flexibility to the Part 2 consent process. It provided patients with more options for designating the types of individuals and entities that may receive protected information. A patient may now consent to disclose Part 2 data to an organization such as an ACO or health information exchange (HIE) that does not have a direct treatment relationship with the patient, but which acts as an intermediary. The intermediary may then disclose the information to some or all of the providers who treat the patient, pursuant to the patient’s consent preferences.

Groups that advocate for the privacy of individuals with substance use disorders generally are satisfied with the final rule because it retains Part 2’s core confidentiality protections. But the reaction of many health care provider organizations has been mixed. While applauding the changes that permit disclosure of Part 2 data to intermediaries such as ACOs and HIEs, providers are critical of other changes that they claim are administratively and technologically burdensome and provide little if any additional privacy protections.

Exchange of Part 2 Data

To facilitate the electronic exchange of Part 2 data, each patient’s consent preferences specifying the type of information that may be shared, and the individuals or entities with whom the information may be shared, must be carefully managed. To control access, patient consent must travel with the data. In addition, the data in a medical record must be segregated to capture a patient’s preferences. Data segmentation allows a patient’s record to be separated into multiple

categories, so that certain protected data elements can be removed (redacted) if a patient has not consented to their disclosure.

SAMHSA has worked with its federal and nonfederal partners to develop Consent2Share, an online tool for data segmentation and consent management. Consent2Share integrates with electronic health record systems and HIEs to support the exchange of Part 2 and other sensitive health data.

Contents

Protecting Privacy in an Evolving Health System.....	1
More Protective Than HIPAA	2
Closer Look at the Final Rule.....	6
Type of Information Disclosed.....	6
General Disclosures	6
Redisclosure	7
Medical Emergencies	7
Electronic Records	7
Research	8
Audit and Evaluation.....	8
Qualified Service Organizations (QSOs)	8
Prescription Drug Monitoring Programs (PDMPs).....	9
SAMHSA Finalizes Additional Changes to Part 2	9
Stakeholder Reaction Has Been Mixed	9
New Technologies Support Part 2 Data Exchange	11
Consent2Share.....	11
Opioid Treatment Program (OTP) Service Continuity Pilot	11

Tables

Table 1. Comparison of the HIPAA Privacy Rule and the Part 2 Regulations	4
--	---

Contacts

Author Contact Information	12
----------------------------------	----

Protecting Privacy in an Evolving Health System

On January 18, 2017, the Secretary of Health and Human Services (HHS) published a final rule that amends the federal regulations responsible for safeguarding the privacy of patient records maintained by substance use disorder treatment programs across the country.¹ These regulations, known simply as Part 2 after their location in the Code of Federal Regulations, were first promulgated in 1975 and had not been revised substantively since 1987.²

According to the HHS Substance Abuse and Mental Health Services Administration (SAMHSA), which administers Part 2, the changes in the final rule are intended “to better align [Part 2] with advances in the U.S. health care delivery system while retaining important privacy protections.”³

The Part 2 law and implementing regulations were written at a time when treatment for substance use disorders was offered primarily by specialty providers. Some individuals with substance use disorders, however, were reluctant to seek treatment because they feared that disclosure of information about their condition might lead to prosecution, discrimination by health insurers, or loss of employment, housing, or child custody. The aim of Part 2 was to encourage these individuals to get the treatment they needed by establishing strong privacy protections.

Today, the health care system is embracing new models for delivering services—including accountable care organizations (ACOs) and patient-centered health homes—that rely on sharing patient information to coordinate and integrate care. There is also a focus on measuring performance and patient outcomes. These efforts, in turn, depend on use of electronic health records (EHRs) and the development of a health information technology (HIT) infrastructure to support the exchange and use of digital health information.

Under Part 2, the disclosure of substance use disorder treatment records requires a patient’s written consent, unless the type of disclosure falls under one of a handful of specific statutory exceptions. For example, Part 2 generally requires consent to release information about a patient’s substance use disorder history and treatment regimens to clinicians at another facility, except in the case of a medical emergency. This contrasts with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, which permits clinicians to share patient information for treatment and payment purposes.

Health care providers have become increasingly frustrated with the restrictions that Part 2 places on their ability to share the medical records of patients with substance use disorders. They argue that Part 2 makes it difficult for addiction treatment providers and general medicine providers to exchange information and coordinate patient care.

Consider a patient who receives counseling and medications at an alcohol or drug treatment program. The records for this care are protected under Part 2. If the patient also receives treatment (including addiction treatment) at a primary care facility, the records for the care at that location are HIPAA-protected. Whereas the primary care facility is permitted under HIPAA to share the patient’s information with the Part 2-covered alcohol and drug treatment program and any other

¹ Department of Health and Human Services, Office of the Secretary, “Confidentiality of Substance Use Disorder Patient Records,” 82 *Federal Register* 6052, January 18, 2017.

² The regulations, which are codified at 42 C.F.R. Part 2 (“Confidentiality of Substance Use Disorder Patient Records”), implement Section 543 of the Public Health Service Act, 42 U.S.C. §290dd–2 (“Confidentiality of Records”).

³ 82 *Federal Register* 6053.

health care facility providing care, the alcohol and drug treatment program generally needs the patient's consent under Part 2 to release information to another health care facility.

Integrated health systems that handle patient records from multiple providers must separate Part 2 data from other medical information and manage patient consent preferences for its use and disclosure. Some health information exchanges (HIEs) exclude Part 2 data altogether because of the difficulty and expense of segregating the data and managing consent.

Researchers, too, have expressed concern about access to Part 2 data. They were especially critical of a decision by the HHS Centers for Medicare & Medicaid Services (CMS) in late 2013 to begin withholding from research data sets any Medicare or Medicaid reimbursement claim that included a substance use disorder diagnosis or procedure code.⁴

CMS took this action to comply with Part 2. While the regulations permit disclosures for research purposes, subject to certain conditions, only substance use disorder program directors are allowed to authorize such disclosures. Third-party payers that receive Part 2 data, including CMS, are subject to the general prohibition on redisclosing the information. Researchers complained that they were losing access to an important data source at a particularly challenging time, as the nation expands its efforts to combat the abuse of prescription opioids and heroin.

SAMHSA launched its effort to revise Part 2 in response to these concerns. Its stated goal in developing the final rule was to ensure that individuals with substance use disorders are able to participate in, and benefit from, the new systems of care without compromising their privacy.

This report summarizes the changes that the final rule made to the Part 2 regulations and describes stakeholders' reactions to these revisions. The report begins with an overview and comparison of Part 2 and the HIPAA Privacy Rule. It concludes with some discussion of new HIT standards and applications for data segmentation and consent management that support the exchange of Part 2 data.

More Protective Than HIPAA

Part 2 is much narrower in scope than the more familiar HIPAA Privacy Rule,⁵ which provides a baseline of privacy protections for health information maintained by payers and providers of health care—including substance use disorder treatment programs subject to Part 2—across the entire health care system. Part 2 also permits significantly fewer uses and disclosures of patient information without consent. **Table 1** compares key provisions of the Privacy Rule and Part 2.

The HIPAA Privacy Rule applies to identifiable health information maintained by health plans, health care clearinghouses, and health care providers.⁶ It also applies to the business associates of

⁴ Austin B. Frakt and Nicholas Bagley, "Protection or Harm? Suppressing Substance-Use Data," *New England Journal of Medicine*, vol. 372, no. 20 (May 14, 2005), pp. 1879-1881.

⁵ The HIPAA Privacy Rule was published on December 28, 2000 (65 *Federal Register* 82461), and is codified at 45 C.F.R. Part 164, Subpart E. For more detail information about the Privacy Rule, see CRS Report R43991, *HIPAA Privacy, Security, Enforcement, and Breach Notification Standards*.

⁶ A health plan is "an individual or group plan that provides, or pays the cost of, medical care." The term encompasses private and government plans. A health care clearinghouse is an entity (e.g., billing service) that (1) receives nonstandard health information and processes, or facilitates the processing of, the information into a standard format required for electronic transaction; or (2) receives a standard transaction and processes, or facilitates the processing of, the information into nonstandard format for the recipient. A health care provider is a person (e.g., physician, nurse) or entity (e.g., hospital, clinic) that "furnishes, bills, or is paid for health care in the normal course of business." For HIPAA to apply, a provider must conduct one or more HIPAA-specified standard electronic transactions such as billing and claims processing. Providers who rely on third-party billing services to conduct such electronic transactions on (continued...)

these HIPAA-covered entities, with whom such protected health information (PHI) is shared. Business associates provide specific services (e.g., claims processing, data management) for covered entities to help them operate as businesses and meet their responsibilities to patients and beneficiaries.

The Privacy Rule describes multiple circumstances under which covered entities may use or disclose PHI. For example, PHI may be used or disclosed for the purposes of treatment, payment, and other routine health care operations—including case management, care coordination, and outcomes evaluation—with few restrictions.⁷ The rule also permits the use or disclosure of PHI for other specified purposes not directly connected to the treatment of the individual, such as public health and research.⁸ Covered entities must obtain a patient’s written authorization for any use or disclosure that is not expressly permitted or required under the Privacy Rule.⁹

By comparison, Part 2 applies specifically to federally assisted substance use disorder treatment programs.¹⁰ Most of the nation’s alcohol and drug treatment programs are covered, comprising more than 12,000 hospitals, outpatient treatment centers, and residential treatment facilities. While Part 2 does not apply to general medical facilities or practices, it does cover specialized substance use disorder treatment units (and staff) within such facilities.¹¹

Part 2 restricts the use or disclosure of any patient information that directly identifies a patient as an alcohol or drug abuser, or that links the patient to an alcohol or drug treatment program.¹² Medical information that does not link the patient to current or past substance abuse, or identify the patient as a participant of a Part 2 program, is not subject to the Part 2 requirements. While such information is not afforded Part 2 protection, it remains covered under the HIPAA Privacy Rule.

Under Part 2, patient-identifying information may not be disclosed without a patient’s written consent except pursuant to certain specified conditions in the following circumstances: (1) medical emergencies, (2) research, (3) program audits and evaluations, and (4) pursuant to a court order authorizing disclosure.¹³ Any information disclosed with the patient’s consent must include a statement that prohibits further disclosure of identifying information unless the consent expressly permits such redisclosure, or it is permitted by Part 2.¹⁴

Substance use disorder treatment programs typically are subject to both sets of regulations—Part 2 and the HIPAA Privacy Rule—unless there is a conflict between the two. In that case, the program must comply with the regulations that are more protective of patient privacy, which generally means following the requirements under Part 2.

(...continued)

their behalf are also covered. However, a provider who operates solely on a paper basis and does not submit insurance claims electronically is not subject to the Privacy Rule. 45 C.F.R. §160.103.

⁷ 45 C.F.R. §164.506.

⁸ 45 C.F.R. §164.512.

⁹ 45 C.F.R. §164.508(a).

¹⁰ 42 C.F.R. §2.12(b).

¹¹ 42 C.F.R. §2.11 (definition of “Program”).

¹² 42 C.F.R. §2.12(a).

¹³ 42 C.F.R. Part 2, Subparts D & E.

¹⁴ 42 C.F.R. §2.32.

Table I. Comparison of the HIPAA Privacy Rule and the Part 2 Regulations

	HIPAA Privacy Rule	Part 2
Who is covered?	<p>The Privacy Rule applies to health plans (public and private), health care clearinghouses, and health care providers—collectively referred to as covered entities. It also applies to business associates of covered entities (i.e., consultants and companies hired by covered entities to help them operate as a business and meet their responsibilities to patients and beneficiaries). Business associates provide claims processing, billing, legal, actuarial, accounting, transcription, data management, peer review, quality review, and financial services, among others, for which they need access to PHI.</p>	<p>Part 2 applies to any individual or entity (other than a general medical facility) that is federally assisted and provides diagnosis, treatment, or referral for treatment of substance use disorders. Part 2 programs include specialized substance use disorder treatment units (and staff) within general medical facilities. An individual or entity is federally assisted if it is authorized, licensed, certified, registered by the federal government, or receives any federal funds.</p>
What is covered?	<p>The Privacy Rule covers protected health information (PHI) created or received by covered entities and their business associates. PHI is individually identifiable information in any form or format that relates to an individual’s past, present, or future physical or mental health; the provision of health care to an individual; and the past, present, or future payment for that care.</p>	<p>Part 2 covers patient records in paper or electronic form disclosed by a Part 2 program that identify the individual—directly or indirectly—as having or having had a substance use disorder, or as being a participant in a Part 2 program.</p> <p>Note: Part 2 does not apply to records on substance use disorder patients maintained by the Department of Veterans Affairs. The privacy of those veterans’ records are governed by 38 U.S.C. §7332.</p>
What types of uses and disclosures are permitted without consent?	<p>Covered entities may use or disclose PHI for the purposes of treatment, payment, and a broad range of health care operations, with few restrictions. Under certain other circumstances (e.g., disclosures to family members and friends), the rule requires covered entities to give the individual the opportunity to object (i.e., opt out), in which case the use or disclosure is prohibited.</p> <p>The rule also permits the use or disclosure of PHI under other circumstances, and for other specified purposes, that are not directly connected to the treatment of the individual. For example, PHI may be used or disclosed, subject to other specified conditions, for public health and health oversight activities; judicial and administrative proceedings (pursuant to a court order, subpoena, or other lawful process); law enforcement (pursuant to a court order, court-ordered warrant, or subpoena, and under certain other situations); research; organ and tissue donation; and to avert serious threats to health and safety. Finally, PHI may be used or disclosed if such use or disclosure is required by (federal or state) law.</p>	<p>Part 2 programs may disclose patient identifying information (1) to medical personnel in a bona fide medical emergency; (2) to qualified researchers, provided the research is subject to the Privacy Rule and/or the Common Rule; (3) to qualified organizations and persons who are conducting a program audit or evaluation, provided certain safeguards are met; and (4) in response to a subpoena, provided a court has issued an order authorizing disclosure that complies with the requirements of Part 2.</p> <p>Note: The Part 2 restrictions on disclosure do not apply (1) to communications among personnel within a Part 2 program—regarding patient diagnosis, treatment, or referral for treatment—or between a Part 2 program and an entity that has direct administrative control over the program; (2) to communications between a Part 2 program and a qualified service organization (QSO) that provides services to the program; (3) to communications between a Part 2 program and law enforcement personnel regarding crimes on program premises or against program personnel; and (4) to reporting incidents of suspected child abuse and neglect pursuant to state law.</p>

	HIPAA Privacy Rule	Part 2
What types of uses and disclosures require consent?	Covered entities are prohibited from using or disclosing PHI except as expressly permitted or required by the rule (see above). All uses or disclosures of PHI that are not otherwise permitted or required by the rule require an individual's prior written authorization.	Part 2 programs must obtain a patient's written consent to disclose identifying information unless the disclosure falls under one of the statutory exceptions (see above).
Are recipients of a disclosure permitted to further disclose the information?	If the recipient of PHI is a HIPAA-covered entity (or business associate), then the Privacy Rule continues to apply to the use or disclosure of the information by that entity. However, if the recipient is not a HIPAA-covered entity (or business associate), then the Privacy Rule no longer applies.	Under Part 2, each disclosure made with a patient's consent must be accompanied by a written statement that prohibits the recipient from making any further disclosure of the information, unless such redisclosure is expressly permitted by the consent or is otherwise permitted under Part 2.
How much information may be used or disclosed?	Generally, but with some exceptions, covered entities must limit the use or disclosure of PHI to the extent practicable to the minimum amount necessary to accomplish the intended purpose of the use or disclosure.	Any disclosure made under Part 2 must be limited to that information which is necessary to carry out the purpose of the disclosure.
Do individuals have access to their health information?	The Privacy Rule gives individuals the right of access to inspect and obtain a copy of their PHI, or have a copy transmitted to a designated third party.	Part 2 programs are permitted to give patients access to inspect and obtain a copy of their records.
Must individuals be informed about their health privacy?	Covered entities are required to provide each individual with a written notice that describes the permitted uses and disclosures of PHI, the individual's rights, and covered entities' legal responsibilities for safeguarding PHI.	Part 2 programs are required to provide each patient with a written summary of the purpose and provisions of the Part 2 law and regulations.
Is information security addressed?	The Privacy Rule requires covered entities and business associates to adopt reasonable administrative, technical, and physical safeguards to protect PHI from any intentional or unintentional use or disclosure in violation of the rule. (The HIPAA security rule specifies a series of standards for those safeguards.)	Part 2 programs and others in lawful possession of patient identifying information—both paper and electronic records—must adopt policies and procedures to reasonably protect against unauthorized uses and disclosures of such information, and to protect against reasonably anticipated security threats or hazards.
Are state health privacy laws preempted?	The Privacy Rule does not preempt state laws that are more protective of privacy (i.e., laws that prohibit or restrict a use or disclosure that would otherwise be permitted under the privacy rule, or that provide individuals with greater access to their information).	Part 2 does not preempt state laws that prohibit a disclosure that would otherwise be permitted under Part 2.

Source: Prepared by CRS based on the text of the HIPAA Privacy Rule (i.e., 45 C.F.R. Part 164, Subpart E) and the Part 2 final rule (42 C.F.R. Part 2).

Closer Look at the Final Rule

The major provisions in the final rule are summarized below. Although SAMHSA’s primary goal was to modify Part 2 to facilitate the sharing of patients’ Part 2 data with other providers participating in clinically integrated health care networks, the agency’s rulemaking options were constrained by the underlying statutory language.

The Part 2 law is prescriptive, which limits SAMHSA’s ability to make significant changes through rulemaking. The law defines the types of entities and information subject to its protections. It requires patient consent to disclose protected information, except in a handful of specified circumstances, and it establishes a strict prohibition on redisclosure.

By contrast, the HHS Secretary was given broad discretionary authority under HIPAA to develop—and periodically amend—the Privacy Rule. HIPAA instructed the Secretary to submit to Congress detailed recommendations on the privacy of individually identifiable health information, and to promulgate privacy standards based on the recommendations. The law provided few details on the scope of the recommendations other than specifying that they must address (1) patient rights, (2) procedures for exercising such rights, and (3) the uses and disclosures of patient information that should be permitted or required.¹⁵

Type of Information Disclosed

The final rule modifies the Part 2 requirement that consent forms include the amount and kind of information to be disclosed. It specifies that the form must now include “an explicit description of the substance use disorder information that may be disclosed.”¹⁶ According to SAMHSA, the types of information that could be specified include diagnostic information, medications, lab tests, history of substance use, employment information, social supports, and claims or encounter data. Patients may select “all my substance use disorder information” as long as the consent form includes more specific types of disclosures from which to choose.¹⁷

General Disclosures

Part 2 traditionally has required patient consent forms to identify “the name or title of the individual or the name of the organization to which the disclosure is made.”¹⁸ Under the final rule, more options are available. A patient can now list any of the following in the “to whom” section of the consent form:

- the name of an individual;
- the name of an entity (e.g., hospital, clinic, physician practice) that has a “treating provider relationship”¹⁹ with the patient;

¹⁵ HIPAA Section 264, 42 U.S.C. §1320d–2 note. The law also stipulated that the privacy standards do not preempt (i.e., supersede) contrary state laws that are more protective of health information.

¹⁶ 42 C.F.R. §2.31(a)(3).

¹⁷ 82 *Federal Register* 6086.

¹⁸ 42 C.F.R. §2.31(a)(2), prior to amendment by the final rule.

¹⁹ A treating provider relationship is one in which “[a] patient is, agrees to, or is legally required to be diagnosed, evaluated, and/or treated ... for any condition by an individual or entity [that] undertakes or agrees to undertake diagnosis, evaluation, and/or treatment of the patient....” 2 C.F.R. §2.11 (Definitions).

- the name of an entity with which the patient does not have a treating provider relationship and which is a third-party payer; and/or
- the name of an entity with which the patient does not have a treating provider relationship and which is not a third-party payer (e.g., ACO, health information exchange, research institution), plus either
 - the name(s) of specific individual participants;
 - the name(s) of an entity participant(s) with which the patient has a treating provider relationship; or
 - a general designation of individual or entity participants, or class of participants, with which the patient has a treating provider relationship (e.g., “all my past, present, and future treating providers”).²⁰

Thus, a patient may now consent to disclose Part 2 data to an organization such as a health information exchange (HIE) that does not have a treating provider relationship with the patient, but which acts as an intermediary. Pursuant to the patient’s general designation, the intermediary may further disclose the information, but only to providers that it can verify have a treating provider relationship with the patient.

The final rule also creates the right to an accounting of disclosures. Patients who provide consent using the general designation are entitled, upon written request, to receive from the intermediary a list of entities to which their information has been disclosed within the past two years.²¹

Redisclosure

The final rule modifies the written statement prohibiting redisclosure that accompanies Part 2 disclosures made with a patient’s consent. The modified language states that the prohibition on redisclosure applies only to information that identifies, directly or indirectly, an individual as having or having had a substance use disorder. That includes not only clinical information, such as diagnoses, treatments, and referrals, but also the origin of the data (such as a treatment clinic) if it reveals that the individual has a substance use disorder.²²

Medical Emergencies

The final rule modifies the regulatory language so that it aligns with the statutory definition of medical emergency. The revised language states that patient-identifying information may be disclosed to medical personnel “to the extent necessary to meet a bona fide medical emergency in which the patient’s prior informed consent cannot be obtained.” The final rule continues to require a Part 2 program, immediately following disclosure, to document specific information related to the medical emergency.²³

Electronic Records

The final rule revises the existing security language by specifying that Part 2 programs and other lawful holders of patient-identifying information must adopt policies and procedures to protect

²⁰ 42 C.F.R. §2.31(a)(4).

²¹ 42 C.F.R. §2.31(a)(4)(iii)(B)(3).

²² 42 C.F.R. §2.32.

²³ 42 C.F.R. §2.51.

both paper and electronic records “against unauthorized uses and disclosures” and “against reasonably anticipated threats or hazards” to the security of such information.²⁴ The policies and procedures for electronic records must address creating, receiving, and transmitting such records; destroying records and sanitizing the electronic media on which such records are stored; and rendering patient identifying information nonidentifiable, among other things.

Research

The final rule eases the restrictions on disclosures for research purposes by allowing a Part 2 program or other lawful holder of Part 2 information²⁵—not just Part 2 program directors—to disclose the information to qualified researchers, provided the researchers (1) have obtained approval from an Institutional Review Board (IRB) or equivalent privacy board under the HIPAA Privacy Rule and/or the Common Rule;²⁶ (2) agree to be fully bound by Part 2; and (3) if necessary, resist in judicial proceedings any efforts to obtain access to the data except as permitted under Part 2.²⁷

The final rule also permits researchers using Part 2 data to link to data sets in federal and nonfederal data repositories, provided that the linkage has been reviewed and approved by an IRB.²⁸

Audit and Evaluation

Part 2 permits the disclosure of patient-identifying information to certain qualified persons who are conducting a program audit or evaluation, provided that certain safeguards are met. The final rule revises and expands the existing language so that ACOs and other CMS-regulated entities are able to access Part 2 data to perform necessary audit and evaluation activities, including financial and quality assurance reviews.²⁹

Qualified Service Organizations (QSOs)

Part 2 permits the disclosure of patient-identifying information to a QSO, subject to a written agreement. The final rule adds population health management to the list of examples of services that may be provided by a QSO.³⁰ SAMHSA defines population health management as “increasing desired health outcomes and conditions through monitoring and identifying individual patients within a group.”³¹ It emphasizes that disclosures for population health management under

²⁴ 42 C.F.R. §2.16.

²⁵ A lawful holder of Part 2 patient-identifying information is an individual or entity that has received such information as a result of a Part 2-compliant patient consent (accompanied by a written statement prohibiting redisclosure) or as permitted under the Part 2 law or regulations.

²⁶ The Common Rule is the informal name for the uniform set of federal regulations that govern the ethical conduct of research involving human subjects. Under the Common Rule, research protocols must be approved by an IRB to ensure that the rights and welfare of research subjects are protected. See 45 C.F.R. Part 46, Subpart A.

²⁷ 42 C.F.R. §2.52(a)-(b).

²⁸ 42 C.F.R. §2.52(c).

²⁹ 42 C.F.R. §2.53.

³⁰ QSO services include “data processing, bill collecting, dosage preparation, laboratory analyses, or legal, accounting, population health management, medical staffing, or other professional services, or services to prevent or treat child abuse or neglect, including training on nutrition and child care and individual and group therapy....” 42 C.F.R. §2.11 (Definitions).

³¹ 82 *Federal Register* 6066.

a QSO agreement must be limited to the specific offices or units responsible for carrying out these activities. The agency does not consider care coordination or medical management to be population health management because they both include a patient treatment component.

Prescription Drug Monitoring Programs (PDMPs)

SAMHSA decided not to address electronic prescribing and state PDMPs in its Part 2 rulemaking. This is a notable omission given the potential importance of PDMPs in combatting the abuse and diversion of controlled prescription drugs such as opioid painkillers. PDMPs collect, monitor, and analyze prescribing and dispensing data submitted electronically by pharmacies and other drug dispensers.³²

Because of the prohibition on redisclosure, a pharmacy that receives an e-prescription from a Part 2 program must obtain patient consent to transmit the information to a PDMP. Patient consent is also required for the PDMP to redisclose that information to others with access to the PDMP.

While recognizing the importance of PDMPs, SAMHSA concluded that these issues are not yet ripe for rulemaking in part because pharmacy data systems currently do not have the ability to manage patient consent or segregate Part 2 data from other prescription information.

SAMHSA Finalizes Additional Changes to Part 2

SAMHSA also published a supplemental final rule in January 2018 that makes additional changes to Part 2 to permit third parties in lawful possession of Part 2 data to disclose the information to their contractors, subcontractors, and legal representatives.³³ The agency finalized two sets of circumstances under which such disclosures would be permissible.

First, if a patient consents to disclosure of his or her Part 2 records for payment and/or health care operations activities, the recipient of the information (i.e., lawful holder) is able to further disclose the information to its contractors, subcontractors, or legal representatives to carry out such activities on its behalf. Any entity that receives data from a lawful holder in this way would itself become a lawful holder and be subject to the Part 2 requirements. SAMHSA includes a list of permissible payment and health care operations activities, which is similar to the HIPAA Privacy Rule's definition of these terms, in the preamble of the rule to provide illustrative examples of these types of activities.

Second, the final rule allows an individual and entity to whom Part 2 data are disclosed for a Medicare, Medicaid, or State Children's Health Insurance Program (CHIP) audit or evaluation to further disclose the information to its contractors, subcontractors, or legal representatives to carry out the audit or evaluation.

Stakeholder Reaction Has Been Mixed

Groups that advocate for the privacy of individuals with substance use disorders generally are satisfied with the final rule because it retains Part 2's confidentiality protections. But

³² For more information, see CRS Report R42593, *Prescription Drug Monitoring Programs*.

³³ Department of Health and Human Services, Substance Abuse and Mental Health Services Administration, "Confidentiality of Substance Use Disorder Patient Records," 83 *Federal Register* 239, January 3, 2018.

organizations that represent payers and providers of health care have criticized the final rule, claiming that on balance it does little to improve information sharing.

The Legal Action Center, a nonprofit law and policy organization representing people with substance use disorders, HIV/AIDS, or criminal records, notes that while the final rule has introduced flexibility to the consent process by providing more options for designating the types of individuals and entities permitted to receive protected information, the core consent requirements under Part 2 remain intact and in other respects have been strengthened. The center applauds the new provision that allows patients to indicate on the consent form the specific types of information that may be disclosed. It also credits SAMHSA for not attempting to loosen the prohibition on redisclosure or to create any new exceptions to the consent requirement.³⁴

The Partnership to Amend 42 C.F.R. Part 2 (the Partnership)—a coalition of national organizations representing health care payers and providers committed to aligning Part 2 with the HIPAA Privacy Rule—has been critical of the final rule. Though the Partnership acknowledges SAMHSA’s efforts to broaden the consent options in an attempt to facilitate the use and disclosure of Part 2 data for research, population health management, and care coordination, it believes more needs to be done to enable Part 2 data to be shared. The Partnership recognizes, however, that SAMHSA’s rulemaking options are limited by the underlying statute—as discussed earlier—and thus more fundamental changes to Part 2 may require new legislation to amend the law.³⁵

Representatives of the behavioral health provider and medical informatics communities support the final rule’s general consent provisions that permit disclosure of Part 2 data to intermediaries such as HIEs and ACOs. But they are critical of the language that will require such intermediaries to have the IT capability to (1) limit access to Part 2 data to providers involved in the patient’s care (i.e., those with a “treating provider relationship”) and (2) be able to track which providers have received Part 2 data so that an accounting of such disclosures within the past two years can be provided to the patient upon request.³⁶ They argue that these requirements are administratively and technologically burdensome and provide little if any additional privacy protections.³⁷

A provision in the 21st Century Cures Act requires the HHS Secretary, not later than one year after first finalizing regulations to update Part 2, to convene stakeholders to determine the final rule’s effects on patient care, health outcomes, and patient privacy.³⁸ On January 31, 2018, SAMHSA held a listening session to implement this requirement.

In tandem with its Part 2 rulemaking activities, SAMHSA has worked closely with federal and nonfederal partners to develop HIT standards and applications that support the use and disclosure of information protected by Part 2. These efforts are briefly described below.

³⁴ See <https://lac.org/resources/substance-use-resources/confidentiality-resources/>.

³⁵ See <http://www.amcp.org/WorkArea/DownloadAsset.aspx?id=21868>.

³⁶ The HIPAA Privacy Rule also includes an accounting of disclosures provision, which was expanded by the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009. Under the HITECH Act, patients have the right to an accounting of disclosures from EHR systems over the past three years for the purposes of treatment, payment, and other routine health care operations. HHS published a proposed rule on May 31, 2011 (76 *Federal Register* 31425), to implement this requirement. The proposal would allow patients to request an access report documenting all the persons who electronically accessed and viewed their PHI. The proposed rule has not been finalized.

³⁷ David Raths, “SAMHSA Releases Part 2 Final Rule on Substance Use Data Sharing,” *Healthcare Informatics*, January 13, 2017.

³⁸ P.L. 114-255, §11002, 130 Stat. 1033.

New Technologies Support Part 2 Data Exchange

To facilitate the electronic exchange of Part 2 data, each patient's consent preferences specifying the type of information that may be shared, and the individuals or entities with whom the information may be shared, must be carefully managed. Patient consent has to travel with the data in order to control access. In addition, a mechanism is required for segregating the data in a medical record to capture a patient's preferences. Data segmentation allows a patient's record to be broken down into multiple categories, allowing certain protected data elements to be removed (redacted) if a patient has not consented to their disclosure.

Consent2Share

In recent years, SAMHSA has worked with the HHS Office of the National Coordinator for Health Information Technology (ONC) on its Data Segmentation for Privacy (DS4P) initiative. Through DS4P, federal and nonfederal stakeholders developed internationally accepted standards and guidelines for segmenting medical data and managing patient consent.³⁹

Based on the DS4P standards, SAMHSA designed Consent2Share, an open-source online tool for data segmentation and consent management.⁴⁰ Consent2Share integrates with existing EHR systems and HIE networks to manage the exchange of health information among providers.⁴¹

Consent2Share provides a patient portal where individuals can learn about and manage their consent options. They can complete and electronically sign consent forms if they wish to permit the disclosure of protected information, whether it is protected under Part 2 or applicable state health privacy laws. Using Consent2Share, patients can indicate the individuals and/or entities with whom they want to share information and select from a list of protected information the specific types of data that are allowed to be disclosed.

Prior to the exchange of patient information, Consent2Share receives a patient's record from an EHR or HIE, confirms that the patient has consented to share information with the intended recipient, and applies the patient's consent choices—for example, redacting some or all of the Part 2 data unless the patient has consented to its disclosure—before sending the modified record to the recipient.

Opioid Treatment Program (OTP) Service Continuity Pilot

In 2015, SAMHSA launched the OTP Service Continuity Pilot (SCP) project to implement electronic health information exchange among OTPs in a way that is compliant with Part 2 and state law and minimizes disruptions in treatment.⁴²

It is critical that individuals receiving behavioral therapy and medications—methadone or buprenorphine—for their opioid addiction at an OTP have consistent, uninterrupted access to treatment. However, OTP patients may experience treatment disruptions when natural disasters or

³⁹ Information on the DS4P initiative is available at <https://www.healthit.gov/providers-professionals/ds4p-initiative>.

⁴⁰ Information on Consent2Share is available at <http://www.feisystems.com/what-we-do/health-it-application-development/consent2share/>.

⁴¹ Under ONC's Health IT Certification Program, EHR technology can now be certified as having the capability to send and receive an electronic document that is formatted in accordance with the DS4P standard. 45 C.F.R. §170.315(b)(7)-(8).

⁴² Information on the OTP-SCP is available at <https://www.samhsa.gov/sites/default/files/otp-application.pdf>.

other unanticipated events temporarily close the OTP and force them to seek treatment at another facility. Patients also may have difficulty maintaining treatment continuity during vacations and business travel, or when they relocate.

SAMHSA selected Arizona Health-e Connection (AzHeC), which operates the statewide HIE, to run the SCP project. AzHeC is working with three Arizona-based behavioral health organizations, each of which operates OTPs connected to the HIE.

Under the SCP, AzHeC has successfully integrated Consent2Share with the Arizona HIE. This enables Consent2Share to apply patient consent preferences to clinical documents handled by the HIE. Each time a patient receives counseling and medication treatment at an OTP, the facility records dosing and other treatment information in the patient's electronic medical record and sends an updated clinical summary document to the HIE. If the patient visits a different OTP, he or she can log into Consent2Share and modify the consent settings, giving the facility access to treatment information. When the facility contacts the HIE to request a copy of the patient's clinical summary document, Consent2Share applies the patient's consent preferences to the document and redacts any data that the requesting provider is not allowed to see.

Author Contact Information

Amanda K. Sarata
Specialist in Health Policy
asarata@crs.loc.gov, 7-7641

C. Stephen Redhead
Specialist in Health Policy
credhead@crs.loc.gov, 7-2261