4153-01-P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

[Docket No.: HHS-OCR-0945-AA00]

45 CFR Parts 160 and 164

RIN 0945-AA00

Request for Information on Modifying HIPAA Rules to Improve Coordinated Care

AGENCY: Office for Civil Rights (OCR), HHS.

ACTION: Request for information.

SUMMARY: The Office for Civil Rights (OCR) is issuing this Request for Information (RFI) to assist OCR in identifying provisions of the Health Insurance Portability and Accountability Act privacy and security regulations that may impede the transformation to value-based health care or that limit or discourage coordinated care among individuals and covered entities (including hospitals, physicians, and other providers, payors, and insurers), without meaningfully contributing to the protection of the privacy or security of individuals' protected health information. This RFI requests information on whether and how the rules could be revised to promote these goals, while preserving and protecting the privacy and security of such information and individuals' rights with respect to it.

DATES: Comments must be submitted on or before [INSERT DATE 60 DAYS AFTER PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: You may send comments, identified by RIN 0945-AA00 or Docket HHS-OCR-0945-AA00, by any of the following methods:

• *Federal eRulemaking Portal.* You may submit electronic comments at http://www.regulations.gov by searching for the Docket ID number HHS-OCR-0945-AA00. Follow the instructions for sending comments.

• *Hand-Delivery or Regular, Express, or Overnight Mail:* U.S. Department of Health and Human Services, Office for Civil Rights, Attention: RFI, RIN 0945-AA00, Hubert H. Humphrey Building, Room 509F, 200 Independence Avenue, SW, Washington, DC 20201.

Instructions: All submissions received must include "Department of Health and Human Services, Office for Civil Rights RIN 0945-AA00" for this RFI. All comments received will be posted without change to http://www.regulations.gov, including any personal information provided. Further instructions are available under PUBLIC PARTICIPATION.

Docket: For complete access to the docket to read background documents or comments received, go to http://www.regulations.gov and search for Docket ID number HHS-OCR-09454-AA00.

FOR FURTHER INFORMATION CONTACT: Marie Meszaros at (800) 368–1019 or (800) 537–7697 (TDD).

SUPPLEMENTARY INFORMATION:

I. Background

This RFI seeks public input on the regulations issued pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA)[1] and modified pursuant to, among other laws, the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009.[2] The HIPAA Privacy and Security Rules protect individuals' medical records and other

[1] *See* the Administrative Simplification provisions of title II, subtitle F, of the HIPAA (Pub. L. 104-191), which added a new part C to title XI of the Social Security Act (sections 1171–1179 of the Social Security Act, 42 U.S.C. 1320d–1320d–8) and included section 264, under which HHS has adopted the HIPAA Privacy Rule.

[2] The HITECH Act was enacted as title XIII of division A and title IV of division B of the American Recovery and Reinvestment Act of 2009 (ARRA) (Pub. L. 111-5).

individually identifiable health information created or received by or on behalf of covered entities, known as "protected health information" (PHI).[3] The Privacy and Security Rules limit the circumstances under which covered entities may use and disclose PHI and require covered entities to implement safeguards to protect the privacy and security of PHI. The Privacy Rule also gives individuals rights with respect to their PHI, including the right to access their PHI and to receive adequate notice of a covered entity's privacy practices. In addition, the HIPAA Breach Notification Rule requires HIPAA covered entities to provide notification following a breach of unsecured PHI to individuals and OCR (and, in some instances, the media) and requires business associates to notify the relevant covered entities of such breaches.[4] In this RFI, the Privacy, Security, and Breach Notification Rules will be referenced collectively as the HIPAA Rules.

OCR seeks public input on ways to modify the HIPAA Rules to remove regulatory obstacles and decrease regulatory burdens in order to facilitate efficient care coordination and/or case management and to promote the transformation to value-based health care, while preserving the privacy and security of PHI. Specifically, OCR seeks information on the provisions of the HIPAA Rules that 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, or that may inhibit the transformation of the health care system to a value-based health care system. Correspondingly, OCR seeks comment on modifications to the HIPAA Rules that would facilitate efficient care coordination and/or case management, and/or promote the transformation to value-based health care. OCR also broadly requests information and perspectives from

[3] *See* the HIPAA Privacy and Security Rules at 45 CFR Part 160 and Subparts A, C, and E of Part 164.
[4] *See* 45 CFR Part 160 and Part 164, Subparts A and D.

regulated entities and the public about covered entities' and business associates' technical capabilities, individuals' interests, and ways to achieve these goals.

In addition, OCR seeks comment on aspects of the Privacy Rule that OCR has identified for potential modification to further these goals, specifically:

- Promoting information sharing for treatment and care coordination and/or case management by amending the Privacy Rule to encourage, incentivize, or require covered entities to disclose PHI to other covered entities.
- Encouraging covered entities, particularly providers, to share treatment information with parents, loved ones, and caregivers of adults facing health emergencies, with a particular focus on the opioid crisis.
- Implementing the HITECH Act requirement to include, in an accounting of disclosures, disclosures for treatment, payment, and health care operations (TPO) from an electronic health record (EHR) in a manner that provides helpful information to individuals, while minimizing regulatory burdens and disincentives to the adoption and use of interoperable EHRs.
- Eliminating or modifying the requirement for covered health care providers to make a good faith effort to obtain individuals' written acknowledgment of receipt of providers' Notice of Privacy Practices, to reduce burden and free up resources for covered entities to devote to coordinated care without compromising transparency or an individual's awareness of his or her rights.

II. Solicitation of Comments

OCR is soliciting public comments that offer recommendations for modifying existing regulations or guidance, or developing new guidance, that could further the goals described below.

a. Promoting information sharing for treatment and care coordination.

The Privacy Rule establishes an individual's right to access and obtain a copy of his or her PHI.[5] The Privacy Rule currently requires a covered entity to provide an individual with access to his or her PHI within 30 days after receipt of a request (with the possibility of one 30-day extension), and requires the covered entity to provide a copy of PHI to a third party, which may be a health care provider, when directed by an individual pursuant to the individual's right of access. These requirements apply equally to health records maintained electronically and in other media (*e.g.*, paper). OCR seeks input on whether potential revisions to the right of access would support and promote care coordination and/or case management by enabling more timely transfer of PHI between covered entities, or between covered entities and other health care providers.

Currently, under the Privacy Rule, the only required disclosures of PHI are (1) to the individual, pursuant to the individual's right to access, 45 CFR 164.524; and (2) to OCR for purposes of determining compliance with the HIPAA Rules. The Privacy Rule permits, but does not require, covered entities to use and disclose PHI for TPO purposes.[6] Further, although

[5] See 45 CFR 164.524.

[6] "Treatment means the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another." 45 CFR 164.501 (definition of "treatment"); also see 45 CFR 164.502(a)(1)(ii) and 164.506. The definition of "health care operations" includes, but is not limited to "any of the following activities of the covered entity to the extent that the activities are related to covered functions: (1) Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; patient safety activities (as defined in 42 CFR 3.20); population-based activities

the Privacy Rule requires covered entities to provide individuals with access to their PHI within 30 days of receiving a request (with the possibility for one 30-day extension),[7] there is no deadline or requirement to disclose records when requested by another health care provider or other covered entity for purposes of coordinating care or managing cases. This can lead to circumstances where records are not transferred between covered entities (or from a covered entity to another health care provider) in a timely fashion to the detriment of coordinated care and/or case management. OCR seeks public input, including from individuals, covered entities, other health care providers, business associates, and other members of the public, on the scope of this problem, and on whether there are potential revisions to the Privacy Rule to support and promote care coordination and/or case management, including by requiring timely transfer of PHI for this purpose or other purposes, such as when a patient switches medical providers and their new provider requests the transfer of records from the previous provider.

The Privacy Rule generally requires that covered entities use, disclose, or request only the minimum PHI necessary to meet the purpose of the use, disclosure, or request.[8] Disclosures to or requests by health care providers for treatment purposes, including care coordination and case management, are excepted from the minimum necessary requirement.[9] Disclosures by covered entities for care coordination and/or case management activities to covered entities that are not health care providers remain subject to the minimum necessary standard.[10] Similarly, disclosures related to care coordination and/or case management but for non-treatment activities nevertheless remain subject to the minimum necessary standard, such as population-based case

---

relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment; . . . ."

[7] 45 CFR 164.524(b)(2)(i).

[8] 45 CFR 164.502(b)(1).

[9] 45 CFR 164.502(b)(2)(i).

[10] Id.

management and care coordination activities,[11] claims management, review of health care services for appropriateness of care, utilization reviews,[12] and formulary development.[13] OCR seeks input on whether disclosures of PHI to non-provider covered entities for care coordination and/or case management as part of treatment, and/or health care operations, should be excepted from the minimum necessary standard, and if so, to what extent.

Finally, some individuals, such as those experiencing homelessness or suffering from chronic conditions, including serious mental illness, receive care from a variety of sources including HIPAA covered entities, social service agencies, and community-based support programs. In addition, some jurisdictions have established multi-disciplinary teams that assist in coordinating the full spectrum of care for individuals who need such assistance. Coordinating the care and related services requires sharing PHI among those involved. Although the Privacy Rule permits a covered health care provider to disclose information to a third party for the coordination or management of treatment,[14] some HIPAA covered entities have expressed reluctance to share this information for fear of violating HIPAA. OCR therefore requests input on whether it should modify or otherwise clarify provisions of the Privacy Rule to encourage covered entities to share PHI with non-covered entities when needed to coordinate care and provide related health care services and support for individuals in these situations. This request asks whether an express regulatory permission should be created for HIPAA covered entities to disclose PHI to social service agencies or community-based support programs, and the requirements or conditions upon which the regulatory permission should be based, including whether covered entities should be required to enter into agreements with such

[11] *See* 45 CFR 164.501 (definitions of "health care operations," para. (1)).
[12] *See* 45 CFR 164.501 (definition of "payment").
[13] *See* 45 CFR 164.501 (definition of "health care operations," para. (6)).
[14] 45 CFR 164.501 (definition of "treatment").

entities that contain provisions similar to the provisions in business associate agreements.[15] For all questions, we request information about any relevant state or other law containing standards that are different from, and perhaps inconsistent with, either existing HIPAA requirements or potential proposed changes to the HIPAA Rules.

OCR requests comment on these issues, including on the following questions:

1) How long does it take for covered entities to provide an individual with a copy of their PHI when requested pursuant to the individual's right of access at 45 CFR 164.524? How long does it take for covered entities to provide other covered entities copies of records that are not requested pursuant to the individual's right of access? Does the length of time vary based on whether records are maintained electronically or in another form (*e.g.*, paper)? Does the length of time vary based on the type of covered entity? For instance, do some types of health care providers or plans take longer to respond to requests than others?

2) How feasible is it for covered entities to provide PHI when requested by the individual pursuant to the right of access more rapidly than currently required under the rules? (The Privacy Rule requires covered entities to respond to a request in no more than 30 days, with a possible one-time extension of an additional 30 days.). What is the most appropriate general timeframe for responses? Should any specific purposes or types of access requests by patients be required to have shorter response times?

3) Should covered entities be required to provide copies of PHI maintained in an electronic record more rapidly than records maintained in other media when responding to an individual's request for access? (The Privacy Rule does not currently distinguish, for

[15] See 45 CFR 164.502(a)(3), 164.504(e)(2)

timeliness requirements, between providing PHI maintained in electronic media and PHI maintained in other media). If so, what timeframes would be appropriate?

4) What burdens would a shortened timeframe for responding to access requests place on covered entities? OCR requests specific examples and cost estimates, where available.

5) Health care clearinghouses typically receive PHI in their role as business associates of other covered entities, and may provide an individual access to that PHI only insofar as required or permitted by their business associate agreement with the other covered entity, just as other covered entities, when performing business associate functions, may also provide access to PHI only as required or permitted by the business associate agreement(s) with the covered entity(ies) for whom they perform business associate functions. Nevertheless, the PHI that clearinghouses possess could provide useful information to individuals. For example, clearinghouses may maintain PHI from a variety of health care providers, which may help individuals obtain their full treatment histories without having to separately request PHI from each health care provider.

   a) How commonly do business associate agreements prevent clearinghouses from providing PHI directly to individuals?

   b) Should health care clearinghouses be subject to the individual access requirements, thereby requiring health care clearinghouses to provide individuals with access to their PHI in a designated record set upon request? Should any limitations apply to this requirement? For example, should health care clearinghouses remain bound by business associate agreements with covered entities that do not permit disclosures of PHI directly to an individual who is the subject of the PHI?

c) Alternatively, should health care clearinghouses be treated only as covered entities—i.e., be subject to all requirements and prohibitions in the HIPAA Rules concerning the use and disclosure of PHI and the rights of individuals in the same way as other covered entities—and not be considered business associates, or need a business associate agreement with a covered entity, even when performing activities for, or on behalf of, other covered entities? Would this change raise concerns for other covered entities about their inability to limit uses and disclosures of PHI by health care clearinghouses? For example, would this change prevent covered entities from providing assurances to individuals about how their PHI will be used and disclosed? Or would covered entities be able to adequately fulfill individuals' expectations about uses and disclosures through normal contract negotiations with health care clearinghouses, without the need for a HIPAA business associate agreement? Would covered entities be able to impose other contractual limitations on the uses and disclosures of PHI by the health care clearinghouse?

d) If health care clearinghouses are not required to enter into business associate agreements with the other covered entities for whom they perform business associate functions, should such requirement also be eliminated for other covered entities when they perform business associate functions for other covered entities?

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.

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?

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?

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 non-covered health care provider.[16] 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 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?

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.

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

[16] *See* 45 CFR 164.506(c)(1)-(3).

notes or other specific types of PHI (such as genetic information) be excluded from the disclosure requirement unless expressly authorized by the individual?

12) What timeliness requirement should be imposed on covered entities to disclose PHI that another covered entity requests for TPO purposes, or a non-covered health care provider requests for treatment or payment purposes? Should all covered entities be subject to the same timeliness requirement? For instance, should covered providers be required to disclose PHI to other covered providers within 30 days of receiving a request? Should covered providers and health plans be required to disclose PHI to each other within 30 days of receiving a request? Is there a more appropriate timeframe in which covered entities should disclose PHI for TPO purposes? Should electronic records and records in other media forms (*e.g.*, paper) be subject to the same timeliness requirement? Should the same timeliness requirements apply to disclosures to non-covered health care providers when PHI is sought for the treatment or payment purposes of such health care providers?

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?

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?

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?

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?[17]

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?

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

[17] Sec 4004, Pub. L. 114-255, 130 Stat. 1033 (amending Subtitle C of title XXX of the Public Health Service Act by adding Sec. 3022(a)(3)).

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?

19) Should OCR expressly permit disclosures of PHI to multi-disciplinary/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 multi-disciplinary teams that include law enforcement officials only if such teams are established through a drug court program?[18] Should such a multi-disciplinary 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?

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,

[18] Information about drug courts is available at https://www.nij.gov/topics/courts/drug-courts/Pages/welcome.aspx.

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?

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?

b. Promoting parental and caregiver involvement and addressing the opioid crisis and serious mental illness

As discussed earlier, the Privacy Rule allows covered entities to disclose PHI to caregivers in certain circumstances, including certain emergency circumstances, and this permission has particular relevance today in relation to the opioid crisis and efforts to address serious mental illness (SMI).[19] Nevertheless, anecdotal evidence suggests that some covered entities are reluctant to inform and involve the loved ones of individuals facing such health crises for fear of violating HIPAA. This reluctance may hinder effective coordination of care and case management involving caregivers, including family members and friends. In an effort to encourage covered entities to share necessary information with caregivers and loved ones, especially when an individual is suffering from substance use disorder (including opioid use disorder) or SMI, OCR is considering a separate rulemaking that would seek to encourage covered entities to share PHI with family members, caregivers, and others in a position to avert threats of harm to health and safety, when necessary to promote the health and recovery of those

[19] *See, e.g.*, 45 CFR 164.510(b)(3), 45 CFR 164.512(j).

struggling with substance use disorder, including opioid use disorder, and/or SMI.[20] OCR would like to consider amendments to the Privacy Rule that would allow OCR to address the opioid crisis as well as facilitate parental involvement in the treatment of their children.

Specifically, OCR requests comment on these issues, including the following:

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?

23) How can OCR amend the HIPAA Rules to address serious mental illness? For example, are there changes that would facilitate treatment and care coordination for individuals with SMI, or ensure that family members and other caregivers can be involved in an individual's care? What are the perceived barriers to facilitating this treatment and care coordination? Would encouraging more sharing in the context of SMI create concerns similar to any concerns raised in relation to the previous question on the opioid epidemic? If so, how could such concerns be mitigated?

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.

[20] See RIN: 0945-AA09, Fall 2018 Unified Agenda, Office of Information and Regulatory Affairs, Office of Management and Budget, www.reginfo.gov.

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.[21] 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?[22] Or are existing permissions sufficient? For instance, should a child be

[21] *See* 45 CFR 164.502(g)(3).
[22] *See* 45 CFR 164.502(g).

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?

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.[23] 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?

c. Accounting of disclosures

The Privacy Rule requires covered entities to provide an individual, upon request, with an accounting of certain disclosures of the individual's PHI that were made by the covered entity or its business associate during the six years before the request. See 45 CFR 164.528. While the Privacy Rule currently excludes certain disclosures from the accounting requirement, including disclosures made for TPO purposes, *see* 45 CFR 164.528(a), section 13405(c) of the HITECH Act directs the Department to modify the Privacy Rule to require that an accounting of disclosures include disclosures made for TPO purposes through an electronic health record during the three years before the request.

In 2010, OCR issued a Request for Information ("2010 RFI")[24] "to help us better understand the interests of individuals with respect to learning of such disclosures [for TPO], the administrative burden on covered entities and business associates of accounting for such disclosures, and other information that may inform the Department's rulemaking in this area." After reviewing public comments, OCR issued a Notice of Proposed Rulemaking ("2011

[23] *See* 45 CFR 164.502(g).
[24] 75 FR 23214 (May 3, 2010). Available at https://www.gpo.gov/fdsys/pkg/FR-2010-05-03/pdf/2010-10054.pdf.

NPRM")[25] proposing several modifications to the Privacy Rule to implement the HITECH Act requirement, improve the workability of the accounting of disclosures, and create a new right to an access report.

Based on public feedback on the RFI that many covered entities' systems could not distinguish between internal access (a "use" under the Privacy Rule) and external access (a "disclosure") for TPO, and that providing a full accounting of disclosures for TPO would be overly burdensome to regulated entities, OCR proposed, in addition, to provide individuals with a right to receive an "access report." The access report would have shown who had accessed the information in an individual's electronic designated record set (which would include any access, not only access that represented a disclosure outside of the entity for TPO). Commenters on the NPRM overwhelmingly opposed the proposed individual right to obtain an "access report." Many commenters expressed concern that their then-existing, commonly used EHR systems did not have the technical capability to produce the required access report and updates would be prohibitively costly for covered entities. In addition, some commenters stated that the content and format of the proposed access report would not provide meaningful, usable information to individuals. A virtual hearing conducted by a federal advisory committee in 2013 elicited similar concerns from the public and presenters at the hearing.[26]

OCR has not taken action to finalize the proposed accounting of disclosures rule since the comment period closed in 2011, and it now believes that the proposed access report requirement would create undue burden for covered entities without providing meaningful information to individuals. Thus, OCR intends to withdraw the NPRM, and requests public input on the questions below to help OCR to implement the HITECH Act requirement and ensure that

[25] 76 FR 31426 (May 31, 2011). Available at https://www.gpo.gov/fdsys/pkg/FR-2011-05-31/pdf/2011-13297.pdf.
[26] https://www.healthit.gov/hitac/events/policy-privacy-security-tiger-team-accounting-disclosures-virtual-hearing.

individuals can obtain a meaningful accounting of disclosures that gives them confidence that their PHI is being disclosed appropriately as part of receiving coordinated care or otherwise, without erecting obstacles or disincentives to the adoption and use of interoperable electronic healthcare records, which is necessary for efficient care coordination, case management, and value-based healthcare.

OCR requests public input on these issues and specifically on following questions:

27) How many requests for an accounting of disclosures do covered entities receive annually and from what percentage of total patients? Of these, how many requests specify a particular preferred electronic form or format, and to what extent do covered entities provide the accounting in the requested form or format?

28) How much time do covered entities take to respond to an individual's request for an accounting of disclosures? How many worker-hours are needed to produce the accounting? What is the average number of days between receipt of a request and providing the accounting to the requesting individual? How would these estimated time periods change, if at all, if covered entities were to provide a full accounting of disclosures for TPO purposes? What is the basis for these revised estimates?

29) If your covered entity does capture and maintain information about TPO accounting, even though it is not currently required by the Privacy Rule, what is the average number of TPO disclosures made by the entity for a given individual in a calendar year? How many such disclosures are made from EHRs?

30) In what scenarios would a business associate make a disclosure of PHI for TPO through an EHR? What is the average number of such disclosures for a given individual in a calendar year, if known?

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?

32) For existing EHR systems:

a) Is the system able to distinguish between "uses" and "disclosures" as those terms are defined under the Privacy Rule at 45 CFR 160.103? (Note that the term "disclosure" includes, but is not limited to, the sharing of information between a hospital and physicians who may have staff privileges but who are not members of its workforce).

b) If the existing system only records access to information without identifying whether such access represents a use or disclosure, what information is recorded about each instance of access? How long is such information retained? What would be the burden for covered entities to retain the information for three years? Once collected, what additional costs or other resources would be required to maintain the data for each subsequent year? At what point would retention of the information be excessively burdensome? OCR requests specific examples and cost estimates, where available.

c) If the system is able to distinguish between uses and disclosures of information, what details regarding each disclosure are automatically collected by the system (*i.e.*, collected without requiring any additional manual input by the person making the disclosure)? What information, if any, is manually entered by the person making the disclosure or accessing the information?

d) If the system is able to distinguish between uses and disclosures of information, what data elements are automatically collected by the system for uses (*i.e.*, collected without requiring any additional manual input by the person making the disclosure)? What information, if any, is manually entered by the person making the use?

e) If the system is able to distinguish between uses and disclosures of information, does it record a description of disclosures in a standardized manner (for example, does the system offer or require a user to select from a limited list of types of disclosures)? If yes, is the feature being utilized? What are the benefits and drawbacks?

f) To what extent do covered entities maintain a single, centralized EHR system versus a decentralized system (*e.g.*, different departments maintain different EHR systems, and an accounting of disclosures for TPO would need to be tracked for each system)? To what extent are covered entities that currently use decentralized systems planning to migrate to centralized systems or vice versa? How is the industry mix of centralized and decentralized systems likely to change over the next five or ten years?

g) Do existing EHR systems automatically generate an accounting of disclosures under the current Privacy Rule (*i.e.*, does the system account for disclosures other than to carry out TPO)? If so, what would be the additional burden to also account for disclosures to carry out TPO? If not, to what extent do covered entities use a separate system or module to generate an accounting of disclosures, and does the system interface with the EHR system? OCR requests cost estimates, where available.

33) If an EHR is not currently able to account for disclosures of an EHR to carry out TPO, what would be the burden, in time and financial costs, for covered entities and/or their vendors to implement such a feature?

34) For covered entities already planning to adopt new EHRs, to what extent would a requirement to track TPO disclosures affect the cost of the new system?

35) A covered entity's Notice of Privacy Practices 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?

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?

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?

38) How frequently do individuals who obtain an accounting of disclosures request additional information not currently required to be included in the accounting (*e.g.*, information about internal uses or about disclosures for TPO)? What additional information do they request, and do covered entities provide the additional information? Why or why not?

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?

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?

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?

42) Please provide any other information that OCR should consider when developing a proposed rule on accounting for disclosures for TPO.

d. Notice of Privacy Practices

The Privacy Rule requires covered providers and health plans to develop a Notice of Privacy Practices (NPP) that describes individuals' heath information privacy rights and how their health information may be used and disclosed by the covered entity.[27] Covered entities are required to provide their NPPs to individuals, consistent with the specific requirements of the Privacy Rule, including prominent display on their websites. In addition, a covered health care provider that has a direct treatment relationship with the individual must clearly and prominently post the NPP in physical service delivery locations. Providers must also provide the NPP to individuals by the date of first service delivery, and to any individual upon request.

In addition, the Privacy Rule requires covered providers that have a direct treatment relationship with an individual to make a good faith effort to obtain a written acknowledgement of receipt of the provider's NPP. If providers are unable to obtain the written acknowledgement, they must document their good faith efforts and the reason for not obtaining an individual's acknowledgment, and the provider must maintain the documentation or sufficient proof to

[27] 45 CFR 164.520.

support compliance with the requirements for six years.[28] OCR established the requirement to make a good faith attempt to obtain a written acknowledgment in the August 14, 2002, final Privacy Rule modifications (67 FR 53182). That final rule strengthened the notice requirements, in part, to replace the previous requirement to obtain an individual's consent for uses and disclosures of PHI for treatment, payment, and health care operations, which would have created unnecessary barriers to the provision of health care and other routine and important health sector activities. The written acknowledgment process was intended to provide an opportunity for the individual to review the NPP, including the individual's privacy rights, to discuss any concerns related to the privacy of her or his PHI, and to request additional restrictions or confidentiality of communications.

The questions below seek public input on whether the signature and recordkeeping requirements should be eliminated to reduce burden on providers and to free up time and resources for providers to spend on treatment and care coordination. The questions also ask how the NPP requirements might be modified in other ways to alleviate covered entity burden without compromising transparency regarding providers' privacy practices or an individual's awareness of his or her rights.

43) What is the burden, in economic terms, for covered health care providers that have a direct treatment relationship with an individual to make a good faith effort to obtain an individual's written acknowledgment of receipt of the provider's NPP? OCR requests estimates of labor hours and any other costs incurred, where available.

[28] 45 CFR 164.520(c)(2)(ii) and (e).

44) For what percentage of individuals with whom a direct treatment provider has a relationship is such a covered health care provider unable to obtain an individual's written acknowledgment? What are the barriers to obtaining it?

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?

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?

47) How often are NPPs bundled with other documents at patient "intake" and with how many other pages of documents? How often are NPPs printed with non-NPP materials, either on the same page, or as a continuation of one integrated document, or as being physically attached to other documents? What is the nature of these non-NPP materials? How often, if at all, are covered health care providers required to have the patient sign updated versions of these forms (*e.g.*, annually, each visit, no subsequent updates required)? Are electronic signatures permitted for these forms? If so, does this make the process less burdensome?

48) If NPP training is part of your general annual training, how much of this training cost do you estimate your organization spends to train covered entity staff on their obligations to seek and maintain documents related to the NPP acknowledgment requirements?

49) What is the burden, in economic terms, for covered health care providers to maintain documentation of the acknowledgment or the good faith effort to obtain written acknowledgement and the reason why the acknowledgment was not obtained? What

alternative methods might providers find useful to document that they provided the NPP? For example, to what extent would the use of a standard patient intake checklist reduce the burden?

50) What use, if any, do covered health care providers make of the signed NPP forms, or documentation of good faith efforts at securing written acknowledgments, that the Privacy Rule requires providers to maintain?

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.

52) Are there modifications to the content and provision of NPP requirements that would lessen the burden of compliance for covered entities while preserving transparency about covered entities' privacy practices and individuals' awareness of privacy rights? Please identify specific benefits and burdens to the covered entity and individual, and offer suggested modifications.

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.

a) While covered entities are required to provide individuals an NPP, use of OCR's model NPPs is optional. Do covered entities use these model NPPs? Why or why not?

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?

c) Should more specific information be required to be included in NPPs than what is already required? If so, what specific information? For example, would a requirement of more detailed information on the right of patients to access their medical records (and related limitations of what can be charged for copies) be useful?

d) Please identify other specific recommendations for improving the NPP text or dissemination requirements to ensure individuals are informed of their HIPAA rights.

e. Additional ways to remove regulatory obstacles and reduce regulatory burdens to facilitate care coordination and promote value-base health care transformation

As noted at the beginning of this RFI, OCR seeks public input on ways to modify the HIPAA Rules to remove regulatory obstacles and decrease regulatory burdens in order to facilitate efficient care coordination and/or case management and promote the transformation to value-based health care, while preserving the privacy and security of PHI. Specifically:

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.

This is a request for information only. Respondents are encouraged to provide complete but concise responses to the questions outlined above. OCR also requests that commenters indicate throughout their responses the questions to which they are responding. OCR notes that a response to every question is not required. This request for information is issued solely for information and planning purposes; it does not constitute a notice of proposed rulemaking.

III. Collection of Information Requirements

This document does not impose information collection requirements, that is, reporting, recordkeeping or third-party disclosure requirements. This request for information constitutes a general solicitation of comments. In accordance with the implementing regulations of the Paperwork Reduction Act (PRA) at 5 CFR 1320.3(h)(4), information subject to the PRA does not generally include "facts or opinions submitted in response to general solicitations of comments from the public, published in the **Federal Register** or other publications, regardless of the form or format thereof, provided that no person is required to supply specific information pertaining to the commenter, other than that necessary for self-identification, as a condition of the agency's full consideration of the comment." Consequently, this document need not be

reviewed by the Office of Management and Budget under the authority of the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 *et seq.*).

Dated: December 10, 2018

_____

Alex M. Azar II

Secretary,

Department of Health and Human Services.

[FR Doc. 2018-27162 Filed: 12/12/2018 11:15 am; Publication Date: 12/14/2018]