February 12, 2019

Via Federal e-Rulemaking Portal

U.S. Department of Health and Human Services
Office for Civil Rights
Hubert H. Humphrey Building
200 Independence Avenue, S.W., Room 509F
Washington, DC  20503
Attn: RFI, RIN 0945-AA00

Re: Request for Information on Modifying HIPAA Rules to Improve Coordinated Care

Dear Sir/Madam:

The Legal Action Center (“LAC”) appreciates this opportunity to provide comments in response to the Office for Civil Rights (“OCR”) Request for Information (“RFI”) on the privacy and security implications of possible changes to the Health Insurance Portability and Accountability Act (“HIPAA”) Privacy, Security, and Breach Notification Rules (“HIPAA Rules”) to improve coordinated care, published in the December 14, 2018 issue of the Federal Register.

LAC is the only non-profit law and policy organization in the United States whose sole mission is to fight discrimination against people with histories of addiction, HIV/AIDS or criminal records, and to advocate for sound public policies in these areas.

LAC strongly opposes changes that weaken patient privacy protections in exchange for perceived benefits of administrative ease. Confidentiality is a crucial element of any treatment relationship, and ensuring patient privacy should be the top priority of efforts to improve treatment outcomes and care coordination. LAC firmly believes that patient-centered care includes putting patients at the center of the decision about when and how their health information is shared. Moreover, in the particular context of the opioid epidemic, ensuring patient confidentiality is vitally important to encourage people to seek medical care, including substance use disorder care, without fearing that their health information will be used against them.
We recognize that the HIPAA Rules play important roles in transmitting and securing patient health information in electronic formats. However, the threats to data integrity have outpaced the regulatory amendments, and protected health information is more vulnerable today than in 1996 when Congress enacted HIPAA. This vulnerability is demonstrated in the nation’s widespread data breaches of individuals’ health information and other personal data, including targeted attacks of protected health information, despite the HIPAA Privacy Rule and its corresponding systems that are designed to protect sensitive information from unauthorized disclosures.1

Instead, coordinated care for people living with sensitive health issues is best achieved by all applicable federal and state privacy laws working in concert to protect confidential patient information, incorporate patients’ informed consent, and share records with the appropriate recipients. Any changes to HIPAA should maximize the ability of these different laws to work together by bringing HIPAA into alignment with stricter privacy protections. Stricter confidentiality laws, such as the federal substance use disorder patient confidentiality law (“42 U.S.C. § 290dd-2”) and its regulations “42 CFR Part 2,” (referred to collectively as “Part 2,”) and rigorous state privacy laws remain better suited to handle sensitive health information since they typically include additional privacy safeguards (e.g., written patient consent) prior to disclosure of health records.2 For example, the existing HIPAA Privacy Rule would allow virtually unlimited disclosures without patients’ knowledge or consent to:

- law enforcement authorities to seize patient records that could lead to arrest and prosecution;3
- judicial or administrative bodies to obtain patient information for civil legal proceedings that could lead to loss of child custody;4

---

2 See, e.g., Mass. Ann. Laws ch. 111E, § 18 (treatment administrators must obtain patients’ consent to disclose substance use disorder information); Ohio Rev. Code Ann. § 3701.24(D) (HIV/AIDS patient information is confidential and only be released by patient consent or other authorized exceptions).
3 But see 42 CFR §§ 2.61-2.67 (describes Part 2’s requirements of disclosures of SUD information for the purposes of criminal investigations).
4 But see 42 CFR §§2.61-2.67 (describes Part 2’s requirements when subpoenas or general court orders request disclosures of SUD information).
• insurers for “treatment, payment, or health care operations” purposes, which could lead to patients losing jobs and access to many types of insurance;\(^5\) and

• re-disclosures of substance use disorder (“SUD”) information that could lead to unnecessary stigma and negative consequences of loss of employment or housing.\(^6\)

In order to improve coordinated care and treatment, LAC strongly support maintaining the core protections of Part 2 to effectively protect the confidentiality of patients’ records, satisfying stringent state privacy laws, and creating a stronger iteration of HIPAA. Despite the assertions of stakeholders who view Part 2 as “antiquated,” the Substance Abuse and Mental Health Service Administration (“SAMHSA”) recently amended the patient privacy regulations in 2017 and 2018 to facilitate the objective of providing integrative care between SUD and other health care information.\(^7\)

We remain concerned that weakening HIPAA Rules and mandating disclosures for treatment, payment, and healthcare operations purposes, will overrule providers’ best judgement about responding to requests for information, and will contribute to the existing level of discrimination and harm to people living with substance use disorders. This will only result in more people who need substance use disorder treatment, being discouraged and afraid to seek the health care they need during the nation’s worst opioid crisis.\(^8\)

We strongly support coordinating patient care by maintaining Part 2’s core protections for SUD information, applying rigorous state privacy laws, and strengthening HIPAA’s privacy and security standards for the following reasons:

1. The heightened privacy protections in Part 2 are as critical today as they were when they were enacted more than 40 years ago and must be preserved.

---


\(^6\) But see 42 CFR. §§2.32, 2.33. Part 2 prohibits re-disclosures of patient identifying SUD information, unless the patient provides written consent, a court order exists, or if an exception to the Part 2 regulations applies.


\(^8\) See, e.g., William Stauffer, Executive Director – Pennsylvania Recovery Organizations Alliance, March 20, 2018 letter to the House Energy and Commerce Committee.
2. During the worst opioid epidemic in our nation’s history, we must do everything possible to increase – not decrease – the number of people who seek treatment.

3. SUD is unique among medical conditions because of its criminal and civil consequences and the rampant discrimination people face.

4. With so much at stake, patients in SUD treatment should retain the right to consent when and to whom their records are disclosed, as currently found in Part 2.

5. Effective integration of SUD treatment with the rest of the health care system is critically important, and information exchange in accordance with confidentiality law and current technology is now possible. To facilitate that process, SAMHSA recently amended the Part 2 regulations to further promote the integration of confidential SUD information into general health records.

We respectfully request that OCR work cooperatively with SAMHSA to issue regulations that clearly demonstrate to all stakeholders that patients’ preferences for the disclosure of their sensitive health care information remain at the core of care coordination policies and standards. As a result, OCR should not weaken privacy as described in the RFI, but instead upgrade HIPAA’s privacy safeguards for sensitive health information to Part 2’s standards to ensure that these rules work in harmony with current federal and state confidentiality laws.

Lastly, our responses to selected OCR’s RFI questions are detailed below:

(6) Do health care providers currently face barriers or delays when attempting to obtain PHI from covered entities for treatment purposes? For example, do covered entities ever affirmatively refuse or otherwise fail to share PHI for treatment purposes, require the requesting provider to fill out paperwork not required by the HIPAA Rules to complete the disclosure (e.g., a form representing that the requester is a covered health care provider and is treating the individual about whom the request is made, etc.), or unreasonably delay sharing PHI for treatment purposes? Please provide examples of any common scenarios that may illustrate the problem.

LAC Response to Question 6:
The existence of other federal and state laws that protect the privacy of patient health information may prevent covered entities from sharing PHI in some instances -- but they should not be considered as hindrances or causes of delay. Their purpose is to protect unauthorized disclosures of health information to unknown recipients that could be detrimental to unsuspecting patients. Moreover, if these federal and state laws are more
protective of patient confidentiality than HIPAA’s requirements – then covered entities must adhere to the requirements of the more stringent law.\(^9\)

In certain instances, particular covered entities (who are health care providers) must adhere to other applicable federal confidentiality laws, such as the federal confidentiality law for substance use disorder records -- 42 U.S.C. §290dd-2, and its regulations, 42 CFR Part 2 (collectively referred to as “Part 2”) and state confidentiality laws before they can share particular PHI for treatment purposes. Often, these specific privacy laws and their regulations serve as the primary source to safeguard the disclosure of sensitive health information without the patient’s knowledge and consent, since HIPAA currently does not have this capacity.

Accordingly, these covered entities may not disclose relevant PHI unless certain requirements have been met. For example, unless certain exceptions apply, Part 2 requires a covered entity to obtain patients’ written consent before their Part 2-protected substance use disorder treatment records can be disclosed to other providers.\(^10\)

The type of patient health care records that Part 2 safeguards from unauthorized disclosures include any information obtained about a patient – including the patient’s identity, address, medical or treatment information, and all communications made by the patient to Part 2 program staff – whether the information is in in writing or is recorded in some other form.\(^11\)

State laws also exist that govern the disclosure of confidential health information. For example, Indiana and Connecticut require the disclosures of patients’ SUD records (PHI) to follow the requirements of Part 2.\(^12\) Massachusetts requires patients’ written consent for the disclosure of patients’ HIV/AIDS test results.

\(^9\) 45 CFR § 160.203(b).
\(^{10}\) 42 CFR § 2.11; 2.12(a)(1)(i). See also 42 CFR § 2.11. Part 2 defines a program as, “[other than a general medical care facility] . . . any person or organization that holds itself out as providing, and provides, substance use disorder diagnosis, treatment, referral for treatment or prevention.” A Part 2 program must also be “federally assisted.” 42 CFR § 2.12. In addition, Part 2 governs substance use disorder (“SUD”) patient records for those patients who receive treatment (or diagnosis or referral for treatment) from (a) an identified unit of a general medical facility that holds itself out as providing, and provides, alcohol or drug abuse diagnosis, treatment or referral for treatment, or (b) medical personnel or other staff in the general medical care facility whose primary function is to provide those services. 42 CFR §§ 2.11, 2.12(e) (1).
\(^{11}\) 42 CFR § 2.11. See id (including the memories and impressions of program staff, even if they are not recorded in any form).
As a result, if covered entities fail to uphold all applicable federal and state privacy laws, sensitive health information can be disclosed to individuals and entities without the patient’s knowledge or consent and result in negative consequences to the patient. When this occurs, patients will avoid seeking the very health care they need.

(7) Should covered entities be required to disclose PHI when requested by another covered entity for treatment purposes? Should the requirement extend to disclosures made for payment and/or health care operations purposes generally, or, alternatively, only for specific payment or health care operations purposes? (a) Would this requirement improve care coordination and/or case management? Would it create unintended burdens for covered entities or individuals? For example, would such a provision require covered entities to establish new procedures to ensure that such requests were managed and fulfilled pursuant to the new regulatory provision and, thus, impose new administrative costs on covered entities? Or would the only new administrative costs arise because covered entities would have to manage and fulfill requests for PHI that previously would not have been fulfilled? (b) Should any limitation be placed on this requirement? For instance, should disclosures for healthcare operations be treated differently than disclosures for treatment or payment? Or should this requirement only apply to certain limited payment or health care operations purposes? If so, why? (c) Should business associates be subject to the disclosure requirement? Why or why not?

LAC Response to Question 7:
We do not support OCR requiring covered entities to disclose PHI when requested by another entity for treatment purposes. If OCR determines that covered entities must disclose PHI when requested by another covered entity for treatment purposes, OCR should clarify that covered entities may only disclose PHI when they have satisfied existing federal and applicable state confidentiality requirements that govern the release of sensitive health information. Specifically, if the covered entity is a Part 2 program, the covered entity must first have obtained patients’ written consent (unless an applicable exception applies) before SUD records can be released to another covered entity.\(^\text{13}\) Similarly, New Jersey considers alcohol treatment records as confidential, which can typically only be released through a court order.\(^\text{14}\)

The 2018 amendments to Part 2 offer flexibility for lawful holders of SUD records (e.g., covered entities/health care providers) who need to re-disclose

\(^{13}\) See 42 CFR §§ 2.32, 2.33.
that information.\textsuperscript{15} Specifically, once patients consent to a disclosure of their patient records for payment and/or health care operations purposes, lawful holders who receive these records pursuant to patient consent may further disclose the records as necessary to their contractors, subcontractors, or legal representatives, in order to perform the payment and/or health care operations functions designated on the consent form.\textsuperscript{16} However, disclosures of SUD records to lawful holders’ contractors, subcontractors, and legal representatives are not permitted for activities related to a patient’s diagnosis, treatment, referral for treatment, or care coordination.\textsuperscript{17}

Policies and practices to satisfy Part 2 and other rigorous state confidentiality laws should already be established and implemented by HIPAA’s covered entities.

\textbf{(8) Should any of the above proposed requirements to disclose PHI apply to all covered entities (i.e., covered health care providers, health plans, and health care clearinghouses), or only a subset of covered entities? If so, which entities and why?}

\textbf{LAC Response to Question 8:} HIPAA covered entities should not be required to disclose PHI to a non-covered healthcare provider, because such a provider may have entirely inadequate privacy protections for PHI and mandating such disclosures would unreasonably expose patients’ PHI to risk of unauthorized disclosures. The risks associated with disclosing PHI to healthcare providers not subject to any standardized privacy and security protections are vast, diverse, and expanding, and greatly outweigh the benefit of sharing PHI among all of an individual’s healthcare providers. Such disclosures can still be made with the patient’s authorization or by the patient’s own self-disclosure of the sensitive health information.

\textbf{(9) Currently, HIPAA covered entities are permitted, but not required, to disclose PHI to a health care provider who is not covered by HIPAA (i.e., a health care provider that does not engage in electronic billing or other covered electronic transactions) for treatment and payment purposes of either the covered entity or the noncovered health care provider. Should a HIPAA covered entity be required to disclose PHI to a non-covered health care provider with respect to any of the matters discussed in}

\textsuperscript{15} See generally Confidentiality of Substance Use Disorder Patient Records, 82 Fed. Reg. 6052 (Jan. 18, 2017). See also 42 CFR §2.11. A “lawful holder” of patient identifying Part 2 information is an individual or entity who has received such information as the result of a Part 2-compliant patient consent (with a prohibition on re-disclosure notice) or as a result of one of Part 2’s exceptions to the consent requirements.

\textsuperscript{16} 42 CFR § 2.33(b).

\textsuperscript{17} 83 Fed. Reg. at 241, 243 (preamble to the Final Rule).
Questions 7 and 8? Would such a requirement create any unintended adverse consequences? For example, would a covered entity receiving the request want or need to set up a new administrative process to confirm the identity of the requester? Do the risks associated with disclosing PHI to health care providers not subject to HIPAA’s privacy and security protections outweigh the benefit of sharing PHI among all of an individual’s health care providers?

LAC Response to Question 9:
Both HIPAA covered entities and noncovered entities should strengthen their current confidentiality requirements by requiring them to also satisfy other federal (i.e., Part 2) and relevant state confidentiality laws in order to disclose SUD records. Both HIPAA covered entities and noncovered entities should be required to secure all health care records pursuant to HIPAA Security requirements, which is currently required for Part 2 (SUD) records. In addition, LAC reiterates its points in response to Question 8 above.

(10) Should a non-covered health care provider requesting PHI from a HIPAA covered entity provide a verbal or written assurance that the request is for an accepted purpose (e.g., TPO) before a potential disclosure requirement applies to the covered entity receiving the request? If so, what type of assurance would provide the most protection to individuals without imposing undue burdens on covered entities? How much would it cost covered entities to comply with this requirement? Please provide specific cost estimates where available.

LAC Response to Question 10:
Due to the significant risk to patient privacy that such a change would present, and for the reasons set forth in LAC’s response to Questions 8 and 9 above, LAC does not support such a modification. If OCR decides to implement this change, LAC urges OCR to require a written assurance that the request is for an accepted purpose, and that the request be accompanied by a copy of the requesting agency’s privacy policies and procedures and the contact information for a privacy officer.

(11) Should OCR create exceptions or limitations to a requirement for covered entities to disclose PHI to other health care providers (or other covered entities) upon request? For example, should the requirement be limited to PHI in a designated record set? Should psychotherapy notes or other specific types of PHI (such as genetic information) be excluded from the disclosure requirement unless expressly authorized by the individual?

---

18 See 42 CFR § 2.16.
LAC Response to Question 11:
LAC does not support the proposal to mandate disclosures, for the reasons stated in LAC’s response to Questions 8, 9, and 10 above. If OCR decides to proceed with this proposal, it should certainly not extend the mandated disclosures to include sensitive health information, such as psychotherapy notes, genetic information, or any other category of health information currently subject to heightened privacy protections.

Under Part 2, Part 2-defined programs have the discretion to decide whether to permit patients to view or obtain copies of their records, unless they are governed by a state law that establishes circumstances in which patients have a right to such access.19

Current HIPAA regulations generally require covered entities to provide patients with access to their records upon request.20 State laws that govern patient access to records may remain in force if they are “more stringent” than HIPAA and relate to patient privacy.21 However, Part 2 programs do not have to provide patient access to psychotherapy notes.22 OCR should also recognize that some states do allow covered entities to deny access to psychotherapy notes in limited circumstances (e.g., if the information is likely to harm that patient or others, or if the information obtained from someone other than a health care provider under a promise of confidentiality when access would likely reveal the source of the information). In addition, some state laws exclude even more than psychotherapy notes. It is important to note that state laws that give patients greater access than HIPAA are “more stringent” than HIPAA, and providers should follow the state law. When the reverse is true, Part 2 programs should follow HIPAA.23

Lastly, covered entities should be able to segment their health care records to assist them in determining if SUD, mental health, and any other sensitive health information can be disclosed to other covered entities, patients, and other stakeholders. These entities should also be required to prove that they

19 42 CFR § 2.23.
20 45 CFR § 164.524.
21 45 CFR § 160.203(b).
22 45 CFR § 164.524(a)(1)(i). See also id. at § 164.501. HIPAA defines “psychotherapy notes” as notes recorded in any medium “by a health care provider who is a mental health professional documenting or analyzing the contents of conversations 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.
23 For example, if a state law provides patients access to all of the information in their records except for information likely to harm someone, that law is more stringent and thus providers (covered entities) must follow that state law. In that case, providers may not deny patients access to all psychotherapy notes (as HIPAA allows), but rather only those parts of psychotherapy notes -- and other part of the record -- that contain information excludable under state law.
can successfully segment confidential health information in their data systems.

(13) Should individuals have a right to prevent certain disclosures of PHI that otherwise would be required for disclosure? For example, should an individual be able to restrict or “opt out” of certain types of required disclosures, such as for health care operations? Should any conditions apply to limit an individual’s ability to opt out of required disclosures? For example, should a requirement to disclose PHI for treatment purposes override an individual’s request to restrict disclosures to which a covered entity previously agreed?

LAC Response to Question 13:
Yes, patients should always have the right and the ability to prevent certain disclosures of their PHI, by opting out of HIPAA required disclosures and/or limiting disclosures of specific information through written patient consent. Patient should always have the right to know and control where their health information may be disclosed. Covered entities should be prepared to explain to patients why the disclosure of certain PHI may be necessary for treatment, payment, and/or health care operations purposes. Even if a patient previously agreed to disclose certain PHI for a particular purpose but refuses to disclose the same PHI in a subsequent occurrence – that patients’ preferences should be met.

In addition, OCR should balance any proposed changes that would increase risk to patient privacy with a concomitant strengthening of patient’s privacy rights, by requiring covered entities to honor patients’ requests to restrict access to a record, unless the covered entity determines that such a restriction would create an unreasonable threat of harm to the patient.

(14) How would a general requirement for covered health care providers (or all covered entities) to share PHI when requested by another covered health care provider (or other covered entity) interact with other laws, such as 42 CFR part 2 or state laws that restrict the sharing of information?

LAC Response to Question 14:
[See LAC response to Question 6, repeated here]: The existence of other federal and state laws that protect the privacy of patient health information may prevent covered entities from sharing PHI in some instances -- but they should not be considered as hindrances or causes of delay. Their purpose is to protect unauthorized disclosures of health information to unknown recipients that could be detrimental to unsuspecting patients. Moreover, if these federal and state laws are more
protective of patient confidentiality than HIPAA’s requirements – then covered entities must adhere to the requirements of the more stringent law.\textsuperscript{24}

In certain instances, particular covered entities (who are health care providers) must adhere to other applicable federal confidentiality laws, such as the federal confidentiality law for substance use disorder records -- 42 U.S.C. §290dd-2, and its regulations, 42 CFR Part 2 (collectively referred to as “Part 2”) and state confidentiality laws before they can share particular PHI for treatment purposes. Often, these specific privacy laws and their regulations serve as the primary source to safeguard the disclosure of sensitive health information without the patient’s knowledge and consent, since HIPAA currently does not have this capacity.

Accordingly, these covered entities may not disclose relevant PHI unless certain requirements have been met. For example, unless certain exceptions apply, Part 2 requires a covered entity to obtain patients’ written consent before their Part 2-protected substance use disorder treatment records can be disclosed to other providers.\textsuperscript{25}

The type of patient health care records that Part 2 safeguards from unauthorized disclosures include any information obtained about a patient – including the patient’s identity, address, medical or treatment information, and all communications made by the patient to Part 2 program staff – whether the information is in in writing or is recorded in some other form.\textsuperscript{26}

State laws also exist that govern the disclosure of confidential health information. For example, Indiana and Connecticut require the disclosures of patients’ SUD records (PHI) to follow the requirements of Part 2.\textsuperscript{27} Massachusetts requires patients’ written consent for the disclosure of patients’ HIV/AIDS test results.

\textsuperscript{24} 45 CFR § 160.203(b).
\textsuperscript{25} 42 CFR § 2.11; 2.12(a)(1)(i). See also 42 CFR § 2.11. Part 2 defines a program as, “[other than a general medical care facility] . . . any person or organization that holds itself out as providing, and provides, substance use disorder diagnosis, treatment, referral for treatment or prevention.” A Part 2 program must also be “federally assisted.” 42 CFR § 2.12. In addition, Part 2 governs substance use disorder (“SUD”) patient records for those patients who receive treatment (or diagnosis or referral for treatment) from (a) an identified unit of a general medical facility that holds itself out as providing, and provides, alcohol or drug abuse diagnosis, treatment or referral for treatment, or (b) medical personnel or other staff in the general medical care facility whose primary function is to provide those services. 42 CFR §§ 2.11, 2.12(e) (1).
\textsuperscript{26} 42 CFR § 2.11. See id (including the memories and impressions of program staff, even if they are not recorded in any form).
\textsuperscript{27} Ind. Code Ann § 16-39-1-9; Conn. Gen. Stat. § 17a-688.
As a result, if covered entities fail to uphold all applicable federal and state privacy laws, sensitive health information can be disclosed to individuals and entities without the patient’s knowledge or consent and result in negative consequences to the patient. When this occurs, patients will avoid seeking the very health care they need.

(15) Should any new requirement imposed on covered health care providers (or all covered entities) to share PHI when requested by another covered health care provider (or other covered entity) require the requesting covered entity to get the explicit affirmative authorization of the patient before initiating the request, or should a covered entity be allowed to make the request based on the entity’s professional judgment as to the best interest of the patient, based on the good faith of the entity, or some other standard?

LAC Response to Question 15:
The patients’ preference for the disclosure should absolutely be required, and certainly not ignored. The requesting covered entity should have to get the explicit affirmative authorization of the patient before initiating the request. Including patients at the center of care means putting patients’ decisions about their health information at the center of their care as well.

For SUD and other sensitive health information, the HIPAA Rule should adopt the more stringent 42 CFR Part 2 requirement that further safeguards private information. For example, the health care provider/covered entity should seek the patients’ consent for the disclosure, unless another regulatory exception exists. If the PHI is SUD information and patients have used a Part 2-compliant consent form to share specific SUD information to “all of their current and future treating providers” within an identified health information exchange, then there would not be a need to obtain further patient consent for the disclosure or name the specific health care providers.28

(16) What considerations should OCR take into account to ensure that a potential Privacy Rule requirement to disclose PHI is consistent with rulemaking by the Office of the National Coordinator for Health Information Technology (ONC) to prohibit “information blocking,” as defined by the 21st Century Cures Act?

LAC Response to Question 16:
OCR should work collaboratively with the HHS Office of the National Coordinator (“ONC”) to require covered entities to have standardized

28 See 42 CFR § 2.11 (defines “treating provider relationship); id. at § 2.31 (describes recent Part 2 consent options).
electronic health record capability to segment, safeguard, and exchange PHI (such as substance use disorder information) and other sensitive health data.

(17) Should OCR expand the exceptions to the Privacy Rule’s minimum necessary standard? For instance, should population-based case management and care coordination activities, claims management, review of health care services for appropriateness of care, utilization reviews, or formulary development be excepted from the minimum necessary requirement? Would these exceptions promote care coordination and/or case management? If so, how? Are there additional exceptions to the minimum necessary standard that OCR should consider?

LAC Response to Question 17:
We oppose this proposal. The minimum necessary standard has been established for both HIPAA and Part 2 to prevent other portions of the health records from being disclosed that are not essential to the original purpose for the release of the information.

It is unlikely that the goals of care coordination and/or case management would be achieved through an exception of the minimum necessary standard for these and other functions. Instead, it is more probable that if more than a “minimum necessary” amount (e.g., an unlimited amount) of sensitive health information became available for formulary development, utilization reviews, care coordination, and other functions – an unlimited amount of PHI would be at risk because of frequently occurring breaches of privacy based on the current weaker HIPAA standard.

(18) Should OCR modify the Privacy Rule to clarify the scope of covered entities’ ability to disclose PHI to social services agencies and community-based support programs where necessary to facilitate treatment and coordination of care with the provision of other services to the individual? For example, if a disabled individual needs housing near a specific health care provider to facilitate their health care needs, to what extent should the Privacy Rule permit a covered entity to disclose PHI to an agency that arranges for such housing? What limitations should apply to such disclosures? For example, should this permission apply only where the social service agency itself provides health care products or services? In order to make such disclosures to social service agencies (or other organizations providing such social services), should covered entities be required to enter into agreements with such entities that contain provisions similar to the provisions in business associate agreements?

LAC Response to Question 18:
While it is necessary to coordinate patient care with the appropriate social services and community-based resources for people living with SUD and
other sensitive health conditions, HIPAA should strengthen its existing privacy standards to prevent negative consequences from occurring in these circumstances. For example, current Part 2 regulations would require patients to disclose specific SUD information by written consent for a particular purpose (e.g., housing) to an individual staff person in a social service agency. If a social service agency required certain information from a patient’s SUD record, the agency should seek a special court order to obtain the information from the Part 2 program.\textsuperscript{29} These requirements minimize the likelihood that a social service agency will use the SUD record for a different purpose that would be harmful to the patient (e.g., child welfare or child custody proceedings).

Instead of weakening the current HIPAA Privacy Rule, we recommend that SAMHSA and OCR provide social service agencies with training and technical assistance on Part 2, HIPAA, and applicable respective state confidentiality laws to facilitate treatment and coordination of care. As part of this outreach effort on patient confidentiality protections, OCR and SAMHSA should correct misconceptions and provide guidance about the scenarios when, to whom, and how specific health information can be disclosed via HIPAA and Part 2 to not only social service agencies – but also to other health care stakeholders, patients, and family members.

(19) Should OCR expressly permit disclosures of PHI to multidisciplinary/ multi-agency teams tasked with ensuring that individuals in need in a particular jurisdiction can access the full spectrum of available health and social services? Should the permission be limited in some way to prevent unintended adverse consequences for individuals? For example, should covered entities be prevented from disclosing PHI under this permission to a multi-agency team that includes a law enforcement official, given the potential to place individuals at legal risk? Should a permission apply to multidisciplinary teams that include law enforcement officials only if such teams are established through a drug court program? Should such a multidisciplinary team be required to enter into a business associate (or similar) agreement with the covered entity? What safeguards are essential to preserving individuals’ privacy in this context?

**LAC Response Question 19:**
OCR should first strengthen HIPAA’s current privacy standards by conforming them to the more protective provisions of Part 2, such as prohibiting disclosures of SUD information to law enforcement entities without a special court order.\textsuperscript{30} If law enforcement entities are not part of

\textsuperscript{29} 42 CFR §§ 2.63-2.67.
\textsuperscript{30} 42 U.S.C. § 290dd-2(c); 42 CFR §§ 2.61-2.67.
the multi-disciplinary/multi-agency teams, then disclosures of health information could be conducted if patients consent to the release of these records. OCR should also incorporate the Part 2 prohibition on certain uses of information, to prevent law enforcement officials from using PHI to criminally investigate or prosecute a patient.\(^{31}\)

(20) Would increased public outreach and education on existing provisions of the HIPAA Privacy Rule that permit uses and disclosures of PHI for care coordination and/or case management, without regulatory change, be sufficient to effectively facilitate these activities? If so, what form should such outreach and education take and to what audience(s) should it be directed?

LAC Response to Question 20:
Yes. Funding and other appropriate resources should be established for HHS (e.g., SAMHSA, OCR, and ONC) to provide technical assistance and outreach to patients, health care providers, other health care industry stakeholders, and families on existing federal and applicable state confidentiality laws. Technical assistance and outreach should include how care coordination and/or case management can be performed while maintaining privacy protections with sensitive health information (e.g., SUD, mental health, HIV/AIDS, domestic violence, etc.). For example, with SUD information: all stakeholders will need to be informed of the use of patient consent to permit disclosures and re-disclosures of SUD records to accomplish care coordination and/or case management to maintain confidentiality safeguards.

(21) Are there provisions of the HIPAA Rules that work well, generally or in specific circumstances, to facilitate care coordination and/or case management? If so, please provide information about how such provisions facilitate care coordination and/or case management. In addition, could the aspects of these provisions that facilitate such activities be applied to provisions that are not working as well?

LAC Response to Question 21:
While the HIPAA Rules are necessary to providing basic privacy protections for PHI, they should be strengthened by incorporating the supplemental confidentiality safeguards of 42 CFR Part 2 (e.g., patient consent) and other stringent state privacy laws. The functionality of care coordination and case management would only improve by involving patients in the processes and discussing with them reasons for the disclosure of their sensitive health information, as well as informing them of the recipients of their PHI.

\(^{31}\) See 42 U.S.C. § 290dd-2(c); 42 CFR § 2.12(d).
b - Promoting Parental and Caregiver Involvement and Addressing the Opioid Crisis and Serious Mental Illness:

(22) What changes can be made to the Privacy Rule to help address the opioid epidemic? What risks are associated with these changes? For example, is there concern that encouraging more sharing of PHI in these circumstances may discourage individuals from seeking needed health care services? Also is there concern that encouraging more sharing of PHI may interfere with individuals’ ability to direct and manage their own care? How should OCR balance the risk and the benefit?

LAC Response to Question 22:
With respect to the anecdotal evidence cited by OCR that some covered entities are reluctant to inform and involve patients' loved ones for fear of violating HIPAA, LAC agrees that this lack of understanding about HIPAA among covered entities is worrisome and should be addressed. LAC firmly disagrees, however, that attacking the patient privacy protections in HIPAA is the appropriate course of action to improve covered entities' understanding of how HIPAA permits providers to communicate with families.

LAC applauds OCR's efforts to improve awareness of how HIPAA permits doctors to respond to the opioid crisis and communicate with family members about the individual’s health condition. We encourage OCR to provide additional resources, training, and educational efforts in the same vein, informed by a systematic review of the needs of covered entities to better understand HIPAA's provisions regarding family members and caregivers.

The objective evidence shows that privacy protections are a key component of many individuals' decisions to access care for substance use disorder, including opioid use disorder. According to a recent survey by SAMHSA, many patients identify privacy and confidentiality concerns as a major barrier to entering care, accounting in part for the enormous treatment gap in the United States. For over 40 years, federal law has recognized the important role that privacy protections play in encouraging patients to enter treatment for substance use disorder, beginning with the passage of the Comprehensive Alcohol Abuse and Alcoholism Prevention, Treatment, and Rehabilitation Act Amendments of 1974, and leading to today's modernized version of those protections at 42 USC 290dd-2 and 42 CFR Part 2 (amended 2017 and 2018). In LAC's experience, many individuals simply would not access care if they were not assured of the confidentiality protections of their SUD treatment.

LAC is also concerned that more sharing of PHI will interfere with individuals' ability to direct and manage their own care. Specifically, individuals living with SUD face harmful stigma, prejudice, and discrimination in health care settings. This stigma, prejudice, and discrimination has a documented effect on lowering the standard of care and diminishing treatment outcomes for individuals with SUDs. Permitting a patient to direct and manage their own care, including managing disclosures of sensitive SUD information, is crucial to help patients avoid this harmful stigma. While Part 2 protects many SUD treatment records, it does not protect SUD information that a patient self-discloses, or SUD treatment information from a provider that is not a "Part 2 program." Common examples of SUD treatment providers that do not fall within Part 2 include private, non-federally assisted SUD treatment programs, and general medical facilities like FQHCs and community health clinics, where SUD services do not constitute the primary function of any given physician. The privacy of this sensitive, non-Part 2 protected, SUD treatment information relies upon HIPAA's basic protections, and OCR should proceed with extreme caution before eliminating these confidentiality protections.

No other changes to the HIPAA Privacy Rule to address the opioid epidemic should be made, except for strengthening HIPAA’s patient privacy rights to those of 42 CFR Part 2 (e.g., prohibiting disclosures of SUD information to law enforcement entities without a special court order), so individuals living with SUD would not be hesitant to seek treatment.33

(24) Are there circumstances in which parents have been unable to gain access to their minor child’s health information, especially where the child has substance use disorder (such as opioid use disorder) or mental health issues, because of HIPAA? Please specify, if known, how the inability to access a minor child’s information was due to HIPAA, and not state or other law.

Response to Question 24:
Privacy laws must strike a careful balance in protecting a minor’s right to engage in confidential medical treatment, without erecting a barrier to beneficial parental involvement in the minor’s care. The HIPAA Rules already permit several types of disclosures of health information from minor patients to their parents, while deferring to providers’ best judgment about when such disclosures would harm the minor patient.

LAC recommends that OCR and SAMHSA provide training to stakeholders (including patients, families, and caregivers) on how and when parents and

33 42 CFR §2.12(d); 42 U.S.C. § 290dd-2(c).
family can access minors’ health information, in light of their respective state laws that govern a minor’s access to treatment and disclosure of their health information.

(25) Could changes to the Privacy Rule help ensure that parents are able to obtain the treatment information of their minor children, especially where the child has substance use disorder (including opioid use disorder) or mental health issues, or are existing permissions adequate? If the Privacy Rule is modified, what limitations on parental access should apply to respect any privacy interests of the minor child? (a) Currently, the Privacy Rule generally defers to state law with respect to whether a parent or guardian is the personal representative of an unemancipated minor child and, thus, whether such parent or guardian could obtain PHI about the child as his/her personal representative; if someone other than the parent or guardian can or does provide consent for particular health care services, the parent or guardian is generally not the child’s personal representative with respect to such health care services. Should these standards be reconsidered generally, or specifically where the child has substance use disorder or mental health issues? (b) Should any changes be made to specifically allow parents or spouses greater access to the treatment information of their children or spouses who have reached the age of majority? If the Privacy Rule is changed to encourage parental and spousal involvement, what limitations should apply to respect the privacy interests of the individual receiving treatment? (c) Should changes be made to allow adult children to access the treatment records of their parents in certain circumstances, even where an adult child is not the parent’s personal representative? Or are existing permissions sufficient? For instance, should a child be able to access basic information about the condition of a parent who is being treated for early onset dementia or inheritable diseases? If so, what limitations should apply to respect the privacy interests of a parent?

LAC Response to Question 25:

We do not recommend that OCR make any changes to the current HIPAA Privacy Rule concerning the treatment of minors and parental access to their health information. Parental access to a minor child’s medical record should depend as much as possible on the minor child’s consent to parental involvement. If the minor child refuses to authorize disclosures to his/her parents, there should be a strong presumption in favor of honoring the minor child’s confidentiality requests, in order to promote more minors entering health care treatment and being forthcoming with their providers about their health. Stakeholders should also consult their state privacy laws and other relevant federal laws concerning requirements for minors’ ability to determine their health care treatment and disclosures of their health information.
(26) The Privacy Rule currently defers to state or other applicable law to determine the authority of a person, such as a parent or spouse, to act as a personal representative of an individual in making decisions related to their health care. How should OCR reconcile any changes to a personal representative’s authority under HIPAA with state laws that define the scope of parental or spousal authority for state law purposes?

LAC Response to Question 26:
OCR should cautiously balance any changes to a personal representative’s authority under HIPAA that diverge from the current deference to state or other applicable law, especially because other federal privacy laws also defer to state law definitions about the authority of personal representatives of a patient.\(^{34}\)

(31) Should the Department require covered entities to account for their business associates’ disclosures for TPO, or should a covered entity be allowed to refer an individual to its business associate(s) to obtain this information? What benefits and burdens would covered entities and individuals experience under either of these options?

LAC Response to Question 31:
OCR should require covered entities to account for their business associates’ disclosures for treatment, payment, and health care operations (“TPO”) for two reasons:

- It would be unduly burdensome on individuals to seek an accounting of disclosures from the covered entity and potentially various business associates.

- Covered entities may not have proper business associate agreements with their business associates, and business associates may not properly account for TPO disclosures – indeed, business associates may be unaware of such a requirement if there is no business associate agreement in place. In the instance that a covered entity is disclosing PHI to a business associate that is failing to comply with its HIPAA obligations, the covered entity, not the individual patient, is in the best position to alert the business associate to its need to come into compliance.\(^{35}\)

\(^{34}\) See, e.g., 42 CFR § 2.14.

(35) A covered entity’s Notice of Privacy Practices ("NPP") must inform individuals of the right to obtain an accounting of disclosures. Is this notice sufficient to make patients aware of this right? If not, what actions by OCR could effectively raise awareness?

LAC Response to Question 35:
LAC encourages OCR to fully study this issue and consult with relevant patient advocates and experts, as well as existing HHS guidance to determine whether the notice is sufficient, and if not, ways to improve patient understanding of the NPP (including for individuals with limited English proficiency and/or health literacy).

(36) Why do individuals make requests for an accounting of disclosures under the current rule? Why would individuals make requests for an accounting of TPO disclosures made through EHRs?

LAC Response to Question 36:
Individuals may request an accounting of disclosures when there is an error in their medical record, in order to make sure the error is corrected with all the entities who subsequently received and re-disclosed the incorrect information. This may be particularly important if sensitive data, like substance use disorder information, mental health information, or certain other illnesses, is incorrectly entered into a patient’s record, or incorrectly made part of a patient’s general medical records.

(37) What data elements should be provided in an accounting of TPO disclosures, and why? How important is it to individuals to know the specific purpose of a disclosure—i.e., would it be sufficient to describe the purpose generally (e.g., for “for treatment,” “for payment,” or “for health care operations purposes”), or is more detail necessary for the accounting to be of value? To what extent are individuals familiar with the range of activities that constitute “health care operations?” On what basis do commenters make this assessment?

LAC Response to Question 37:
At a very minimum, the accounting should include what information was disclosed, the date, name and entity to whom the information was}

disclosed, and the purpose of the disclosure. With respect to the purpose of the disclosure, it is Legal Action Center's experience that very few individuals, their families, or even health providers are aware of the range of activities and corresponding recipients that constitute "health care operations." "Health care operations" is too broad and vague of a designation that requires more specific descriptions of the purpose, date of disclosure, recipient, and type of PHI that is subject to disclosure.

More specific descriptions should be required for “treatment” disclosures to include the date and the recipient of the disclosures, and the type of health condition the requested PHI is treating in order to be of value to individuals and inform them of the reason for the disclosures.

(39) If covered entities are unable to modify existing systems or processes to generate a full accounting of disclosures for TPO (e.g., because modification would be prohibitively costly), should OCR instead require covered entities to conduct and document a diligent investigation into disclosures of PHI upon receiving an individual’s request for an accounting of disclosures for TPO? If not, are there certain circumstances or allegations that should trigger such an investigation and documentation by a covered entity? How much time should a covered entity be allowed to conduct and provide the results of such an investigation?

LAC Response to Question 39:
First, OCR should work closely with other agencies as appropriate to minimize out-of-pocket costs for covered entities to make the modifications necessary to generate a full accounting of disclosures for TPO. Not only would this help bring covered entities into compliance with HIPAA, but it may also be required under state laws. Second, OCR should set forth specific standards and quantifiable measures of what constitutes "prohibitive cost," e.g., percentage of overall costs, or percentage of overall operating budget. Finally, to the extent that making such a modification would prove "prohibitively costly," OCR should grant a substitute remedy for patients that is as broad as possible to serve as a complete accounting of disclosures for TPO purposes.

(40) If OCR requires or permits covered entities to conduct an investigation into TPO disclosures in lieu of providing a standard accounting of such disclosures, what information should the entities be required to report to the individual about the findings of the investigation? For example, should OCR require covered entities to
provide individuals with the names of persons who received TPO disclosures and the purpose of the disclosures?

LAC Response to Question 40:
If OCR permits certain covered entities to conduct an investigation instead of providing a standard accounting, OCR should require the investigation to include: the names of persons who received disclosures; the purpose of the disclosures; the amount and type of health information that was disclosed; and the dates of the disclosures. The investigation should provide a similar scope of information to a patient as the standard accounting would provide; LAC is concerned that in the alternative, covered entities would seek to avoid providing the standard accounting, and instead offer to conduct an investigation that would be of limited utility to the patient.

(41) The HITECH Act section 13405(c) only requires the accounting of disclosures for TPO to include disclosures through an EHR. In its rulemaking, should OCR likewise limit the right to obtain an accounting of disclosures for TPO to PHI maintained in, or disclosed through, an EHR? Why or why not? What are the benefits and drawbacks of including TPO disclosures made through paper records or made by some other means such as orally? Would differential treatment between PHI maintained in other media and PHI maintained electronically in EHRs (where only EHR related accounting of disclosures would be required) disincentivize the adoption of, or the conversion to, EHRs?

LAC Response to Question 41:
Patients’ right to an accounting should not depend on whether or not their provider uses paper records or EHRs. Similarly, patients should not be penalized because their providers do not have access to an EHR. In order to equalize the opportunity for patients to receive an accounting of disclosures, we recommend that covered entities with paper record systems or other media be required to issue similar written documentation of disclosures for TPO purposes upon request by the individual.

(45) How often do individuals and covered entities mistake the signature or acknowledgment line that accompanies NPPs as contracts, waivers of rights, or required as a condition of receiving services? What conflicts have arisen because of these or other misunderstandings?

LAC Response to Question 45:
Some stakeholders (including patients and their families, covered entities, and policymakers) continue to mistakenly consider the acknowledgement line for NPPs as creating a contract or written consent for the release of PHI. OCR should investigate the best ways to clarify and indicate that NPPs are for notification purposes and are not considered as a contract or waiver.
(46) What other state and federal laws, guidelines or standards require covered health care providers to obtain the patient’s acknowledgement or signature on a document at their first visit? How many of those documents require patient signatures? What is the nature of those other documents that require signatures?

LAC Response to Question 46:
Many substance use disorder treatment programs require patients to sign consent forms upon the first visit in order to authorize disclosure of Part 2-protected information to the patient’s insurance company, for the purpose of payment. Treatment programs may also request—but not require—patients to sign a consent form authorizing disclosure to the following recipients, in order to better coordinate care: emergency contact; primary care doctor and other treatment providers; and parent/guardian for minor patients.

Substance use disorder treatment programs that meet the definition of a federally-assisted “program” under 42 CFR Part 2 must also provide patients with a privacy notice explaining the privacy protections for substance use disorder treatment records. This notice may be combined with the HIPAA NPP in a single form.

State laws may also require patients to sign a written consent form for treatment purposes.

(51) What benefits or adverse consequences may result if OCR removes the requirement for a covered health care provider that has a direct treatment relationship with an individual to make a good faith effort to obtain an individual’s written acknowledgment of the receipt of the provider’s NPP? Please specify whether identified benefits or adverse consequences would accrue to individuals or covered providers.

LAC Response to Question 51:
Eliminating the requirement for the provider (who has a direct treatment relationship with a patient) to make a good faith effort to obtain the patient’s acknowledgement of receipt of the provider’s NPP would result in a lost opportunity for both providers and patients, as well as adverse consequences. In this circumstance, providers would not have any indication that their patients have been informed of the possible disclosures and recipients of their PHI. Without the written acknowledgement requirement of receipt of the NPP, treating providers may overlook or forget to verbally inform their patients about the possible recipients of the patients’ PHI. Similarly, if patients do not receive the NPP, they would not
be informed enough to inquire about the disclosures and/or the potential recipients of their PHI with their treating provider.

(53) With the assistance of consumer oriented focus groups, OCR has developed several model NPPs, available at https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/model-notices-privacy-practices/index.html, that clearly identify, in a consumer-friendly manner, an individual’s HIPAA rights and a covered entity’s ability to use and disclose PHI. (b) OCR has received anecdotal evidence that individuals are not fully aware of their HIPAA rights. What are some ways that individuals can be better informed about their HIPAA rights and how to exercise those rights? For instance, should OCR create a safe harbor for covered entities that use the model NPPs by deeming entities that use model NPPs compliant with the NPP content requirements? Would a safe harbor create any unintended adverse consequences?

LAC Response to Question 53(b):
LAC recommends that OCR support efforts to inform individuals, families, and caregivers of federal and state privacy rights, including Part 2, HIPAA, and applicable state laws. To do so, OCR should work jointly with SAMHSA to provide ongoing technical assistance and outreach to covered entities, and organizations that represent patients, families, and caregivers on issues such as how PHI can be shared within health systems and among providers, while maintaining patient privacy rights; and consent requirements to disclose sensitive health information.

(54) In addition to the specific topics identified above, OCR welcomes additional recommendations for how the Department could amend the HIPAA Rules to further reduce burden and promote coordinated care. (a) What provisions of the HIPAA Rules may present obstacles to, or place unnecessary burdens on, the ability of covered entities and/business associates to conduct care coordination and/or case management? What provisions of the HIPAA Rules may inhibit the transformation of the health care system to a value-based health care system? (b) What modifications to the HIPAA Rules would facilitate efficient care coordination and/or case management, and/or promote the transformation to value-based health care? (c) OCR also broadly requests information and perspectives from regulated entities and the public about covered entities’ and business associates’ technical capabilities, individuals’ interests, and ways to achieve these goals.

LAC Response to Question 54:
Covered entities and business associates may not have the technical capability to comply with health privacy law due to the shortcomings of recent financial incentives to adopt new technology. Health
information technology that permits integrated record management while maintaining patient privacy preferences currently exists, and is necessary for covered entities' electronic health records to comply with privacy laws, including HIPAA as well as 42 CFR Part 2 and state laws that provide greater privacy protections for sensitive health information. However, the HITECH incentives did not include a requirement that health information technology comply with applicable privacy laws, and not all covered entities were eligible for the funding. In particular, behavioral health providers - which play a critical role in addressing the opioid epidemic - were not eligible for this crucial funding. Any new federal funding incentives for covered entities to adopt health information technology should include a requirement that the technology comply with federal and state privacy laws.

The importance of maintaining individuals' health privacy is only increasing, in the face of increasing data breaches and the rapidly developing marketplaces for raw data.36

In conclusion, the Legal Action Center looks forward to working with your agency to support efforts to strengthen patient privacy rights to integrate and coordinate health care services. If you should have any questions about these recommendations, please contact Deborah Reid, Senior Health Policy Attorney at (202) 544-5478 or dreid@lac.org.

Sincerely,

Paul Samuels  
Director/President

---