February 12, 2019

Roger Severino, Director
U.S. Department of Health and Human Services
Office for Civil Rights
Attn: RFI, RIN 0945-AA00
Hubert H. Humphrey Building
Room 509F
200 Independence Avenue, SW
Washington, DC 20201

Submitted via https://www.regulations.gov

**Re: RIN 0945-AA00 Request for Information on Modifying HIPAA Rules to Improve Coordinated Care**

Dear Director Severino,

Consumer Reports[1] submits this response to the Request for Information (RFI)[2] issued by the Office for Civil Rights (OCR) Request for Information on Modifying HIPAA Rules to Improve Coordinated Care. Our organization has a rich history of advocacy for affordable, high quality healthcare and coverage and also a deep commitment in protecting the privacy of all consumers. Thank you for the opportunity to provide information at this early stage in policy development.

Consumers have a vested interest in the success of efforts to improve value-based care and care coordination as well as ensuring that the time-honored bonds of trust that come with private interactions between patients and their providers are upheld as sacrosanct. Both are achievable – privacy must not be compromised to achieve the goal of value-based care and improved care coordination. For that reason, Consumer Reports urges caution in proposing to modify HIPAA privacy and security rules. We also encourage the OCR to pursue changes that would improve patients' access to their own medical information as well as easing the flow of information, which in some cases could be improved without changing the rules as they exist today.

Our responses to the questions, which are answered selectively in numerical order, reflect four major themes:

---

[1] Consumer Reports is an independent, nonprofit membership organization that works side by side with consumers to create a fairer, safer, and healthier world. For 80 years, CR has provided evidence-based product testing and ratings, rigorous research, hard-hitting investigative journalism, public education, and steadfast policy action on behalf of consumers' interests. Unconstrained by advertising or other commercial influences, CR has exposed landmark public health and safety issues and strives to be a catalyst for pro-consumer changes in the marketplace. From championing responsible auto safety standards, to winning food and water protections, to enhancing healthcare quality, to fighting back against predatory lenders in the financial markets, Consumer Reports has always been on the front lines, raising the voices of consumers.

[2] The Federal Register notice appeared on December 14, 2018, 83 Federal Register 64302, https://www.federalregister.gov/documents/2018/12/14/2018-27162/request-forinformation-on-modifying-hipaa-rules-to-improve-coordinated-care.

I. Patients must be in control of how and when information is shared about them.

II. Privacy policies must be meaningful for patients.

III. Patients must have timely access to their own medical information.

IV. Significant caution should be exercised in describing patient privacy as a "burden."

Overall, Consumer Reports strongly encourages OCR to promote policies that reflect patient's needs and priorities while maintaining strong privacy and confidentiality protections.

## I. Patients must be in control of how and when information is shared

Consumer Reports supports the goal of improving care coordination and care management. However, it greatly concerns us that the role of capable patient's in core coordination is dwarfed by the emphasis on caregivers – providers, family, and social services – throughout the RFI.

Healthcare providers, family, and caregivers play an important role in the care continuum. But, the emphasis on providers and caregivers, and the de-emphasis of patients themselves, is borne of an outdated model of healthcare. Instead, the OCR should recognize patients as the keystone of their healthcare. In this paradigm, it is clear that patients must have access to their medical information and the right to decide what information is shared and when.

To be sure, there are cases where patients are unable to exercise their autonomy.[3] Those cases should be the rare exception. Only then should individual autonomy give way to the judgment of others.

## II. Privacy policies must be meaningful for patients

Privacy policies play an important role for all consumers, but the current system of notice for patients is far from ideal. In trying to facilitate as much transparency as possible, privacy policies fail to provide the notice intended. Instead, Consumer Reports recommends a bifurcated notice system, where information is publicly available and tailored for the place and time that it is consumed.

Patients must continue to receive information about their providers' privacy practices as well as relevant laws and regulations. However, the current system of signing notices and waivers is not one in which patients are truly aware of their providers' privacy policies and of their rights as patients. We recommend that the OCR evaluate how consumers receive information best, their ability to read and digest privacy policies at the moment they are delivered at the point of care, and whether there is opportunity to improve the timing, methods, and format in which information is delivered to patients. This evaluation must be done transparently and in partnership with a representative assortment of patients and patient advocacy groups.

Apart from the notice provided to patients, healthcare providers must continue to provide more detailed information about their actual practices within their privacy policies – not so much for patients at the point of care, but for regulators and patient advocates. As such, privacy policies would function more like financial filings, which are important accountability documents, and which are not necessarily read by ordinary investors, but which are processed by intermediaries

[3] For example, in the experience detailed in this article: Jeneen Interlandi, *When My Crazy Father Actually Lost His Mind*, New York Times Magazine (June 22, 2012).

to convey meaningful information in the marketplace. Of course, because some patients may want a comprehensive understanding of their providers' practices, if the privacy notice is bifurcated as suggested here, the comprehensive version of that privacy notice must always be easily available to patients.

## III. Patients must have timely access to their own medical information

There are many reasons why patients would need or want access to their medical records, such as getting a second opinion, when changing doctors, and simply to check accuracy. In most cases, HIPAA affords patients the right to access their medical information within thirty days of a request. That may not be soon enough. Thirty days may have been reasonable when patient medical records were stored in hard copy. Nowadays, medical records are often digitized making transfer of medical records much more nimble. Patients' ability to access their medical records should advance with record keeping technology.

We urge the OCR to speed the rate at which providers must make medical records available, especially where digital medical information could be shared with the click of a button. Certainly, circumstances between providers will vary as will the ability to transmit medical records. At a minimum, though, patients should be able to get information at the same speed as their providers especially when transmitted in the same format as their providers.

## IV. Significant caution should be exercised in describing patient privacy as a burden

Consumer Reports strongly agrees with the OCR that improved care coordination is a means to improved health outcomes. However, framing current components of HIPAA as a burden and easing patient privacy protections as efficiency is problematic especially when patient preference is underemphasized. We encourage OCR to expand its analysis to consider the burden on patients who continue to experience unnecessary delays in receiving their own medical information[4], or for whom having personal health information shared could have negative repercussions. Further, much of the burden experienced by providers is attributable to proprietary systems limiting the extent to which information can be shared[5] and would be appropriately be addressed elsewhere rather than in the HIPAA privacy and security rules.

There is room for improvement in the quality of data shared and the efficiency with which it is shared. But, pitting providers against patients, and failing to reflect much of the hardship experienced by patients, is a disservice to the consumers served by the healthcare system. We therefore urge the OCR, in future rulemaking, to centralize the interest of patients and to recognize that a certain amount of effort to secure patients' data and to protect their privacy is a necessary component of providing healthcare services.

Finally, but not of least importance, any evaluation of the workload associated with HIPAA adherence must also distinguish between *actual* versus *perceived* barriers to information sharing. We believe that some of the burden perceived by providers is actually caused by

[4] According to the Office of the National Coordinator for Health Information Technology, 37% of individuals experienced one or more gaps in health information among their providers or between themselves and their providers when seeking care for a medical problem. V. Patel, W. Barker & E. Siminerio, Individuals' Access and Use of their Online Medical Record Nationwide. ONC Data Brief no. 20 (Sept. 2014).

[5] According to a recent report, 63 percent of hospital leaders surveyed said that their hospital is unable to send patient information because the other provider either doesn't have an EHR or lacks the ability to receive the information, and 57 percent reported challenges exchanging data across different vendor platforms. Modern Healthcare, *Data Points: Data exchange still a struggle 10 years after HITECH Act*, (Feb. 9, 2019).

covered entities that misunderstand or misinterpret HIPAA.[6] Although both the Privacy Rule[7] and the Security Rule[8] of HIPAA require covered entities, and their business associates, to be trained in the rules, variability in training programs combined with an absence of enforcement by OCR of training requirements has contributed to a decline in properly educated covered entities and business associates.[9] We expect care coordination between providers and with caregivers and support services could be improved, and the perceived burden of HIPAA adherence reduced, simply by understanding the law as it currently exists.

## V. Answers to questions asked in numerical order

**Question 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?**

Under HIPAA, providers currently have thirty days to provide PHI when request for an individual but in some states, the time frame is shorter.[10] Thirty days may have been reasonable when medical information was stored in hard copy. But, it is not always fast enough for patients' needs. Delays in receiving information could be life or death for patients who are waiting on needed information to determine eligibility for a treatment trial, avoiding adverse reaction in medicine, or seeking a second opinion for their healthcare.

Nowadays, medical records are often digitized making transfer of medical records much more nimble. Patients' ability to access their medical records should advance with record keeping technology. Certainly, circumstances will vary between providers as will the ability to transmit medical records. But, access should be provided as quickly as possible. The existence of shorter time frames for providing medical information in some states illustrates that a quicker turnaround is possible. At a minimum, patients should be able to get information at the same speed as their providers especially when transmitted in the same format as received by their providers.

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

Yes, covered entities should 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 current standard of thirty days to produce medical information may have been reasonable when medical information was stored in hard copy. But, more modern digital

[6] Paula Span, *HIPAA's Use as a Code of Silence Often Misinterprets the Law*, The New York Times (July 17, 2015).
[7] 45 CFR §164.530(b)(1).
[8] 45 CFR §164.308(a)(5).
[9] Julie L. Agris and John M. Spandorfer, *HIPAA Compliance Training: A Perfect Storm for Professionalism Education? Journal of Law*, Medicine & Ethics 44 (2016) 652-656.
[10] California, Colorado, Hawaii, Louisiana, Tennessee, Texas, Virginia, and Washington each have laws requiring record requires be fulfilled within a shorter period of time than the HIPAA standard.

medical records make transfer of medical records much more nimble. Patients' ability to access their medical records should advance with record keeping technology and access should be provided as quickly as possible. At a minimum, patients should be able to get information at the same speed as their providers especially when transmitted in the same format as their providers. And, medical information that is already in digital form, than can be transmitted to the patient in digital form, should be available sooner than thirty days.

Delays in receiving information could be life or death for patients who are waiting on needed information to determine eligibility for a treatment trial, avoiding adverse reaction in medicine, or seeking a second opinion for their healthcare. When information, such as digital medical records, can be transmitted more quickly than in the past, that is what should be done.

**Question 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.**

We caution the OCR to evaluate whether responses to this question are rooted in fact or perception, and to balance the burden on providers of a shortened time frame against the burden to patients of not having timely access to medical information. We also recommend comparison of the effort required to accelerate response to patient medical information requests versus the timeline of providing the same records to providers. Especially when it comes to digital medical records, it is difficult at best to see how accelerating the pace at which medical records must be made available to patients would incur unreasonably significant effort or cost. Finally, we caution the OCR to be wary of commenters who use the concept of burden as an excuse to continue the harmful practice of information blocking.

**Question 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?**

Ease of flow of information between healthcare providers is certainly an important piece of care coordination. The fact is that covered entities are already allowed, but not required, to share information for treatment purposes *without first obtaining* an individual's authorization[11] (with an exception for psychotherapy notes[12]). "Treatment" is broadly defined and already includes care coordination and care management, the focal points of this RFI.[13]

Although in most circumstances PHI can be disclosed when requested by another entity for treatment purposes, there is no deadline or requirement to disclose records. As a result, in some cases, patient records are not transferred in a timely fashion, to the detriment of coordinated care and case management.

There are many reasons why health information does not flow the way it should. For example: incorrect interpretation of the law, inefficient provider workflow, and intentional information blocking. Getting over these barriers is important in improving the care patients receive.

[11] 45 CFR 164.506(c)(2).
[12] 45 CFR 164.508(2).
[13] Health and Human Services Office for Civil Rights fact sheet, *Permitted Uses and Disclosures: Exchange for Treatment*, (January 2016).

However, we strongly disagree with creating a blanket rule that would require covered entities to disclose PHI on the basis of any request from another covered entity. Such a rule could be harmful for patients, for example by leading to disputed medical information about a patient being shared with other providers without patients being aware, or by a patient being discriminated against by healthcare providers who learn that the patient is being treated elsewhere for a stigmatized condition.

Finally, requiring sharing of PHI would threaten patient autonomy. Patients want control over their own healthcare, whether that means partnering with their providers to choose the care that is right for themselves or delegating their healthcare decisions to providers they trust. Ultimately, patients who are capable of making their own decisions should have the final say in who has access to their medical records.

Our comments to this question, of course, are not intended to support deliberate attempts by information creators or information gatherers to hoard medical information in a practice known as data blocking or information blocking. We support efforts of the OCR to address this troubling practice in the healthcare sector and believe there is a way to break information blocking practices while upholding patients' rights to choose where and when their information is shared.

**Question 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?**

If OCR creates a requirement for covered entities to disclose PHI to other healthcare providers or other covered entities, there must be exceptions and/or limitations that would allow for patients to specify PHI that may not be shared or to limit sharing of PHI to certain providers or to specific circumstances. Simply put: the priority must be in keeping patients as the final arbiter of when this sensitive information is shared and with whom.

**Question 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?**

We strongly disagree with the premise that covered entities should always be required to disclose PHI on the basis of a request from another covered entity. Although there may be limited exceptions, such a blanket rule requiring disclosure could be dangerous for patients. For example, in cases of intimate partner violence, elder abuse, and substance abuse treatment.

Ultimately, patients who are capable of making their own decisions should have the final say in who has access to their medical records. Patients want control over their own healthcare, whether that means partnering with their providers to choose the care that is right for themselves or delegating their healthcare decisions to caregivers or providers they trust.

There will be times when a provider may disagree with a patient regarding when, what, and with whom disclosure is necessary. That should be an opportunity for a dialogue between the patient and the provider, not a junction when the providers' opinion surpasses that of the patient. In some cases, the provider may prevail upon the patient; at other times, the provider will learn from the patient why he or she does not want the information to go somewhere else. Ultimately, patients that are capable of making their own decisions should have the final say.

**Question 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?**

Ultimately, a patient who is capable of making their own decisions should have the final say in who has access to their medical records. We encourage the OCR to carve out limited circumstances where authorization is not feasible – such as where a patient is incapacitated or when time is of the essence – and to otherwise require affirmative consent. Only in those cases should individual autonomy give way to the judgment of others such as providers and caregivers.

**Question 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?**

Without clear evidence that the minimum necessary rule is constraining providers from coordinating care, we see no reason to expand the exceptions to the Privacy Rule minimum necessary standard. The minimum necessary rule is interpreted broadly and it is likely that some barriers to case management and care coordination result from misunderstandings or misinterpretation of the current law, not the actual law itself. The solution to that problem may instead be changes to training requirements to specify curriculum and frequency requirements paired with more frequent and rigorous enforcement actions.

**Question 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 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?**

Consumer Reports has long supported care coordination as an avenue for improved health outcomes. However, we question how broad an exception like this could be before privacy protections dissolve altogether or create an imbalance of rights to privacy based on qualifying for health or social services. Providing whole-person care cannot come at the expense of patient privacy. Instead, all individuals should retain control over their PHI whether they need health or social services or not. Furthermore, given that patient consent is all that is needed for release of information to multidisciplinary/multi-agency teams, we believe the goal of this question could also be achieved by engaging the patients themselves in consenting to release their information, and in better educating and training professionals in how information can already be shared within the current framework of HIPAA.

**Question 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

Family and friends can serve an important role in patients' healthcare. When patients elect to have their PHI shared with a caregiver or loved one, covered entities should certainly do so as quickly as possible. However, there are reasons why patient do not want their PHI shared with family or friends.

The HIPAA privacy and security rules are necessary and core to protecting patient privacy and confidentiality. These rules balance keeping health information private while allowing for information to be appropriately and securely shared for patient care. The fact is that there is already leniency for sharing the PHI of an individual that is incapacitated or experiencing an emergency.[14] Indeed, the OCR itself has explained "HIPAA helps you stay connected with your loved one by permitting health professionals to contact you with information related to your family member, friend, or the person you are caring for, that is necessary and relevant to your involvement with the patient's health care or payment for care."[15] Given that there is already leniency to do the things suggested in this question, we discourage the OCR from going further and risking creating an imbalance of rights to privacy based on substance use disorder.

Instead, the OCR should make efforts to correct HIPAA misconceptions and misinterpretations by disseminating more information on when and what information can be shared and by providing clarifying guidance and FAQs more broadly. The OCR should also consider modifying the Privacy Rule and Security Rule training requirements to specify curriculum and frequency requirements for covered entities and business associates, paired with more frequent and

[14] 45 CFR 165.510(b)(3).
[15] U.S. Department of Health and Human Services Office for Civil Rights, *HIPAA Helps Caregiving Connections*, available at https://www.hhs.gov/sites/default/files/hipaa-helps-prevent-harm.pdf.

rigorous enforcement actions. This should include training on federal and state confidentiality laws that would apply to the person's particular condition and the type of care being received.

**Question 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?**

HIPAA is necessary and core to protecting patient privacy and confidentiality. The privacy and security rules balance keeping health information private while allowing for information to be appropriately and securely shared for patient care. While the impact of opioid abuse has been felt in communities across the country and demands a well-informed and coordinated response, the Privacy Rule is not the correct venue to address the opioid epidemic.

There is already leniency for sharing the PHI of an individual that is incapacitated or experiencing an emergency.[16] When a patient is capable of making decisions for themselves, they must be granted the autonomy to do so. An opioid addiction, as with any other healthcare condition, should not by default lower a person's rights to privacy. Otherwise, patients in their moment of need could have their healthcare impacted or suffer from discrimination. Indeed, there can be legal ramifications associated with disclosure of substance use disorders, such as loss of employment, loss of housing, loss of child custody, and even discrimination by medical professionals.[17] Also troubling, patients may forego substance abuse treatment altogether, putting them at greater risk, if they realize that privacy protections have been lowered.

Instead, the OCR should make efforts to correct HIPAA misconceptions and misinterpretations by disseminating more information on when and what information can be shared and by providing clarifying guidance and FAQs more broadly. The OCR should also consider modifying the Privacy Rule and Security Rule training requirements to specify curriculum and frequency requirements for covered entities and business associates, paired with more frequent and rigorous enforcement actions. This should include training on federal and state confidentiality laws that would apply to the person's particular condition and the type of care being received. There should also be more education for social service providers, who may not be covered entities or business associates, and for patients and caregivers themselves.

**Question 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?**

[16] 45 CFR 165.510(b)(3).
[17] Karla Lopez and Deborah Reid, *Discrimination Against Patients with Substance Use Disorders Remains Prevalent and Harmful: The Case for 42 CFR Part* 2, (April 13, 2017).

In most cases, parents already have access to the medical information about their child, as the child's personal representative, when such access is consistent with State or other law.[18] There are only a few discrete circumstances where parents do not by default have a right to their minor child's medical information. Given the breadth at which parents already have access to their minor child's medical information, we question whether broadening access is necessary or appropriate.

Parental access to their minor children's medical information should be limited where the information could cause harm to the minor child or could discourage the minor child from accessing care. When it comes to reproductive healthcare, for example, the CDC found that young women aged 15-17 were 34% less likely to receive sexual or reproductive health services in the past year if they had concerns about their parents finding out.[19] Patients, including minors such as teenagers need to feel safe and secure when seeking care. Changes to the Privacy Rule that could expose minors' sensitive health information to their parents against their wishes could unintentionally impact the extent which minors access sensitive healthcare altogether.

Without compelling reasons to lower a privacy standard that is already rather lenient, the OCR should refrain from modifying the Privacy Rule to allow parents greater access to their children's medical information. Rather, the OCR should continue its current deference to other federal and state laws, as well as provider discretion, for safeguarding minors' privacy and confidentiality.

**Question 25(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?**

Adult children can serve an important role as caregivers for patients. When patients elect to have their PHI shared with an adult child, covered entities should certainly do so as quickly as possible. However, there are a number of reasons why a parent would not want PHI shared with their adult child. For example, in the case of elder abuse.

There is already leniency for sharing the PHI of an individual that is incapacitated or experiencing an emergency.[20] Rather than altering the right to privacy for older adults who happen to have adult children, providers should be informed of where they already have the right to share PHI, and should also be encouraged to work with patients to identify caregivers or loved ones who should have access to PHI.

**Question 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/guidancemodel-notices-privacy-practices/index.html, that clearly identify, in a**

[18] Office for Civil Rights (OCR), *Does the HIPAA Privacy Rule Allow Parents the Right to See Their Children's Medical Records?* (created 12/19/2002, last reviewed on July 26, 2013). Available at https://www.hhs.gov/hipaa/for-professionals/faq/227/can-i-access-medical-record-if-i-have-power-of-attorney/index.html

[19] Casey E. Copen, MPH et. al., *Confidentiality Concerns and Sexual and Reproductive Health Care Among Adolescents and Young Adults 15-25*, NCHS Data Brief (No. 266) December 2016.

[20] 45 CFR 165.510(b)(3).

**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?**

Privacy policies play an important role for all consumers, not the least of which are patients. But privacy policy practices are currently imperfect. Creating a safe harbor for covered entities that use the model NPPs will not necessarily solve the problem. Indeed, in trying to facilitate as much transparency as possible, privacy policies fail to provide the notice intended. Instead, Consumer Reports recommends a bifurcated notice system, where information is publicly available and tailored for the place and time that it is consumed.

Patients must continue to receive information about their providers' privacy practices as well as relevant laws and regulations. However, the current system of signing notices and waivers is a not system in which patients are truly aware of their providers' privacy policies and of their rights as patients. We recommend that the OCR evaluate how consumers receive information best, their ability to read and digest privacy policies at the moment they are delivered at the point of care, and whether there is opportunity to improve the methods and format in which information is delivered to patients. This evaluation must be done transparently and in partnership with a representative assortment of patients and patient advocacy groups.

Individuals are not the only ones who are not fully aware of their rights under HIPAA. Although both the Privacy Rule[21] and the Security Rule[22] of HIPAA require covered entities, and their business associates, to be trained in the rules, the variability in training programs combined with an absence of enforcement by OCR of training requirements has led to a decline in properly educated covered entities and business associates.[23] We believe that care coordination could be improved, and the burden felt by providers reduced, simply by understanding the law as it currently exists. This could be addressed by amending the training requirements to specify curriculum and frequency requirements paired with more frequent and rigorous enforcement actions.

**Question 53(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?**

Privacy policies play an important role for all consumers, not the least of which are patients. But privacy policy practices are currently imperfect. In trying to facilitate as much transparency as possible, privacy policies fail to provide the notice intended. Rather than tinkering with current

[21] 45 CFR §164.530(b)(1).
[22] 45 CFR §164.308(a)(5).
[23] Julie L. Agris and John M. Spandorfer, *HIPAA Compliance Training: A Perfect Storm for Professionalism Education?*, Journal of Law, Medicine & Ethics 44 (2016) 652-656.

NPPs, Consumer Reports suggests that OCR consider requiring a bifurcated notice system, where information is publicly available and tailored for the place and time that it is consumed.

Patients must continue to receive information about their providers' privacy practices as well as relevant laws and regulations. However, the current system of signing notices and waivers is not a system in which patients are truly aware of their providers' privacy policies and of their rights as patients. We recommend that the OCR evaluate how consumers receive information best, their ability to read and digest privacy policies at the moment they are delivered at the point of care, and whether there is opportunity to improve the methods and format in which information is delivered to patients. This evaluation must be done transparently and in partnership with a representative assortment of patients and patient advocacy groups.

Apart from the notice provided to patients, healthcare providers must continue to provide more detailed information about their actual practices within their privacy policies – not so much for patients at the point of care, but for regulators and patient advocates. As such, privacy policies would function more like financial filings, which are important accountability documents, and which are not necessarily read by ordinary investors, but which are processed by intermediaries to convey meaningful information in the marketplace. Of course, because some patients may want a comprehensive understanding of their providers' practices, if the privacy notice is bifurcated as suggested here, the comprehensive version of that privacy notice must always be available to patients.

In addition to receiving more streamlined information about their rights as patients, patients would also benefit from improved provider/staff training about HIPAA and patients' rights, and receiving the privacy notice in the language that the patient speaks.

**Question 53(d): Please identify other specific recommendations for improving the NPP text or dissemination requirements to ensure individuals are informed of their HIPAA rights.**

Patients may get more out of receiving a streamlined privacy statement than the current NPP text they are presented at their doctors' offices. It is clear that the current system of signing notices and waivers is not a system in which patients are truly aware of their providers' privacy policies and of their rights as patients. We recommend that the OCR evaluate how consumers receive information best, their ability to read and digest privacy policies at the moment they are delivered at the point of care, and whether there is opportunity to improve the methods and format in which information is delivered to patients. This evaluation must be done transparently and in partnership with a representative assortment of patients and patient advocacy groups.

Some options the OCR should consider when improving the NPP text or dissemination:

- Having the patient receive the signature page separately from the NPP itself, so the patient can leave the signed page with their provider and take the NPP home to record or review later.
- Have the NPP accessible from the patient portal.
- Accept electronic signature for the NPP.

In addition to the suggestions, above, for improving the NPP text and dissemination requirements, we also recommend that:

- Providers be required to provide cost estimates if patients will be required to pay for their medical information (within the amount permitted by HIPAA).
- Providers be prohibited from charging for access to digital records for which transferring information to the patient does not incur an expense for the provider.
- OCR develop new approaches to making its vast resources[24] on HIPAA privacy and security rules educational material more widely known and used.

## VI. Conclusion

Consumer Reports thanks the ONC for the opportunity to submit these comments. We look forward to meaningful conversation and collaboration around improving value-based care and care coordination while upholding the private confidence between patients and providers. The twin goals of improved health outcomes and cost containment are noble but it is critically important that in the effort to achieve these new heights, patient rights do not fall. Please reach out to us for additional comments or questions.

Respectfully submitted,

Dena B. Mendelsohn
Senior Policy Counsel
Consumer Reports

[24] For example, the Office's FAQs, fact sheets, and educational videos.