COPPERSMITH BROCKELMAN LAWYERS

UPDATE: On March 9, 2021, the U.S. Department of Health and Human Service, Office for Civil Rights (OCR) announced a 45-day extension of the public comment period noted below, so the current deadline to submit comments to the proposed changes is May 6, 2021.

Proposed Changes to the HIPAA Privacy Rule: The Good, The Bad and The Ugly – An Operational Perspective

Erin Dunlap, Kristen Rosati, Melissa Soliz, Coppersmith Brockelman PLC
January 26, 2021

On January 21, 2021, the U.S. Department of Health and Human Service, Office for Civil Rights (OCR) published proposed changes to the HIPAA Privacy Rule in the Federal Register.[1] Public comments on these proposed changes are due in 60 days after publication, or by March 22, 2021. Please contact us if you would like further information or assistance with submitting comments.

According to OCR, these proposed changes are intended "to support individuals' engagement in their care, remove barriers to coordinated care, and reduce regulatory burdens on the health care industry."[2] While these are important goals for the transformation to value-based health care, most health care providers and health plans want to know how the proposed changes will impact operations. In this alert, we categorize the key changes in terms of operational impact: the good, the bad and the ugly. We also offer some guidance on likely implementation steps.

The Good: Reduction of Regulatory Burden

We are enthusiastic about the proposed changes that would reduce regulatory obligations on HIPAA covered entities (CEs) and allow for greater data sharing for care coordination and care management activities:

- ***No Acknowledgement of NPP*** – Change to 45 C.F.R. § 164.520. Under the proposed changes, CEs would no longer be required to get a written acknowledgment of receipt of the Notice of Privacy Practices (NPP). Some CEs have struggled with how to obtain and maintain these acknowledgments, particularly when the NPP is provided electronically, so this is a welcome change.

    - Implementation Steps: This change would eliminate the regulatory requirement (and corresponding liability) to obtain an acknowledgement, but CEs may continue to do so if they do not want to make changes to current operations. If a

[1] 86 Fed. Reg. 6448 (January 21, 2021). The proposed changes can be found here. Please note, while the proposed rule has a publication date of January 21,2021, it appeared in the Federal Register on January 20, 2021. It is unclear whether the proposed rule is subject to the "regulatory freeze" issued by the new administration on January 20, 2021.

[2] *See* OCR's press release on the proposed changes here.

CE no longer wants to obtain the acknowledgment, it will need to revise its intake process and likely will need to revise the NPP and the NPP policy to remove references to the acknowledgment.

- ***Limited Right of Individuals to Direct Disclosure to Third Parties*** – Addition of 45 C.F.R. § 164.524(d). Under the current HIPAA rules, an individual has a right to direct a CE to send the individual's protected health information (PHI) to a third-party (often referred to as a "third-party directive").[3] In January 2020, a federal court vacated the third-party directive rule to the extent it went beyond requests to transmit an electronic copy of PHI maintained in an electronic health record (EHR).[4] The proposed changes would align the HIPAA rules with that federal court decision.

  The proposed changes also add a definition of EHR to the HIPAA rules. The proposed definition of EHR is:

  > *Electronic health record means an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and their staff.* ***Such clinicians shall include, but are not limited to, health care providers that have direct treatment relationships with individuals as defined at § 164.501, such as physicians, nurses, pharmacists, and other allied health professionals.*** *For purposes of this paragraph, "health-related information on an individual" covers the same scope of information as the term individually identifiable health information as defined at § 160.103.*[5]

  Although the plain language limiting the definition of EHR to clinicians with a direct treatment relationship includes the modifier "but are not limited to" those clinicians, OCR's commentary clearly demonstrates an intent to limit the application to direct treatment providers only. OCR explains in the preamble that only covered health care providers that have a direct treatment relationship with individuals will maintain an EHR under this proposed definition. OCR said it "does not propose to include covered health care providers who have indirect treatment relationships with individuals," which the HIPAA rules define as "providers that deliver health care based on the orders of another health care provider, and… typically provide services, products, or reports to another

[3] In the preamble to the proposed changes, OCR explains that the third-party directive right is distinct from the provision that permits a CE to disclose PHI to a third party with an individual's valid authorization in at least four key respects: (1) the mandatory versus permissive nature of the disclosure; (2) the manner in which the request is made (*e.g.*, with or without a form containing required elements); (3) the form and format of the information provided; and (4) the fees that may be charged. 86 Fed. Reg. at 6462

[4] In *Ciox Health LLC v. Azar, et al*., No. 18-cv-0040 (D.D.C. January 23, 2020), the U.S. District Court for the District of Columbia vacated certain parts of the third-party directive rule (among other provisions of the 2013 Final Omnibus Rule), finding that the rule unlawfully broadened the third-party directive to reach requests for PHI contained in any format, not just in an EHR. A copy of the decision can be found here. *See also* OCR's notice regarding the decision here.

[5] 86 Fed. Reg. at 6532 (amendments to 45 C.F.R. § 164.501) (emphasis added)

health care provider."[6]

OCR provided an example: "[T]he term EHR would not include health-related electronic records of [] providers that only supply durable medical equipment to other providers."[7] Another typical example of indirect treatment providers are clinical laboratories that are not part of a large health system (with a potential exception for consumer-ordered testing). OCR also stated that health plans do not maintain an EHR, so the rules relating to third party directives do not apply to health plans. OCR seeks comments on whether the EHR definition is too broad or not broad enough, and whether there are circumstances in which a health plan would create or maintain an EHR.

Overall, this proposed change is good for CEs because they would only be required to treat a third-party directive as an "access request" if CEs maintain the records in an EHR. On the downside, the proposed changes would allow individuals to submit a third-party directive orally, electronically or in writing. Under the current HIPAA rules, a third-party directive must be in writing.

- Implementation Steps: Unless a CE already made operational changes in response to the *Ciox Health* decision, this proposed change likely will require revisions to patient access and release of information (ROI) policies. A health plan (and possibly indirect treatment providers) will need to revise policies to remove references to the third-party directive right, which means these CEs will need to obtain patient authorization before releasing PHI to a third party unless otherwise permitted under the HIPAA rules. Other health care providers will need to consider whether they maintain records in an EHR, as defined in the final rule. If so, a provider will need to revise its access and ROI policies to limit the third-party directive right to electronic copies of PHI contained in EHR. If a covered health care provider does not maintain records in an EHR, or if the request is for a non-electronic copy or for information that resides outside an EHR, the provider will need to obtain patient authorization before releasing PHI to a third party unless otherwise permitted under the HIPAA rules.

- ***Limitations on Minimum Necessary Rule for Care Coordination and Case Management*** – Change to 45 C.F.R. § 164.502(b). The current minimum necessary rule (MNR) applies in most circumstances, other than treatment. This means most uses or disclosures of PHI must be limited to the minimum necessary to accomplish the intended purpose. However, under the proposed changes, the MNR would not apply to disclosures to or requests by a health plan for care coordination and case management activities with respect to an individual. This change is welcome because the determination of what

[6] 45 C.F.R. § 164.501 ("indirect treatment relationship means a relationship between an individual and a health care provider in which: (1) The health care provider delivers health care to the individual based on the orders of another health care provider; and (2) The health care provider typically provides services or products, or reports the diagnosis or results associated with the health care, directly to another health care provider, who provides the services or products or reports to the individual.")

[7] 86 Fed. Reg. at 6456

information may be provided to a health plan for these purposes consistent with the MNR often is not clear. The proposed changes also clarify that the MNR does not apply to disclosures to or requests by health care providers for treatment, including care coordination and case management activities with respect to an individual.

  - Implementation Steps: This change likely will require revisions to MNR policies and MNR provisions included in other policies.

- ***"Good Faith Belief" Standard and Presumption of Compliance*** – Changes to 45 C.F.R. §§ 164.502, 164.510 and 164.514. The proposed changes incorporate a "good faith belief" standard and presumption of compliance with the "good faith" standard (absent evidence of bad faith) when disclosing PHI in certain situations: (i) disclosures to a parent or guardian who is not the personal representative of an unemancipated minor under certain circumstances; (ii) uses or disclosures for a facility's directory under certain emergency circumstances; and (iii) disclosures to an individual's family or others involved in the individual's care under certain conditions. The presumption would also apply when a CE is acting on a good faith belief in making a disclosure to avert a serious threat to health or safety. This change will give covered health care providers more flexibility in sharing data in difficult circumstances. OCR requests comments on whether the good faith standard should be applied to other provisions of the HIPAA rules, including the personal representative provisions.

  - Implementation Steps: This change likely will require revisions to several disclosure policies and may require revisions to verification policies.

- ***Disclosures to Social Service-Type Organizations*** – Change to 45 C.F.R. § 164.506. While OCR issued guidance several years ago clarifying that PHI may be shared with certain social service-type organizations for purposes of treatment/continuity of care, the proposed changes would expressly allow CEs to disclose PHI to a social services agency, community-based organization, home and community-based services provider, or a similar third party that provides health or human services to an individual for individual-level care coordination and case management activities (regardless of whether the activities constitute "treatment" or "health care operations," as defined by the HIPAA rules). This change gives certainty and more flexibility to CEs wishing to care for the entire person and to advance the use of social determinants of health, but the MNR will continue to apply to disclosures to or requests by these types of organizations.

  - Implementation Steps: We think a new policy on disclosure to social service-type organizations will be warranted. Revisions to other policies to reflect this new policy may be necessary.

- ***Expanded Scope of Serious Threat to Health or Safety*** – Change to 45 C.F.R. § 164.512(j). The proposed rules would allow a CE to disclose PHI if the CE, in good faith, believes the disclosure is necessary to prevent a serious and reasonably foreseeable harm, or lessen a serious and reasonably foreseeable threat to the health or safety of a person or the public. The term "reasonably foreseeable" means:

> *[A]n ordinary person could conclude that a threat to health or safety exists and that harm to health or safety is reasonably likely to occur if a use or disclosure is not made, based on the facts and circumstances known at the time of the disclosure.*[8]

This is a departure from the use of the term "imminent" under the current HIPAA rules. OCR explained that the change would "further enable a health care provider to timely notify a family member that an individual is at risk of suicide, even if the provider cannot predict that a suicide attempt is likely to occur 'imminently.'"[9] The proposed changes also include a "heightened deference" to a determination made by a covered health care provider or one of its workforce members who specializes in assessing risk to health or safety, such as a licensed mental or behavioral health professional. This means there would be an express presumption that the provider has met the reasonably foreseeable standard. Overall, this change would give CEs greater ability and comfort in sharing data in difficult circumstances.

- Implementation Steps: This change likely will require revisions to any policy addressing the "serious threat to health or safety" exception.

The Bad: Increased Regulatory Burden

Some of the proposed changes create further limitations or obligations on CEs, and will require additional compliance measures:

- ***No Unreasonable Access Requirements*** – Change to 45 C.F.R. § 164.524(b). A CE would be prohibited from imposing "unreasonable" measures that impede individual access to PHI if a less burdensome measure is practicable. The proposed rules state that requiring individuals to complete a standard form containing only the information the CE needs to process the request is reasonable, but requiring an individual to fill out an extensive request form, to obtain notarization, or to submit a request in person or only through an online portal is not reasonable. OCR requests comments on any burdens that CEs believe may result from this proposed change.

  - Implementation Steps: This change will require a review of the steps an individual is required to take to request access to PHI, and the removal or revision of any requirement that could be deemed unreasonable. A CE will also need to make any corresponding changes in its policies and procedures. A CE may also want to explicitly state in its policies that it will not impose (and prohibits workforce members from imposing) unreasonable measures on individuals requesting access to PHI, with examples to guide compliance on the ground.

- ***No Unreasonable Verification Measures*** – Change to 45 C.F.R. § 164.514(h)(2)(v). Consistent with the prohibition on imposing unreasonable measures on individual access rights, the proposed change to 45 C.F.R. § 164.514(h)(2)(v) would prohibit a CE from

[8] 86 Fed. Reg. at 6533 (amendments to 45 C.F.R. § 164.512) (emphasis added)
[9] *Id.* at 6483

imposing unreasonable verification measures on the exercise of individual rights under the HIPAA rules, including access, amendment and accounting requests. An "unreasonable measure" is "one that causes an individual to expend unnecessary effort or resources when a less burdensome verification measure is practicable," considering technical capabilities, safeguards and security and cost.[10] Examples of an unreasonable measure include requiring an individual: (i) to provide proof of identity in person when remote verification is practicable; or (ii) to obtain notarization on a written request to exercise an individual right.[11]

- Implementation Steps: This change will require a review of steps an individual must take to exercise any right under HIPAA, and to change any requirements that could be deemed unreasonable. The CE will also need to make any corresponding changes in its policies and procedures, including any verification policies. A CE may also want to explicitly state in its policies that it will not impose (and prohibits its workforce members from imposing) unreasonable verification measures on individuals exercising their rights, with examples to guide compliance on the ground.

- ***Reduced Time to Respond to Access Requests*** – Change to 45 C.F.R. § 164.524(b). Under the proposed changes:

  - CEs would be required to fulfill a patient access request within 15 calendar days (versus the current 30-day requirement) with the opportunity for an extension of no more than 15 calendar days (versus the current 30-day extension). In proposing this change, OCR said it was persuaded by the fact that several states require patient access to health records in less than 30 calendar days.

  - CEs would be required to implement a written policy for prioritizing urgent or other high priority access requests (especially those related to health and safety) to limit the need to use a 15 calendar-day extension for such requests. Examples of urgent or high priority requests include "when an individual voluntarily reveals that the PHI is needed in preparation for urgent medical treatment, or the individual needs documentation of a diagnosis of severe asthma in order to bring medication to school the next day."[12]

  - When PHI is readily available at the point of care, such as an x-ray or ultrasound or lab results performed during or ancillary to an appointment, a provider would not be permitted to delay the individual's right to inspect such PHI. OCR anticipates that "the time and place where an individual obtains health care treatment generally would be considered a convenient time and place for an individual to inspect the PHI that is immediately available in the treatment

[10] 86 Fed. Reg. at 6534 (amendments to 45 C.F.R. § 164.514)
[11] *Id.* at 6493
[12] *Id.* at 6499

area."[13]

- Implementation Steps: These changes will require revisions to access and ROI policies and any instructions related to access described in the NPP. A CE will also want to train ROI personnel and point of care staff on new response requirements to make sure requests are processed (and escalated if needed) in a timely fashion.

- ***Requirement to Transmit PHI by Email or to Personal Health Application*** – Change to 45 C.F.R. § 164.524(c). A CE would be required to send PHI electronically at the individual's request, including by email or to or through an individual's personal health application (personal health app), if "readily producible"[14] to or through such an application. According to OCR: "More and more individuals use personal health [apps] to access and manage their personal health information, and [this proposal will] clarify that… one of the mechanisms by which a request for access can be fulfilled is by transmitting an electronic copy of an individual's PHI to a personal health [app] used by the individual."[15]

  Under the proposed changes, a "personal health application" means:

  > *an electronic application used by an individual to access health information about that individual, which can be drawn from multiple sources, provided that such information is managed, shared, and controlled by or primarily for the individual, and not by or primarily for a covered entity or another party such as the application developer.*[16]

  Put another way, a personal health app is a service offered directly to consumers; a personal health app is not acting on behalf of, or at the direction of a CE or another third party (such as a life insurance company, a research organization, or data aggregator). OCR requests comments on the proposed definition of personal health app.

  - Implementation Steps: This change likely will require revisions to access and ROI policies and discussions with information technology (IT) personnel. A CE will also want to train ROI personnel on these new response requirements.

- ***Required Notice If Summary Is Provided*** – Change to 45 C.F.R. § 164.524. Under the current HIPAA rules, a CE may provide an individual with a summary of PHI requested, in lieu of providing access to the PHI if (i) the individual agrees in advance to such summary, and (ii) the individual agrees in advance to the fees imposed, if any, for such

[13] *Id.* at 6457

[14] The preamble to the proposed rules includes quite a bit of commentary on form and format of access and what is considered "readily producible," such as any form or format required by applicable state and other laws, internet-based access and standards-based APIs. See 86 Fed. Reg. at 6455, 6461, 6491, 6499, 6504 and 6509. We do not cover this commentary in this alert, but it will be important for CEs to consider the commentary in determining how they can and must provide access to PHI.

[15] 86 Fed. Reg. at 6457

[16] 86 Fed. Reg. at 6533 (amendments to 45 C.F.R. § 164.501)

summary. Under the proposed changes, if a covered health care provider offers to transmit such a summary, the provider must inform the individual that she retains the right to access a copy of the PHI – unless the provider is offering the summary because it is denying a request for a copy the PHI (in which case it would be required to follow the denial of access requirements).

- Implementation Steps: This change likely will require revisions to access and ROI policies. A CE will also want to train ROI personnel on this new notice requirement.

- ***No Charge for Access*** – Change to 45 C.F.R. § 164.524(c). CEs would be required to provide access free of charge when an individual (i) inspects PHI in person (*e.g.*, recording/copying using the individual's own device), or (ii) uses an internet-based method such as a personal health app.[17]

    - Implementation Steps: This change will likely require revisions to access and ROI policies, the individual access provision in the NPP, and any documents that address fees for records. A CE will also want to train ROI personnel and point of care staff on what types of access must be provided for free.

- ***Required Revisions to NPP*** – Change to 45 C.F.R. § 164.520. The proposed changes would require several revisions to the NPP, including revisions to the introductory statement and the right of access provision. Providers will also need to include a statement that patients have the right to discuss the notice with a designated contact person, and to provide such person's email address (in addition to a telephone number).

    - Implementation Steps: This change will require revisions to the NPP and appropriate distribution of the revised NPP. It will also require revisions to the NPP policy if the policy addresses content of the NPP.

The Ugly: Substantial Increase in Regulatory Burden

In our view, three of the proposed changes would place undue burden on CEs, and one change likely would create additional risk and liability:

- ***Requirement to Transmit Access Requests to Other Providers*** – Addition of 45 C.F.R. § 164.524(d). The proposed rule would create a new obligation on CEs to submit an individual's access request to a covered health care provider. Under the proposed changes, upon the written or oral direction of a current or prospective patient of a covered health care provider or a current member (or dependent) of a health plan, a CE (a "Requester-Recipient") would be required to submit an individual's request for an electronic copy of PHI in an EHR to a covered health care provider ("Discloser") within

[17] For other types of access, CEs would be limited in the amount they can charge to a "reasonable, cost-based fee." There are host of complicated rules around what constitutes a "reasonable cost-based fee," and the proposed changes add more restrictions. We do not address the "reasonable, cost-based fee" provisions in this alert.

15 calendar days. Extensions would not be permitted.

The Discloser would then be required to respond to such a request in accordance with the right of access provisions. (See discussion above on reduced time to respond to access requests.) This change seems unnecessary (and overly burdensome on CEs) given other proposed changes to the right of access. If a patient's ability to request and obtain access is expanded, and CEs are required to respond to those requests in a shorter period of time, it seems unnecessary to require CEs to make those requests on behalf of the individuals, particularly upon an oral request made at any time.[18]

- Implementation Steps: This change likely will require development of a new policy that requires the CE to send access requests to other providers and plans within 15 days upon request, and revisions to a covered provider's access and ROI policies on responding to an access request transmitted by another CE. A CE will also need to train point of care staff on the new requirement and the process for documenting (if oral) and responding to these requests.

- ***Fee Schedule*** – Addition of 45 C.F.R. § 164.525. Under the proposed changes, if a CE imposes fees for access to PHI and for disclosures with an individual's valid authorization, the CE would be required to: (i) post a fee schedule[19] on its website (if applicable); (ii) provide a fee schedule to an individual at point of service upon request; and (iii) provide, upon request, an individualized estimate of approximate fees that may be imposed for any type of request covered by the fee schedule. A CE would also be required to provide, upon request, an itemized list of the specific charges for labor, supplies, and postage (if applicable), that constitute the total fee charged for any type of request covered by the fee schedule.

  With respect to fee schedule availability at the point of service, the expectation would be that a covered health care provider would make the fee schedule available upon request, in paper or electronic form, at the point of care or at an office that is responsible for releasing medical records, as well as orally (*e.g.*, over the phone), as applicable.

  - Implementation Steps: This change will require the development of a fee schedule and revisions to any policies that address charging and responding to questions or requests about fees. If fees are handled by an outside vendor, this change will require a discussion with the vendor and possibly revisions to the service contract to cover these requirements. If fees are handled internally, a CE will need to train ROI personnel and point of care staff on the fee schedule and individualized estimate requirements. Either way, this change likely will

[18] 86 Fed. Reg. at 6537 (amendments to 45 C.F.R. § 164.524)

[19] The fee schedule would be required to specify (i) all types of "free of charge" access; (ii) standard fees for copies of PHI (a) provided to individuals pursuant to an access request, with respect to all readily producible electronic and non-electronic forms and formats; (b) in an EHR and directed to third parties designated by the individual, with respect to any available electronic forms and formats; and (c) sent to third parties pursuant to a valid authorization, with respect to any available forms and formats. 86 Fed. Reg. at 6538 (amendments to 45 C.F.R. § 164.525)

create a significant amount of work and/or increased cost for CEs.

- ***Patient Notes, Videos and Photographs*** – Change to 45 C.F.R. § 164.524(a). In addition to the general right to inspect and make a copy of PHI, the proposed changes would give individuals the right to take notes, videos and photographs of, and to use other personal resources to capture, PHI in a designated record set (DRS), subject to a few limitations. For instance, the proposed rule change expressly provides that: "A [CE] is not required to allow an individual to connect a personal device to the [CE's] information system and may impose requirements to ensure that an individual records only [PHI] to which the individual has a right of access."[20]

  OCR requests comments on whether individuals recording their own PHI through video, still camera photos, or audio recordings would be inconsistent with federal and state recording laws or IP rights protection – as well as possible unintended consequences of the proposed expansion of right to inspect PHI. We believe it will be difficult for workforce members to manage and control individuals using cameras and other recording devices in day-to-day operations. This likely will result in impermissible disclosures of PHI, which will add extra burden (and potential exposure) on CEs.

  - Implementation Steps: This change will require revisions to access and ROI policies – as well as development of policies or protocols around when/how to allow individuals to take photographs and videos and how to minimize security and disclosure risks. A CE will also need to train point of care staff on these requirements.

[20] 86 Fed. Reg. at 6535 (amendments to 45 C.F.R. § 164.524)