ciitizen

February 11, 2019

Roger Severino, Director
Office for Civil Rights (OCR)
U.S. Department of Health and Human Services
Re: RIN 0945-AA00 ("Request for Information on Modifying HIPAA Rules to Improve Coordinated Care")

Dear Director Severino:

On behalf of Ciitizen, I appreciate the opportunity to provide public comments on the "Request for Information on Modifying HIPAA Rules to Improve Coordinated Care." As your former Deputy Director for Health Information Privacy, I am not far removed from the challenges of how to keep the privacy, security, and breach notification regulations of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") relevant in a rapidly changing health care ecosystem, and I congratulate you and your staff on the publication of this RFI.

Ciitizen's mission is to empower the world's 7 billion citizens to have complete control of their health data: to share it with whomever, whenever, and wherever they want. With a focus on empowering sick patients, beginning with cancer, the Ciitizen online platform democratizes health care by putting data ownership and control back in the hands of patients – the stakeholders most highly motivated to collect it, use it, and share it liberally to save their own lives and the lives of others just like them.

Ciitizen leverages the HIPAA Privacy Rule's individual right of access in order to populate a user's Ciitizen profile. Our cancer patient users, with their complete, relevant health histories in hand, are empowered to seek treatment options, help their providers better coordinate their care, and contribute their data to research and other population health initiatives, such as value-based care programs.

In summary, our comments (which respond to most, but not all, questions) urge OCR to take the following actions:

- Change the Privacy Rule to require covered entities (and business associates operating on their behalf) to respond to an individual right of access request in a shorter time frame.
- Issue regulations and/or guidance to enable Business Associates (BAs) to directly respond to individual access requests and holding business associates fully accountable for complying with the requirements of 45 CFR 164.524 when they do so.
- Refrain from turning the treatment, payment, and/or operations provisions of the Privacy Rule into mandatory disclosures due to the potential privacy harms that could result.
- Collaborate with ONC and CMS on initiatives to require or incentivize sharing among providers and payers, and issue guidance making clear to providers that disclosures that are directed by the individual are required under the Rule.
- Improve the individual right of access through more robust, publicly-visible enforcement efforts, as well as by modifying the Privacy Rule (and/or issuing subregulatory guidance) to:
    - Require entities to implement protected health information (PHI) request submission processes that do not impose undue burdens on individuals (for example, by requiring entities to accept e-mail requests from individuals).

- Require entities to accept any written or digital individual access request form that complies with HITECH requirements.
- Assure that individuals can request that PHI be sent to a third party designee pursuant to the Privacy Rule access right, even if an app or service is assisting the individual in making those requests.
- Require entity acceptance of individual identity credentials meeting National Institute of Standards (NIST) Level of Assurance 2.
- Require entity acceptance of electronic signatures on individual requests.
- Further clarify fee limitations.
- Require entities to accept continuous (persistent) requests from individuals.
- Clarify that the individual's app or personal health record service or platform vendor is responsible for the PHI once it is conveyed.
- Clarify the scope of the designated record set, such as by expressly including information collected from individual (patient) devices and information generated in caring for an individual through that individual's death.
- Reconfirm the right of the individual, or the individual's designee, to access PHI by unsecure e-mail or document upload.
- Increase publicly visible enforcement efforts with respect to the right of access.

Section a. Promoting information sharing for treatment and care coordination

1) How long does it take covered entities to provide an individual with a copy of their protected health information (PHI) when requested pursuant to the individual's right of access? Does the length of time vary depending on whether records are maintained electronically or on paper? Does the length of time vary based on the type of covered entity?

Ciitizen Response: Today individuals have two main pathways for obtaining copies of PHI:

- By accessing it through a provider's certified electronic health record (EHR) technology (such as by downloading it from a portal or accessing it via a consumer app through an open application programming interface (API)) and
- By contacting the provider's medical records department or, in the case of small providers, the staff member responsible for responding to HIPAA-related inquiries.

Regarding the first pathway, a number of consumer-facing apps and services are enabling individuals to access their health information via portals in EHRs or open APIs. However, Centers for Medicare and Medicaid Services' (CMS) incentives for professionals and hospitals to make information available to an individual's chosen application or app do not require this capability be available for all of a provider's patients. In addition, the information that is available through a portal or an open API – the "common clinical dataset" – does not include the entire designated record set. For example, this information often does not include images (e.g., x-rays that show size and location of cancer tumors); pathology reports; genomic test reports (necessary to enable individuals to explore potential precision medicine cancer therapies); and physician or other clinician notes, which often contain the details of an individual's treatment regimens (such as chemotherapy and immunotherapy), except in cases where the providers (and their vendors) have cooperated to voluntarily make this available to individuals, such as through the Open Notes[1] project. The information that a cancer patient needs to seek treatment options, coordinate care, and potentially contribute data to value-based care initiatives is part of the

[1] https://www.opennotes.org/.

designated record set but is NOT part of the common clinical dataset. The HHS Office of the National Coordinator (ONC) has proposed over time to increase the types of data required to be made available through certified EHR technology, but this effort could take many years. **Individuals with serious illness and their families need this information today**.

Because this information is not part of the common clinical dataset, Ciitizen acquires designated record set information on behalf of users of the Ciitizen platform primarily through the second pathway: via the medical records (or health information management or HIM) departments of hospitals and larger physician practices and directly from the staff of smaller physician practices. **From our experience, nearly all of the providers to whom we have sent records requests are out of compliance with at least one – and most often more – of the requirements of 45 CFR 164.524**.

The next several RFI questions focus on the length of time it takes for a covered entity to release information pursuant to a right of access request, and our response addresses that issue. In our response to question 54 we provide information on some of the other ways covered entities (or business associates operating on their behalf) fail to comply with the right of access, frustrating (and in some cases, blocking) the ability of individuals to have the information they need to pursue treatment options, and help coordinate their care and payment for that care. Ciitizen is also hosting a campaign to improve awareness of, and compliance with, the HIPAA Right of Access; see https://blog.ciitizen.com/myhealthmydata. We invite OCR to monitor this campaign, as we will be continuing to post stories on the struggles of individuals to obtain their health information (and our struggles to obtain this information on behalf of patients) well past the RFI deadline.

Ciitizen is not yet open to the public but does submit record requests for beta users of our platform. We send request letters, signed by individuals and accompanied by a copy of the individual's government photo ID, to covered entities requesting that all PHI in the designated record set covering a specified timespan be sent in digital form to Ciitizen, ideally via e-mail or through upload into a secure portal maintained by Ciitizen. Once Ciitizen receives this information, it is populated into the individual's Ciitizen Profile. Ciitizen users can then use and share this information easily, in accordance with *their* preferences.

On average, Ciitizen receives responses from covered entities (or a business associate working on their behalf, such as a Release of Information or ROI vendor) in 28 days. Most often these responses are a digital, pdf version of information from the certified electronic medical record, plus a CD of image files, which strongly suggests that this information could be produced much more quickly if shorter timeframes were mandated. For our users with a more urgent need for this information – for example, those individuals facing a particularly grim diagnosis who need to send information quickly in order to obtain a second opinion on treatment – we have appealed (by phone) to hospital records departments and/or privacy officials and received the requested information within 2-3 days.

In addition, the 28-day average obscures the reality of just how long this process can take, or the effort it takes to obtain the records within the 30 days. We published a blog post (see link – also attached as an appendix to this letter) recently regarding one particular request which dragged on for several months - and ultimately resulted in a response of "no records".

Most of our requests have been to hospitals and are handled either by the hospital's Release of Information (ROI) vendor or its HIM/medical records department. To date, about 70% of our requests have been honored within the 30 day request timeline:

- 15% of our requests were honored in under 10 days of receipt of the request;
- 12% of our requests were honored between 10-19 days of receipt of the request;
- 27% of our requests were honored between 20-29 days of receipt of the request; and
- 15% of our requests were honored by the 30th day.

Of the 30% that were received beyond 30 days, half of those took over 40 days (and in no case did we receive notification within the 30 day deadline of the reason for the delay, or an approximate time when the records would be received). We learned early on that following up by phone regarding our requests to make sure they were received was essential to assuring that the requests would be timely processed. Often these phone calls required an appeal to the institution's privacy official, as the staff in the HIM or medical records departments frequently seemed misinformed on the elements of the HIPAA right of access.[2] In general, particularly when we have followed up these requests with a phone call to make sure the request had been received, we obtain the information from these entities within or close to the 30 day deadline. On occasion, when we directly appeal to a privacy official when one of our users has a more urgent need for their PHI (such as to get information to an oncologist for a second opinion prior to the date of the appointment), we get the information within a week. However, one particular ROI vendor has consistently not produced records within the 30 day deadline.

Based on anecdotal reports we have heard, PHI is produced by HIM departments and office staff much more quickly to respond to health care provider requests. For example, HIM departments have told us we can expect records within two-to-three days, until we clarify that we are requesting on behalf of a patient; for patients the timeline defaults to 30 days. We believe the 30 day timeframe creates disincentives to: prioritize requests from individuals; provide sufficient staffing, training and resources to medical records/HIM departments; or to adopt more efficient technological solutions to enable more consistent, rapid responses. If a response is not due any sooner than 30 days, there is little incentive to produce it more quickly. Of note: although the Privacy Rule right of individual access does not require individuals to provide the purpose for their request, Ciitizen's request letters all state that we are requesting information on behalf of a cancer patient who is seeking the information for treatment and care continuity. Only when we make a phone call to that department or the covered entity's privacy official are we able to shorten that timeframe. Merely stating in the request that the information is needed for ongoing treatment or care continuity has rarely resulted in information being sent to us more quickly.

There are a number of states that set shorter deadlines for individuals to get their medical records – but we have found that most medical record offices operate under the HIPAA deadline, even in those states where the deadlines are shorter. Thus, it is critical for OCR to set the standard by which individuals can obtain their health information, which will then enable them to share it to meet their needs, including for care coordination and management and to support value-based purchasing initiatives.

Although most of our requests have been submitted to hospitals, we have sent requests to small physician practices and to genetic testing laboratories that are covered by HIPAA. It surprises us how

[2] Please see the following study for the researchers account of receiving different information from HIM or medical records staff in response to calls inquiring about the process for individuals obtaining their records (hereinafter the "Yale Study"). Lye CT, Forman HP, Gao R, et al. Assessment of US Hospital Compliance With Regulations for Patients' Requests for Medical Records. *JAMA Netw Open.* 2018;1(6):e183014. https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2705850

frequently the institutions with greater resources are the most noncompliant with HIPAA.[3] We have sent requests to three HIPAA-covered genetic testing laboratories – for two of these requests, the response took 43 and 44 days; for the third, the information requested was provided within 24 hours.

2) How feasible is it for CEs to provide PHI more rapidly? What is the most appropriate general timeframe for responses? Should any specific purposes or types of access requests be required to have shorter response times?

Ciitizen Response: See response to Question 1 above. Based on our experience, we believe that in most cases, PHI can be produced for individuals on a much quicker timeframe than 30 days. We urge OCR to modify the Privacy Rule to require that PHI be provided to individuals or their designees as promptly as possible,[4] but no later than 10 days from receipt of the request; information maintained digitally should be required to be provided within no more than five (5) days of receipt of the request. Although OCR has historically sought to keep the Privacy Rule medium agnostic, individual's access requests should not be delayed by antiquated timelines that reflect a paper-based world. Mandating shorter timeframes for digital data, particularly when coupled with more robust, publicly visible enforcement, provides incentives to covered entities (and business associates working on their behalf) to deploy technology solutions that automate more of the HIM department functions. OCR also will need to include guidance (or regulatory provisions) that make it a violation of the Rule to provide paper copies of digital information in an effort to circumvent the shorter time requirement. For example, one widely used ROI vendor has consistently provided us with paper copies of digital information in response to our requests for access; each request clearly specified that the designated records set information was to be provided in digital form and sent by e-mail per the Privacy Rule. Each request was also accompanied by an invoice for per-page fees (and, of course, with no estimate of charges provided in advance.)

3) Should CEs be required to provide copies of PHI maintained in electronic form more rapidly than records maintained in other media when responding to an individual's request for access?

Ciitizen Response: See response to Question 2 above.

4) What burdens would a shortened timeframe for responding to access requests place on covered entities.

Ciitizen Response: See responses to Questions 1 and 2 above (particularly with respect to the shorter timeframes offered to providers seeking PHI). The individual right of access is foundational to assuring that comprehensive health information is available for treatment and care coordination/care management activities. No person is more motivated to collect and share their health information than the individual and his/her caregivers, particularly when an individual is sick or has chronic health challenges. As noted below, failure of covered entities to share information with one another, with other health care entities, or with payers for treatment, care coordination, or value-based care purposes is frequently due to business concerns,[5] particularly given HIPAA's broad permissions enabling sharing

[3] See also the Yale Study, supra note 2, where the hospitals surveyed were all from a list of "Best Hospitals."
[4] The HITECH and HIPAA Breach Notification Rules use a similar approach, requiring covered entities to notify impacted individuals (and OCR) without unreasonable delay, but no later than 60 days after the breach.
[5] See, for example, ONC's Report to Congress on Information Blocking, https://www.healthit.gov/sites/default/files/reports/info_blocking_040915.pdf; Mello et al., Legal Barriers to the Growth of Health Information Exchange – Boulders or Pebbles, Milbank Quarterly, v.96 Issue 1 (March 2018),

for these purposes. Consequently, if HHS is focused on assuring data "interoperability" for critical purposes, it should be doubling down on "portability" initiatives that provide individuals with seamless access to all of their health information and allow them to share it in accordance with *their* personal needs and preferences.

The right of access is a required disclosure under the HIPAA Privacy Rule and has been since the inception of the Rule (nearly 20 years). Our experience in getting PHI for our users suggests there is widespread noncompliance with this right (see our responses to question #54 in addition to our responses in questions 1-4 on the timing issues), so it will take resources for covered entities to get into compliance – but OCR should not reward this recalcitrance by easing access requirements or by missing an opportunity to join with other federal (for example, CMS and ONC) initiatives to require sharing of PHI with individuals in a short timeframe that enables that data to be useful for treatment, care coordination, and value-based care initiatives.

We also note that shorter timeframes for digital data could help motivate covered entities to push harder for or at least support technology solutions that better facilitate providing individuals (and their designees) with seamless digital access to their PHI (such as supporting ONC's efforts to more rapidly increase the information required to be made available to individuals via certified EHR technology).

5) Health care clearinghouses.
    a) How typically do business associate agreements (BAAs) prevent clearinghouses from providing PHI directly to individuals?

    Ciitizen Response:
    Ciitizen has had conversations with a number of business associates (BAs) who have expressed interest in directly responding to individuals requesting copies pursuant to the Privacy Rule. We believe BAs, who frequently maintain information on behalf of multiple covered entities, could be enormously helpful in enabling individuals to more quickly obtain a comprehensive record of their health information. This is particularly true of clearinghouses and health information organizations.

    We have tried to help some of those BAs determine whether their BAAs permit them to directly facilitate getting individuals their PHI. In most cases, these BAAs either expressly prohibited the BA from responding directly to any individual requests (such requests, if made to the BA, were required to be routed to the covered entity for response) or contained only language obligating the BA to provide data to the covered entity to enable the covered entity to respond to an individual access request, leaving the BA with uncertainty regarding whether it could be potentially subject to a penalty from regulators (or a breach of contract action) for responding directly to an individual access request. Consequently, BAs who are interested in facilitating this right face the prospect of renegotiating what could be hundreds of BAAs in order to do so without potentially significant legal risk.

    b) Should clearinghouses be subject to individual access requirements? Should any limitations apply to this requirement? For example, should health care clearinghouses remain bound

---

https://onlinelibrary.wiley.com/doi/abs/10.1111/1468-0009.12313; Savage et al., Digital Health Data and Information Sharing: A New Frontier for Health Care Competition, forthcoming in March: Antitrust Law Journal, Vol. 82, Issue 2 (2019))

by BAAs with covered entities that do not permit disclosures of PHI directly to an individual who is the subject of the PHI?

Ciitizen Response:

As noted above, we believe there is great benefit to BAs like clearinghouses providing access directly to individuals, as it allows individuals to get their PHI across multiple providers and/or payers with a single request. In the long-term, Ciitizen believes this should be a requirement of all business associates, consistent with international privacy laws that increasingly require all holders of personal data to provide the subjects of that data with access and copies upon request (see, for example, the Global Data Protection Regulation). Because clearinghouses meet the definition of a "covered entity" under HIPAA, this is a logical step for OCR to take. (Of note: we are aware of legislation in prior Congresses that would have treated clearinghouses as covered entities but also provided them with additional rights not enjoyed by other covered entities under the Privacy Rule. Because treating clearinghouses as a covered entity would require clearinghouses to comply with the individual rights provisions of the Privacy Rule – including the right to access – there is some benefit to individuals in OCR taking this step. However, clearinghouses should then be treated equivalent to other covered entities under the Privacy Rule, with all of the same rights and obligations with respect to PHI.)

We also note that BAs already have some authority under the 21st Century Cures Act to provide information directly to individuals if they want to, at least with respect to information that comes from an "electronic health record" (which is defined in HITECH broadly and not just limited to certified EHR technology).[6] Section 4006(b) of the 21st Century Cures Act (P.L. 114-255), which amended HITECH, provides as follows:

> if the individual makes a request to a business associate for access to, or a copy of, protected health information about the individual, or if an individual makes a request to a business associate to grant such access to, or transmit such copy directly to, a person or entity designated by the individual, a business associate may provide the individual with such access or copy, which may be in an electronic form, or grant or transmit such access or copy to such person or entity designated by the individual….

However, it is not clear that many BAs (including clearinghouse BAs) have done so given the absence of implementing regulations in the HIPAA Privacy Rule. The Cures statutory provision provides BAs with sufficient legal authority to act, at least with respect to PHI that comes from an "electronic health record" as that term is defined in HITECH – but where the BAA has contrary or less than clear language, BAs will be reluctant to take on potential liability in making information directly available to individuals. We have spoken with a number of BAs (health information exchanges in particular) who are interested in enabling individuals to have direct access to their PHI but are hesitant due to lack of clarity from OCR and/or contrary or unclear provisions in their BAAs

[6] Section 13400(5) of HITECH defines and "electronic medical record" as an "electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff."

OCR should, at a minimum, promptly issue guidance to at least enable BAs who seek to rely on the Cures language in Section 4006(b) to provide individuals directly with access to be able to do so, regardless of existing provisions in the BAA, and provide them (and the covered entities with whom they contract) a generous grace period for revising BAAs to make them consistent with both 21st Century Cures and the decision of the BA to opt into providing individual access. OCR did this with respect to implementation in BAAs of the HITECH changes in the Omnibus regulations.[7] In addition, OCR should use its general statutory authority under HIPAA to modify the Privacy Rule to enable BAs who maintain PHI that is not from a covered entity's "electronic health record" to have the same permission to make PHI directly available to individuals (or their designees) pursuant to the Privacy Rule right of access.

For those BAs who make PHI directly available to individuals seeking to exercise their right of access - including ROI vendors, who, like other BAs, take on this responsibility by choice - OCR should fully enforce 45 CFR 164.524 against entities who fail to provide such access in accordance with the Privacy Rule.[8] Otherwise, covered entities would have liability for BA noncompliance.

c) Alternatively should covered entities be treated only as covered entities and not be considered BAs?

Ciitizen Response:
We believe it is confusing to individuals (and companies like Ciitizen who help them exercise their right of access) when they are told by a covered entity that PHI possessed by that entity nevertheless must be obtained from another covered entity because the covered entity receiving the individual's request is holding the requested information in its capacity as a business associate. A clear advantage of treating all covered entities as covered entities is more clear accountability with respect to the individual rights provisions of the Privacy Rule (and likely overall less confusion). Prior to the passage of HITECH and the enactment of provisions making business associates directly liable for HIPAA compliance, it was necessary for the Privacy Rule to include provisions that would at least require covered entities to hold business associates accountable. However, in a post-HITECH era, where the overall goal should be regulatory compliance, OCR can take steps to reduce confusion (and the inefficiencies it causes) but without any meaningful reduction in privacy and security protections.

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

Ciitizen Response: Treating covered entities as covered entities, regardless of the role they play, has the potential to reduce confusion and inefficiencies.

[7] See discussion of transition provisions at 78 Fed. Reg. 5566, at 5602-03 (January 25, 2013).
[8] Potentially relevant statutory authorities: Section 4006(b) of the 21st Century Cures Act (P.L. 114-255) expressly amended the HITECH Act to make clear that if an individual makes a request to a BA under the individual right of access, the BA may provide that individual (or his or her designee) with the requested access or copy. Section 13404 of the HITECH Act provides that the "additional requirements of this subtitle that relate to privacy and that are made applicable with respect to covered entities shall also be applicable to such a business associate…".

6) Do health care providers currently face barriers or delays when attempting to obtain PHI from covered entities for treatment purposes?

Ciitizen Response: It is not my experience (as a regulator, in working as counsel to covered entities, and as a privacy thought leader) that the permissive disclosure provisions of the HIPAA regulations present obstacles to, or place unnecessary burdens on, the ability of CEs or BAs to conduct care coordination and case management. HIPAA's permitted uses and disclosures enable a broad range of uses and disclosures to facilitate care coordination and case management. The problem is not that the rules themselves introduce obstacles – but overly conservative or mis-interpretation of those rules. As noted above, entities also use HIPAA as an excuse not to use or share data (or to place complicated obstacles in front of such uses and disclosures) when the real reason for not sharing data is a business or other anti-competitive reason. HIPAA provides very few, if any, outright barriers – instead, there are clearly articulated pathways for uses and disclosures that facilitate health care system transactions (including those that contribute to better care coordination, case management and value-based care) while protecting individual privacy rights. In circumstances where the refusal to use or share data for care coordination, case management or to contribute to value-based care is due to genuine misunderstanding of HIPAA, the solution is more clear guidance – not modifications to HIPAA that 1) are not really necessary (since the law is not the obstacle) and 2) could do more harm than good in terms of violating the privacy rights of individuals and quite possibly discouraging them from seeking treatment.

As a further note, in our efforts to obtain PHI for users of the Ciitizen platform, we are frequently told by hospital HIM departments that the PHI could be obtained more quickly if the provider requested it directly. If physicians can get this information more quickly, surely individuals (or companies acting on their behalf) exercising their right of access should be able to do so.

We also are frequently told that with respect to requests for images, hospitals will not release them directly to individuals – only to physicians (these requests typically need to be escalated to the institution's privacy official in order to get them released to individuals pursuant to the right of access). (See appendix to our comments.) These are artificial barriers. They do not reflect "burdens" created by HIPAA regulations but by misunderstanding, misapplication, and/or noncompliance with existing regulations.

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 generally, or alternatively, only for specific payment or operations purposes?

Ciitizen Response: See response to Question 6 above. When I was the Deputy Director for Health Information Privacy at OCR, I heard countless stories of covered entities (in particular, health care providers) who refused to share PHI or imposed unnecessary obstacles to sharing PHI with other health care providers, with friends and family members, for legitimate research initiatives, and even to public health authorities. HIPAA or generic privacy concerns were frequently cited as the reason for obstructions to sharing – and most of the time, HIPAA clearly permitted such sharing.

In some cases these obstructions were due to genuine misunderstandings about the Privacy Rule. ONC and OCR have worked together to produce easy-to-understand resources to clarify the provisions of the

HIPAA Privacy Rule that permitted such sharing in order to improve stakeholder understanding.[9] But far too often, HIPAA was a convenient "cover" – a stalking horse for business concerns.

The ability to pursue a covered entity or business associate for "overinterpretation" of HIPAA is an appealing prospect. But Ciitizen has significant concerns about turning any or all of the permissive disclosures for treatment, payment, and/or health care operations into required disclosures under HIPAA. U.S. and international privacy laws, including HIPAA, are based on fair information practices (FIPs)[10] that customarily require the consent or authorization of the subject of the information in order to use and disclose information, but with exceptions *allowing* uses and disclosures that are reasonably anticipated given the context of information collection (e.g., permitted uses and disclosures for treatment, payment and operations (TPO)). To turn some or all of TPO disclosures to other CEs into mandatory disclosures is inconsistent with FIPPs and runs counter to historical and recent privacy laws enacted here in the U.S. and internationally. Making disclosures for health care operations mandatory is of particular concern given the breadth of the definition of health care operations in the Privacy Rule.

Typically privacy laws require disclosure in only two circumstances – to the subject of the information and to enforcement authorities. If the goal is care coordination, the federal government has other policy levers that are much better suited to provide strong incentives for TPO disclosures (for example, Medicare payment or participation incentives and ONC and OIG's information blocking authorities under Cures).

It is also unclear how mandatory TPO disclosure provisions in the HIPAA Privacy Rule would interface with state privacy laws, which require consent or authorization to disclose sensitive health information, including serious mental illness and substance use disorder information, which Congress expressly sought to preserve in the HIPAA statute.

Ciitizen also has concerns with stretching OCR's limited enforcement resources toward enforcing TPO disclosure mandates to other CEs, which could crowd out enforcement of the individual right of access, unauthorized disclosures of PHI, and poor security practices. For example, in 2016, complaints regarding the right of access became the top category of types of HIPAA Privacy Rule complaints, surpassing unauthorized uses and disclosures for the first time.[11] At the same time complaints about unauthorized uses and disclosures continue to rank among the top five complaints,[12] and large breaches of PHI are frequently reported. The need for enforcement of Privacy, Security and Breach Notification Rules violations already surpasses OCR's enforcement resources. Asking OCR to investigate and enforce failures to affirmatively disclose information to CEs for TPO will further constrain the resources available for privacy and security violations.

As a final note, disclosures that support care coordination, case management and value-based purchasing are mandatory when they are directed by the individual who, pursuant to the HIPAA Privacy

[9] https://www.healthit.gov/sites/default/files/exchange_treatment.pdf; https://www.healthit.gov/sites/default/files/exchange_health_care_ops.pdf; https://www.healthit.gov/sites/default/files/12072016_hipaa_and_public_health_fact_sheet.pdf; https://www.healthit.gov/sites/default/files/phi_permitted_uses_and_disclosures_fact_sheet_012017.pdf.

[10] Robert Gellman, "Fair Information Practices: A Basic History," https://bobgellman.com/rg-docs/rg-FIPshistory.pdf.

[11] https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/top-five-issues-investigated-cases-closed-corrective-action-calendar-year/index.html. We do not see data for 2017 on the website.

[12] Id.

Rule right of access, requests that their PHI be sent directly to a third party. When the individual directs a disclosure to another treating provider, or a health plan, that disclosure is mandatory under the Privacy Rule and is sent with the knowledge and consent of the individual. Consequently, OCR could, through further education of covered entities and business associates regarding permitted uses and disclosures, and by strengthening and enforcing the individual right of access provisions in 45 CFR 164.524, increase disclosures of PHI for TPO, without risk of overriding individual privacy concerns.

8) Should any of the above proposed requirements to disclose PHI apply to all covered entities or only a subset?

Ciitizen Response: See response to Question #7.

9) Should a HIPAA covered entity be required to disclose PHI to a non-covered health care provider with respect to treatment, payment and/or operations?

Ciitizen Response: See response to Question 7. We further note that when an individual uses their right of access and designates the PHI be sent to a third party designee, that disclosure is both consented to by the individual and mandatory, regardless of whether the designee is or is not a covered entity. Covered entities may not refuse to fulfill the individual's request based on concerns that the recipient is "not covered by HIPAA."

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?

Ciitizen Response: See response to Question 7, where we raise significant concerns regarding OCR's proposal to make some or all TPO disclosures mandatory. If OCR does decide to move forward with making TPO disclosures (or some subset thereof) required, some verification that the request is for an accepted purpose should occur regardless of whether the recipient is or is not covered by HIPAA. In addition, there should be some verification or validation of a relationship with the individual whose information is being shared.

If the request to release information comes from an individual designating a third party recipient, there is no need to verify or validate the designee's purpose for receiving the information. As long as the request from the individual is clear and in writing, the disclosure is mandated by the Privacy Rule.

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?

Ciitizen Response: See answer to Question 7. We share the concerns submitted by individual regarding the dangers of mandating disclosures of sensitive information, such as genetic information and psychotherapy notes. Psychotherapy notes are already not required to be shared with individuals pursuant to the Privacy Rule, so disclosure to others – without the express, clear authorization of the individual – should be prohibited. Similarly, genetic information is often subject to state laws requiring consent or authorization prior to disclosure.

12) What timeliness requirement should be imposed on covered entities to disclose PHI that another covered entity requests for TPO purposes, or non-covered health care provider requests for treatment or payment purposes?

Ciitizen Response: The timeliness requirement for any required disclosures between covered entities and PHI recipients should not be shorter than the timeliness requirement for individuals to exercise their right of access. Mandatory requests for TPO disclosures should not be prioritized over individual access requests.

13) Should individuals have a right to prevent certain disclosures of PHI that otherwise would be required for disclosure? …. 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?

Ciitizen Response: See response to Question 7. A clear way to assure an individual is comfortable with a disclosure is to require it only when it is pursuant to an individual request. The HIPAA Privacy Rule right to restrict disclosures is only required to be honored in self-pay circumstances. OCR should re-examine the comments received in response to changes required under the HITECH Act necessitating disclosure restrictions and the difficulties that arise with respect to implementing that requirement.[13] Other than this requirement, covered entities are not required to honor requests for restrictions. Although there is no data available on requested Privacy Rule restrictions (at least that I am aware of), it has been my understanding (largely via anecdotal conversations with covered entities) that these requests are rarely honored due to entity concerns about facing liability if a restriction is accepted but then, operationally, cannot be fully honored. On the one hand, entities may be even less likely to accept restrictions in the face of having to honor them notwithstanding legally required disclosures; on the other hand, restrictions may be more needed if more disclosures are mandated by HIPAA.

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?

Ciitizen Response: Such concerns strongly suggest that requiring sharing for TPO only when the individual has directed such sharing (and therefore has consented to it) is the more viable policy option.

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 interests of the patient, based on the good faith of the entity, or some other standard?

Ciitizen Response: Please see responses to questions 7-15.

[13] See preamble to the Omnibus Rule, 78 Fed. Reg. 5566, at 5626-28 (January 25, 2013).

16) What consideration should OCR take into account to ensure that a potential Privacy Rule requirement to disclose PHI is consistent with the rulemaking by ONC to prohibit "information blocking"?

Ciitizen Response: As noted above in the answer to Question 7, the information blocking rule – or incentives through CMS – may be the better route for assuring that information is shared among providers for treatment and care coordination purposes.

17) Should OCR expand the exceptions to the Privacy Rule's minimum necessary standard? For instance, should population-based care management and care coordination activities, claims management, review of health care services for appropriateness of care, utilization review 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?

Ciitizen Response: Data minimization - collecting, using, and/or disclosing only the identifiable information that is needed to fulfill the purpose thereof - is a critical component of fair information practices (FIPs), which are the basis for all privacy laws, both in the U.S. and internationally. The Privacy Rule already exempts disclosures for treatment (which includes care coordination for an individual) from the minimum necessary requirement.

Eliminating the minimum necessary requirement for other purposes risks oversharing of sensitive health information, as entities, no longer required to define up front their needs for information, ask for the "entire record" or more than they need in order to be covered. This problem will be exacerbated if OCR makes the decision to make TPO disclosures (or any subpart thereof) mandatory. This data, once in the hands of the recipient, may end up being retained and used in multiple ways (as long as consistent with HIPAA, if the recipient is HIPAA covered) but potentially well beyond (and potentially unconnected to) the purpose for which it was originally shared. Already covered entities are entitled to rely on a request from another covered entity with respect to whether data requested is minimum necessary, so it's unclear why the minimum necessary protections need to be eliminated.

Of note, OCR should further clarify that minimum necessary does not apply to disclosures that occur when an individual requests information pursuant to their individual right of access, including when that information is to be disclosed directly to a third party of their choice.

18) Should OCR modify the Privacy Rule to clarify the scope of covered entities' ability to disclose PHI to social services agencies and community-based support programs where necessary to facilitate treatment and coordination of care with the provision of other services to the individual?

Ciitizen Response: OCR's previously published guidance on a similar topic is very helpful and needs wider distribution[14]; additional guidance and outreach and education on this topic could help further clarify the circumstances when it is permissible for covered entities to share PHI with social services agencies and community-based support programs where necessary to facilitate treatment and care coordination. This is also another example of where an individual, through the right of access, could

[14] https://www.hhs.gov/hipaa/for-professionals/faq/2073/may-covered-entity-collect-use-disclose-criminal-data-under-hipaa.html

direct PHI to be shared with social services agencies and community-based support programs, which helps assure this information is being disclosed with the individual's knowledge and consent.

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 ways to prevent unintended adverse consequences for individuals? For example, should CEs 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 multi-disciplinary team be required to enter into a business associate (or similar) agreement with the covered entity? ….

Ciitizen Response: OCR's previously published guidance on a similar topic is very helpful;[15] additional guidance on this topic could help further clarify the circumstances when it is permissible for covered entities to share PHI with law enforcement and multi-disciplinary/multi-agency teams. We further note that it is unlikely a BAA would be required in the context, as the agency receiving the PHI is not likely working "on behalf of" the covered entity. With respect to what "other agreement" should be required, the Privacy Rule has never necessitated the execution of data sharing agreements for disclosure of PHI under any of the permissive provisions, and we question whether such a requirement would actually frustrate such disclosures when they are helpful for treatment and care coordination.

This is yet another example of where an individual, through the right of access, could direct PHI to be shared with multi-disciplinary/multi-agency teams, which helps assure this information is being disclosed with the individual's knowledge and consent.

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

Ciitizen Response: In short, yes. See answers to Questions 18 and 19 above. We add that further clarification that the sender of the PHI is not responsible for what the recipient subsequently does with the information (as long as the disclosure is in compliance with the Privacy) would be helpful. (ONC and OCR covered this in guidance on TPO disclosures (see supra footnote 9) but reinforcement of those messages through increased outreach and education would help ensure entities are aware of them.) We have heard stories of entities reluctant to share information (particularly when requested by the individual to be sent to a third party designee) for fear of what the recipient might do with the data. This reluctance, particularly when not based on legitimate safety concerns about a particular recipient designated by the individual, cannot be permitted to stand in the way of individuals sharing their PHI with their chosen designees.

21) Are there provisions of the HIPAA rules that work well, generally, or in specific circumstances to facilitate care coordination and/or risk management?

Ciitizen Response: The right of individuals to access their health information and have it sent directly to the designee of their choice – which facilitates sharing of PHI for care coordination, case management

[15] https://www.hhs.gov/hipaa/for-professionals/faq/2073/may-covered-entity-collect-use-disclose-criminal-data-under-hipaa.html

and value-based care – has only been in effect since 2013. As noted above, complaints from individuals regarding difficulties in fulfilling the individual right of access appear to have increased in recent years (2016 year-end data show an increase; we note OCR has not posted enforcement data for 2017). Ciitizen is also reporting such stories on its website at https://blog.ciitizen.com/myhealthmydata. If the right of access were made more robust (see Ciitizen comments to Questions 1-8 above and Question 54 below), and more actively publicly enforced (versus enforced primarily through technical assistance), we could evaluate whether this pathway for facilitating the sharing of PHI for care coordination results in improved data sharing.

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

22) What changes can be made to the Privacy Rule to help address the opioid crisis…?

Ciitizen Response: We believe the Privacy Rule provides sufficient permission to covered entity providers to disclose information to friends, family, and authorities in circumstances where the individual poses a potential harm to themselves or others (or needs the assistance of family members or friends in order to combat addiction), and OCR's recent guidance on this topic is both comprehensive and helpful. Lack of adequate HIPAA training and misinformation has resulted in a climate of fear regarding disclosing information even to friends and family members. The path of least resistance (i.e., least concern about violating the law) has been to refuse to disclose and to blame HIPAA. In most cases, absent clearly articulated objection from the data subject (which should continue to be that individual's right), the information can be disclosed – but too often is not. However, forcing such disclosures – particularly over an individual's objection or without giving an individual a chance to object in circumstances where it is possible to provide the individual with the choice – could have the disastrous effect of discouraging individuals from seeking treatment.

23) How can OCR amend the HIPAA Rules to address serious mental illness? Are there changes that would facilitate treatment and care coordination for individual with SMI, or ensure that family members and other caregivers can be involved in an individual's care?

Ciitizen Response: See response to Question 22, which applies as well in the context of serious mental illness. Creating separate rules to govern disclosures of "serious mental illness" introduces the difficulty of defining what constitutes "serious mental illness" in a way that appropriately and accurately captures the nuances in levels of functionality among persons with a qualifying diagnosis.

We further note that individuals can also affirmatively authorize or designate disclosures to friends and family and other caregivers via 45 CFR 164.524 and 45 CFR 164.508.

25) Could changes to the Privacy rule help ensure that parents are able to obtain the treatment information of their minor children…if the Privacy Rule is modified, what limitations on parental access should apply to respect any privacy interests of the minor child?

Ciitizen Response: We repeat our prior comments regarding the right of individuals, including minors, to access their health information pursuant to 45 CFR 164.524 and have that information directed to a caregiver, including a parent or guardian. As long there is no coercion involved, this is a way for minors – as well as adults -- to both authorize and mandate disclosure to a parent or caregiver. To diminish the

rights of minors or elderly individuals risks discouraging them from seeking treatment for sensitive conditions.

26) The Privacy Rule currently defers to state or other applicable law to determine the authority of a person, such as a parent or spouse, to act as a personal representative of an individual in making decisions related to their health care. How should OCR reconcile any changes to a personal representative's authority under HIPAA with state laws that define the scope of parental or spousal authority for state law purposes?

Ciitizen Response: Rather than making any changes to the personal representative's authority under HIPAA, or expanding – by federal regulation – the classes of persons who can serve in this role (which could get quite complicated and risks privacy violations when the rights of individuals to make their own choices are set aside), OCR should leverage the tool they already have: enabling individuals to, through their right of access, liberally share information with friends, family, and caregivers. If the individual is not capable of executing an access request, that is likely a scenario where a person seeking to make decisions for that individual can achieve personal representative status under state law. Or it can be handled as a permissive sharing scenario where the health care provider, absent a known objection from the individual, can disclose treatment or payment-related information with a person or who is involved in that individual's care or payment for care when that provider believes that such disclosures are in the best interest of the individual.

Section c Accounting of Disclosures

Ciitizen Response: I remind OCR of the work done by the Health IT Policy Committee on this issue back in 2014 (https://www.healthit.gov/sites/default/files/facas/PSTT_Transmittal010914.pdf). These recommendations, carefully considered by a multi-stakeholder federal advisory committee after a full-day hearing on the topic, have yet to receive serious consideration.

Section d Notice of Privacy Practices

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

Ciitizen Response: As a privacy advocate, attorney to covered entities, and as a regulator, I have heard stories about individuals being told that would not be able to get health care (e.g., getting kicked out of a doctor's practice) for refusal to sign the NPP, because front desk staff thought the signature was required by law. I have also heard stories from individuals who thought the NPP was a consent form and attempted to edit the language prior to signing it or declined to sign it altogether.

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? …..

Ciitizen Response: It has been my experience as a patient that the NPP is almost always bundled with other intake documents.

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 acknowledgement of the receipt of a provider's NPP? Please specify whether identified benefits or adverse consequences would accrue to individuals or covered providers.

Ciitizen Response: The acknowledgement requirement was a well-intended effort to try to assure that individuals actually read (and ideally understood) the NPP – but I believe it instead has resulted in a lot of confusion about the purpose of the signature, as well as a belief on the part of at least some entities that individuals are required to sign it. The importance of the NPP is to provide transparency about an individual's HIPAA rights, as well as permitted uses and disclosures of data. To promote the important goal of transparency, it is far better for covered entities – and for OCR – to spend time and resources in improving the NPP so that individuals are more likely to understand their rights and have a better sense of how an entity actually uses and discloses their information (versus just what is permitted by HIPAA). With respect to the individual rights in the Privacy Rule, we know individuals are often misinformed about their rights, which may be summarized accurately in the NPP but then are miscommunicated to them when they seek to exercise those rights.

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.

Ciitizen Response: If elimination of the requirement on direct treatment providers to use good faith efforts to obtain acknowledgement of the NPP will result in time and cost savings to those providers, OCR should leverage these savings to improve the NPP with respect to communicating information about individual rights under HIPAA, as well as an entity's actual information sharing practices. For example:

- Consistent with FTC recommendations to entities regarding privacy policies, notices should be layered (with concise, easy-to-understand summaries of key aspects, accompanied by a more detailed document for individuals seeking greater information).[16]
- Notices should ideally be more clear about how rights – such as the individual right of access – can actually be exercised (for example, details regarding how to submit a request and who to talk to (with contact information) about a request, as well as information about how to file complaints with OCR, not buried at the end of a long notice).
- Notices – like privacy notices required to be posted by commercial entities – should provide information about actual uses and disclosures (versus just informing individuals about the broad categories of uses and disclosures permitted by HIPAA).
- Entities should be permitted – or even encouraged – to develop mechanisms for transparency that are not tied just to do the publication of a single document. For example, NIH's All of Us Research program includes online modules that walk people through the process of consenting to participate in the program.[17]

[16] See, for example, https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf, and https://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf

[17] https://allofus.nih.gov/about/protocol/all-us-consent-process#all-us-consent-process-videos-1.

53) With the assistance of consumer-oriented focus groups, OCR has developed several model NPPs 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. 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 consequences?

Ciitizen Response: As noted above in the answer to Question 52, transparency to individuals about their rights under HIPAA, as well as an entity's data sharing practices, should be the overall goal of the NPP. However, granting a safe harbor for use of the model NPP will lock in the current model and eliminate any incentive for entities to innovate in how they educate patients and community stakeholders regarding uses and disclosures of sensitive information. When I was at OCR, entities frequently asked for OCR to develop model HIPAA documents, such as a model BAA or a model request for individual access; if entities are not currently using the Model NPP, it is likely because entities are either unaware the Model NPP exists or they have a need to bundle the NPP with other intake documents (and hence the model NPP doesn't work for them). Issuing safe harbor protection for use of the Model NPP seems unnecessary. We also cannot recall any OCR settlement or civil monetary penalty that alleged an insufficient NPP.

b. 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?

Ciitizen Response: Please see response to Question 52.

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

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 transformation of the health care system to a value-based health care system?

Ciitizen Response:
As noted in Questions 1-6, Ciitizen has been designated by its users to collect PHI in the designated record set, and we have faced numerous obstacles – most of which are in direct contravention of the Privacy Rule, as further explained in OCR's accompanying interpretive guidance.[18] For example:

- Covered entities have told us that they cannot – or will not – provide copies of images directly to individuals or their designees. They will only provide images to health care providers. (See appendix for a recent Ciitizen blog post on this topic.)
- Covered entities, or business associates working on their behalf to process individual access requests (ROI vendors), have refused to send us copies of digital information in electronic (pdf in most cases) form.
- Covered entities or ROI vendors have refused to send us copies by unsecure email, notwithstanding a clear request acknowledging and accepting the security risks.
- We have received invoices that include "basic charges" (i.e., for search and retrieval), as well as per page charges, even when the PHI was held in electronic form and we requested a digital (pdf) copy. (We continue to get notice of delinquent charges, even though we sent letters protesting them, and we may end up having to pay them to avoid the invoices going to collection even though the charges are blatantly in contravention of the Privacy Rule.)
- Some covered entities (via the HIM Department staff) have told us that the individual must request their records in person.
- Some covered entities have treated written requests for PHI that are signed by the individual (and accompanied by individual ID or NIST LoA level 2 compliant authorization of identity) as third party requests (which are not subject to the timelines and fee limitations of the HIPAA right of access), which only results in delays for the individual.
- Some covered entities have insisted that requests must be submitted on a HIPAA authorization form (45 CFR 164.508), notwithstanding that HITECH expressly provides that PHI must be sent to the individual's designee as long as the request is in writing and clearly designates to whom the PHI must be sent (i.e., no other information should be required).
- Certified EHR technology vendors, used by covered entity health care providers to facilitate getting PHI to individuals' designated apps or services via portals or open APIs, have indicated they will charge the individual's app or personal health record service high fees for facilitating the connection (which arguably also would violate 45 CFR 164.502(a)(5)(ii), in addition to 45 CFR 164.524).
- Covered entities using Release of Information (ROI) vendors who provide only what is in a certified EHR technology portal and not the rest of the designated record set, even in circumstances when the full record, and all designated record set information, was specifically requested.

In addition, some covered entities adopt processes for medical record release – even to individuals and their designees – that, while not clearly in contravention of the Privacy Rule,

[18] We also urge OCR to review the Yale Study, supra footnote 2, for information gathered by those researchers regarding the difficulties individuals face in obtaining their health information pursuant to the HIPAA right of access.

arguably make it unnecessarily burdensome for individuals to exercise their right of access. For example:

- Covered entities refuse to accept a digital signature (such as Docusign or use of digital signature pads), even in circumstances where the request is accompanied by other evidence of the individual's identity and their authorization for the request (for example, a copy of the individual's official government photo ID like a passport or driver's license). It makes no sense that an individual can sign financial documents (for example, in my case some home purchasing documents and stock purchase agreements) using Docusign, and yet cannot use this method for requesting medical records.

- Covered entities accept only mail or fax requests – but (1) many individuals do not have access to fax machines, and (2) often the fax number is so busy with inbound requests (or the fax machine is not located close to the HIM or medical records department) that inbound requests get bounced or lost (even in circumstances where the sender has received confirmation that the fax went through).

- Covered entities require submission of their home-grown form versus accepting a HIPAA and HITECH-compliant request that is accompanied by other evidence of the individual's identity and their authorization for the request. This makes it difficult for services like Ciitizen to scale processes for obtaining records on individual's behalf.

- Covered entities not properly training HIM or medical record department staff on what HIPAA requires,[19] or not adequately monitoring the performance of their Release of Information (ROI) vendor to assure HIPAA compliance.

As noted above, we are publishing, on an ongoing basis, our experiences (and the experiences of others) in trying to exercise the right of access on our website, www.ciitizen.com, and we encourage OCR to visit the site.

These manufactured obstacles make it difficult for individuals– and also make it difficult for services like ours to scale obtaining records across patient populations. In enacting the HITECH provisions enabling individuals to use their right of access to have information sent to a third party of their choice, such as a mobile health app or an online aggregator (similar to Mint.com for your health data), Congress envisioned giving individuals the power to control all of their health data and use it and share it for their benefit. This patient-powered ecosystem cannot happen if the processes for collecting this information are allowed to still function like we are still in a paper world.

We understand and appreciate the need for covered entities (or BAs working on their behalf) to have processes for vetting requests, in order to assure that the request is coming from the individual whose records are being requested. However, we believe there are solutions covered entities and business associates can adopt in order to address these identification and

[19] We have learned it is common to locate the HIM or medical record departments within Revenue Cycle Management units of a hospital (vs. vesting them within legal or compliance departments).

authorization questions that will still enable the robust patient-centered, patient-controlled ecosystem Congress envisioned in HITECH.

We also appreciate the efforts of CMS and ONC to automate the process for individuals (and services operating on their behalf) to collect PHI – but these efforts, even at accelerated pace, will take years to be implemented. Strengthening HIPAA to make current processes work more efficiently is critical to empowering patients with their health information.

We urge OCR to give broader consideration to the many manufactured obstacles individuals (and apps or services acting on their behalf) face and make modifications to the Privacy Rule, and/or issue guidance that address obstacles beyond the timing questions raised in Questions 1-6. OCR's goal (particular in leveraging the individual right of access to facilitate greater sharing for care coordination, care management and value-based care) should be to facilitate seamless, prompt, and accurate responses to an individual access request, which benefits all stakeholders - individuals and caregivers (and services working on their behalf), as well as the providers, plans, and vendors who are required to comply with these requests. For example:

- **Require entities to implement request submission processes that leverage e-mail (widely used in other industries) and do not require in-person or mailed requests (already the case) or require use of fax.** Regulatory change would have the most impact, but OCR could start to improve this through guidance.

- **Require entities to accept any written or digital individual access request form that complies with the HITECH requirements** (i.e, entities cannot insist on submission of their own form). This likely requires regulatory change, although OCR could start to address this with guidance. We suggest three potential options to ease covered entity and business associate concerns about how to comply:
    1. Have OCR recognize a model, HITECH-compliant form and require (or provide safe harbor protections for) its acceptance.
    2. Require acceptance of any form submitted by the individual (or an app or service acting on the individual's behalf) that meets HITECH requirements.
    3. Hybrid – require acceptance of model form or any other form that meets basic requirements.

  Of note, state laws often include access requirements – but those would be preempted by HIPAA unless they provide individuals with greater access rights. More expedited timeframes or cheaper fees for access should not necessitate a submission of an institution or practice-specific request form.

- **More robustly enforce the right of individuals to make a request to have information sent to the designee of their choice pursuant to the HIPAA right of access.** The HITECH provisions giving individuals the right to have their PHI sent directly to the third party of their choice, as further articulated by OCR in the Omnibus Rule, indicated Congress' intent to enable individuals to use apps and other services to aggregate their health information. Such apps and services can help individuals navigate what can be a frustrating process to get their health information (a process that is particularly frustrating for individuals who are sick and need their information promptly for care) – but this is only possible if the covered entities honor access requests executed by individuals regardless of whether these requests come directly from the individuals, or are submitted by an app or service on their behalf.

We understand concerns from covered entities about third parties abusing this process (and seeking to get information pursuant to 45 CFR 164.524 (access) that they previously could only obtain through 45 CFR 164.508 (authorization) – but the response of covered entities to this issue cannot be allowed to create obstacles to individuals seeking to exercise their right to access their PHI and have it directly delivered to the designee of their choice. OCR could also issue further guidance and regulatory modification to improve implementation.

- **Require entity acceptance of individual identity credentials (as presented by the individual or a vendor working on the individual's behalf) meeting National Institute of Standards (NIST) requirements level of assurance (LoA) 2.** This likely requires regulatory change. To facilitate more widespread, seamless access by individuals to their health information, while also protecting the security of that information, it will be essential for entities to establish processes to honor credentials vetted by third parties (for which there are multiple options available in the marketplace). Ciitizen is happy to expend the resources necessary to credential users at LoA 2 – but if entities receiving record requests do not accept those credentials, it raises unnecessary obstacles to individuals accessing their PHI. In some cases entities impose no requirements with respect to credentials, or require submission of sensitive identity documents via mail, e-mail or fax, which also introduces security risks, both for entities and individuals. Requiring acceptance of credentials that meet federal standards creates a pathway for facilitating individual access requests in a way that provides some protections against unauthorized access. In the alternative to requiring acceptance of LoA 2 credentials, OCR could create a safe harbor for acceptance of LoA2 credentials (i.e., such credentials are presumed to meet identity proofing requirements under the HIPAA Security rule absent evidence of fraud).

  Guidance also should address OCR expectations with respect to risk mitigation. For example, OCR's expectation from an enforcement perspective is that entities take reasonable steps to address those risks (in ways that still make the request process as seamless as possible for the individual) versus imposing measures in the name of risk reduction that make the process more burdensome than necessary. Guidance should also offer acceptable steps covered entities and BAs can take, or could even establish safe harbors. For example, the VA uses a third party service to vet identities of individuals for provisioning of My HealtheVet accounts remotely. Guidance indicating that this is an acceptable approach to vetting identity and authorization could go a long way to smoothing the request process, while also managing privacy and security risks.

- **Require entities to accept electronic signatures on individual requests (such as those widely used in other commercial contexts).** Likely requires regulatory change, as guidance already is clear that electronic signatures are acceptable. Coupled with requirements for NIST LoA2 for identity credentials, the use of digital signatures creates a more seamless PHI request process for individuals, while also addressing privacy and security risks.

- **Further clarify, and more robustly enforce, the fee limitations.** Fees continue to be a problem notwithstanding extensive guidance from OCR regarding permissible fees. OCR could consider moving some of the key aspects of the guidance (such as the prohibition on state law fees that exceed HIPAA's limitations) into regulation to help make entities more aware of their obligations and assure the guidance can be enforced in its entirety. Guidance or regulation should also expressly address the charging of an individual's app or personal

record service vendor exhorbitant registration fees, in contravention of 45 CFR 164.524 and 45 CFR 164.502(a)(5)(ii).

- **Require entities (in particular, those using certified EHR technology) to accept a continuous request (e.g., "set it and forget it") from an individual**. Today entities are permitted to require individuals to submit requests each time there is new information generated in a record. This likely requires regulatory change in order to be enforceable.

- **As noted above in our response to Question 6, issue guidance (and ultimately, modify the Privacy Rule) to permit BAs to respond directly to individual access requests if they choose to do so, without respect to what is in the BAA (at least for a grace period).** BAs who choose to do so should stand in the shoes of the CE with respect to complying with 45 CFR 164.524.

- **Clarify that vendors who offer individuals an app or service for their PHI (referred to in HITECH as a personal health record (PHR) vendor) are responsible for protecting the PHI, including reporting breaches of data (per HITECH), once the PHI has been sent to the app or service per the individual's request.** Covered entities and business associates frequently raise concerns regarding whether they will be held responsible for what happens to PHI after it is communicated to the individual's designated endpoint. Clarifying that covered entities (or business associates working on their behalf) are not legally responsible for PHI communicated to an individual's designated third party could go a long way to easing these concerns. This can be done in guidance (ideally issued by OCR and the Federal Trade Commission (FTC), since FTC enforces the HITECH PHR breach notification rules).

- **Maintain the breadth of the definition of "designated record set" but provide additional clarity.** For example, we understand from some of our users that they are being denied access to information from devices (in particular, implantable devices) on the basis that this information is not "designated record set" information because it is not being used to make decisions about individuals. We disagree with this interpretation; if PHI is being routinely collected directly from an individual and stored in a record, the individual should have access to this PHI as part of the right of access, particularly if it is information that the individual could use in understanding more about his or her health or making decisions. We also have heard of questions about whether an individual's request for information to be sent to a designee can be honored through the date of the individual's death, as long as it has not been revoked, to enable information generated in caring for dying individuals to be sent to the designee of the individual's choice (for example, where an individual has designated their PHI be shared for research). Clarification in guidance from OCR should resolve both of these issues.

- **Re-confirm the right of the individual, or the individual's designee, to access PHI by unsecure e-mail** (or document upload to secure web link) if that's what the individual requests. This can be done by guidance (although perhaps instantiating in regulation might get this adopted more rapidly). Even with open APIs in more widespread adoption, individuals and apps and services acting on their behalf will need mechanisms for obtaining PHI that is part of the designated record set but is not accessible via open APIs or portals. E-mail works for many clinical documents but not for large files such as images; uploading should be another option.

- **Increase publicly visible enforcement efforts with respect to the right of access.** Enforcement through the more visible channels of settlements or imposition of civil monetary penalties sends a strong message to covered entities and business associates that OCR is serious about the right of access (whereas the provision of technical assistance, while fixing one individual's issue, is like the tree falling in the forest that no one sees or hears). This requires no regulatory modification or guidance.

Of note, some of the issues raised above are likely to become less of an obstacle with more widespread adoption of open APIs by covered entities; however, until the entirety of the designated record set is available through this pathway, efforts OCR takes to require covered entities (and business associates where applicable) to improve their processes of releasing information to individuals and their designees will empower individuals to take control of their health and assure PHI is shared to both benefit the individual (such as for treatment or care coordination) and population health.

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?

Ciitizen Response: See response to Question 54(a) above. Individuals, through their right of access, can mandate disclosures to a third party designee for care coordination, case management, and in ways that promote the transformation to value-based health care (after all, individuals pay for health care, too).

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.

Ciitizen Response: See response to Question 54(a) above.

We appreciate the opportunity to submit these comments. Please feel free to contact me at deven@ciitizen.com if you have any questions.

Respectfully,

Deven McGraw
General Counsel & Chief Regulatory Officer

Appendix (two blog posts from https://blog.ciitizen.com/)

Appendix

Blog post from 1/31/19

Documenting a Records Request

As we continue to advocate for patients and help them get their records, we wanted to give the world an inside view into what can be a thankless, endless, and often fruitless process.

These are medical records which already exist in their entirety.

Records that are a patient's lifeline to continuity of care.

Records that can provide access to life-saving clinical trials.

And lest we forget - records which are ***a patient's right to have and to hold in 30 days or less.***

Let's take a peek at the timeline of a real request by Ciitizen for records on behalf of a real cancer patient. Brace yourselves.

August 20th, 2018 - Ciitizen submits a faxed patient access request form to a leading medical institution in New York. The request asks for all health records on file. Upon receiving no response to this rather urgent request, Ciitizen calls to check on the progress. On this first call Ciitizen is advised that the request has been outsourced to a records copy service and Ciitizen must follow up with them directly.

September 17th, 2018: Ciitizen calls the copy service company. The wait time to reach a customer service representative is over 15 minutes. The patient's date of birth and name is given - the passport for receiving any information about a request - and Ciitizen is advised that there is no request on file for these records.

Ciitizen reaffirms that the medical institution confirmed the faxed request had been received and duly passed along. The copy service is unmoved by this information. They have nothing on file. Ciitizen is asked to re-fax the request. A new fax number is given.

Ciitizen re-faxes the request. Ciitizen places a *second* call to the copy service to confirm receipt of said fax. The copy service, citing their procedural policy advises Ciitizen that they will have to wait another 15 days to confirm *receipt* of the request form, let alone fulfill it.

In order to bypass this unacceptable delay, Ciitizen places a *third* call to the copy service; this time to the supervisor's department with the goal of explaining that proof of the first fax could be provided, and to remind said copy service that the records in question belong to that of a cancer patient, to whom any additional wait would be extraordinary and life-threatening. A third fax number is provided and Ciitizen is once again asked to refax. This time Ciitizen is promised a call back to confirm receipt and to advance an expedited timeline for sending the data, given the amount of days that have already passed.

At 12.41 pm EST an agent calls Ciitizen. Shockingly the agent is both aggravated and annoyed at having to place this call, talking over our patient advocate and raising her voice in sheer frustration of our

persistence. Dismayed by the agents tone, our patient advocate vehemently voices discontent at the sheer lack of professionalism, only to be hung up on!

Understandably furious, our Ciitizen employee reaches out to yet another supervisor; this time a gentleman in all senses of the word. He is horrified by the account and very much motivated to help us with our cause. He states he is now going to help with the records retrieval process moving forward, and requests a short time to review our original request. At 4.45 PM, Ciitizen receives a call back confirming the record request and a corresponding transaction number.

September 18th, 2018: The new supervisor calls our Ciitizen employee to confirm that the records will now be sent out. *By mail.* He supplies a transaction number advising that we could reasonably expect records within a week. He also offers that if we were to provide and pay for an overnight service then records could be expedited.

Given that the request form clearly, concisely, and specifically requests the records be sent *electronically* - i.e. by email - our patient advocate questions why such a request cannot be fulfilled. We're told that records cannot be sent in such a manner due to encryption reasons, as this would be a HIPAA violation. *(Side note - it is a HIPAA violation NOT to send them this way since the request asks for them in this format.)* Our patient advocate politely points out that our form addresses that issue in the full context of the HIPAA law, therefore rendering the electronic release HIPAA compliant.

And then we're put on hold. Five minutes later, the supervisor returns to the call with "great news." An electronic link to Ciitizen is offered where Ciitizen can download the patient's information with an access code. A link that provides immediate access to said records. *Finally!*

September 26th, 2018: Ciitizen receives an invoice from the company for the processing fees of these ready-to-go electronic records. Ciitizen pays the fee immediately.

September 27th, 2018: On day 37, seven days after the required 30 day time period for compliance, the link arrives.

So to sum this unsavory experience up:

7 phone calls

3 faxes

2 escalations

…and almost 2 hours of phone time to retrieve ready-to-go electronic records that are sitting waiting to be emailed out. And finally records are retrieved.

Now imagine that this responsibility befalls ***the patient*** - a cancer patient dealing with health issues that many of us can only imagine. It's utterly inexcusable.

But in reality, this is what transpires every day at a mind boggling number of major hospitals and medical centers across the USA. Change has to happen and it has to happen now. This needed change is what Ciitizen is fighting for. For you, your families, and for patients across America.

Blog post from 2/7/19

Imaging Included

As Deven stated this past Tuesday, the "designated record set"—the data that we as patients have a right to—is an often misunderstood aspect of our rights under HIPAA. As an example, many patients don't realize they have a right to copies of all of their imaging—every x-ray, CT scan, MRI, and even the photos from your colonoscopy!

Today we want to talk about our efforts at Ciitizen to obtain copies of images for our users.

When we first started asking for medical records on behalf of patients, we relied on hospital websites for guidelines on how to submit those requests. With each request we specifically stated that we were seeking images as part of the "designated record set." Early on, we gave each institution the benefit of the doubt and waited to follow-up until we were close to the HIPAA 30-day deadline. (Of note: we have since learned that follow-up within 48 hours is necessary to avoid the request going into a black, bureaucratic hole.)

When we did call to check on these early requests, it surprised us to learn that, for many institutions, a separate imaging request had to be specifically submitted to the hospital's radiology department. Needless to say, this tidbit of information was not included as part the website page of instructions on how patients should submit their requests; we actually learned this information when we called to check on the request. One institution even told us (confidentially, we presume!) that, when they received requests for radiology images, they ignored that aspect of the request, as the health information management (HIM) department was not authorized to release images to patients.

As we know, however, imaging is indeed part of the "designated record set." Yet, when we call radiology departments to determine their processes for getting x-rays to patients (or their designees), we too often hear that the radiology department will not release images to patients—only to other medical professionals. In fact, roughly one out of every ten institutions we've queried seems to think imaging is not included under the HIPAA right of access.

First, if an institution wants radiology requests going directly to the radiology department, this needs to be communicated to patients up front. Secondly, the institution is still obligated under HIPAA to provide this information to patients, so if the radiology department isn't properly trained on the HIPAA right of access (which seems to be the case at least 10% of the time), that's a serious non-compliance issue.

In one particular instance, we sent a request to a community hospital for a "designated record set," including images, on behalf of a cancer patient and had to follow up when we did not receive the information by the 30 day deadline. (Our request also had to be sent by mail—no other communication method was permitted—but we'll take on that issue on in a future blog post.)

Our request clearly indicated that the patient wanted designated record set information to be sent to Ciitizen by email (with acknowledgements of the security risks of unsecure email, as required by HIPAA), and that the institution could mail a CD with images if they were too large to be e-mailed. Nevertheless, we received a CD by mail of medical records over a month and a half later—accompanied by a letter indicating that the radiology images needed to be requested directly from the radiology department. We had already had phone conversations with the community hospital's HIM department when the records were in danger of being post-30 days, and at no point did the HIM staff tell us we needed to send a separate request to radiology. Not until we received the letter well past the compliance deadline did we learn of this necessity.

As a result of this all-too-frequent scenario, we now call all facilities ahead of time to find out directly from hospital administrative staff about the specific processes for filing requests, including for images, and we hear from far too many radiology departments that images "cannot" be released to patients as they are not part of the "designated record set" (yet, we know from Deven's blog post this is incorrect!).

It is not unusual for us to hear different policies regarding the release of radiology images (will they or won't they release to patients) from different locations of the same hospital system. That some large hospital systems don't standardize their policies isn't necessarily shocking, but the fact that they're non-compliant with HIPAA is entirely unacceptable.