OCR Consultation:

RIN 0945–AA00 Proposed Modifications to the HIPAA Privacy Rule to Support, and Remove Barriers to, Coordinated Care and Individual Engagement

February 4, 2026

Presented by:

Robert Tennant, WEDI Executive Director

(rtennant@wedi.org)

About WEDI

WEDI was formed in 1991 by then-HHS Secretary Dr. Louis Sullivan.

1992 and 1993 WEDI reports leveraged into legislative language (HIPAA).

Named in HIPAA as an advisor to HHS, we have worked closely with every Administration. We have productive working relationships with OCR, CMS, and ASTP/ONC.

WEDI has 17 workgroups, including a WG on Privacy & Security, and conducts educational programming on a wide array of health IT topics..

WEDI Convenes, Collaborates, Educates and Advises

WEDI's Member Position Advisory Process

Purpose: Ensure members provide input and data to assist the WEDI Board in developing recommendations, comments and positions that reflect the views of our diverse members.

Stakeholders: WEDI's diverse members include Federal and State Government, Payers and Payer associations, Providers and Provider Associations, Clearinghouses, Health IT Vendors, Standards Development Organizations, and Patient Advocate Organizations.

OCR NPRM Events: WEDI held a member event on April 7, 2021 to discuss the Privacy Rule NPRM and an event Feb. 11, 2025 on the Cybersecurity NPRM. 100+ members participated at each, representing every major stakeholder group.

Output: Discussions at these events were leveraged in the development of the WEDI comment letters-approved by the Board of Directors.

OCR 2021 NPRM Proposals and WEDI Responses/Recommendations

1. Timing

OCR Proposal: *…the Department proposes to amend the individual access right provisions to require CEs to provide copies of PHI as soon as practicable, but no later than 15 calendar days (with the possibility of one 15 calendar-day extension)*

WEDI Response:

WEDI is very supportive of patients having access to their health information. The challenge is balancing that right of access with the burden CEs incur producing the requested information. There are many reasons for why a CE might require more than the proposed 15 days (plus extension) to retrieve the PHI, including.

–PHI maintained in multiple facilities.

–PHI maintained in multiple systems.

–PHI maintained by business associates.

–PHI maintained in different forms and formats (i.e., electronic, PDF, Excel, images, paper).

–Physician review of the record.

WEDI Recommendations

1. **Maintain the current approach** of providing the CE up to 30 days to fulfill the patient request for access to their medical record and the current approach of providing a one-time additional 30-day extension.
2. Many CEs, especially smaller one, do not maintain continuous operations and may temporarily suspend business due to volunteer activities, vacations, emergencies, staffing limitations, or severe weather events. Accordingly, we encourage OCR to clarify that any response timeframe is calculated based on the **number of days the covered entity is open** and providing services, rather than calendar days.
3. **Maintain the current approach of permitting the clinician to review** the designated record set and to redact any information that could prove, in their professional judgement, harmful to either the patient or someone else.
4. Should any modification be made to the length of time a CE is permitted to respond to the request, we urge the agency to **ensure any final rule provides sufficient time** for CEs to change internal policies and modify the content of NPPs.
5. **Engage in an educational campaign** aimed at informing patients of their right to access their medical record (or a specific component of the record) and that they can request that it be provided to them in a specific time frame and format.

2. Form and Format (APIs)

OCR Proposal: *For example, if a covered entity has implemented a secure, standards-based API that is capable of providing access to ePHI in the form and format used by an individual's personal health application, that ePHI is considered to be readily producible in that form and format, and that is also the manner by which the ePHI may be directed to a third party."*

WEDI Response:

–WEDI fully supports moving to a health care system where data flows seamlessly among stakeholders to achieve improved health outcomes for all individuals, while at the same time ensuring that the privacy and security of the information is maintained.

–We continue to be concerned that patients will not have adequate information to be educated consumers and may not fully comprehend that they are assuming the risk of the security practices implemented by their chosen app.

–Consumers do not necessarily understand when their information is and is not protected by HIPAA. While we appreciate HHS's guidance clarifying that health care providers are not responsible under the HIPAA Security Rule for verifying the security of a patient's chosen third-party app, this "safe harbor" does not address the potential vulnerability of patient information when sent to the app.

WEDI Recommendations

1. HHS should develop an approach for **how CEs share PHI with these non-HIPAA entities** and ensure that such third-party apps are equipped to securely handle sensitive patient information.
2. Under current regulation, CEs are not permitted to require formal verification checks on individual third-party apps before allowing the application to connect to its API. HHS should provide **further guidance on what "verification" will be permitted** and how CEs should review of third-party apps themselves before permitting them to connect.
3. Further, HHS should engage with the private sector in the **development of a certification framework for third-party apps** seeking to connect to APIs of certified health IT. Such a program would not only foster innovation but also establish improved assurance to patients of the security of their information.

3. Notes, Videos, Photographs

OCR Proposal: *The Department also proposes to add a new right at 45 C.F.R. 164.524(a)(1)(ii) that generally would enable an individual to take notes, videos, and photographs, and use other personal resources to view and capture PHI in a designated record set as part of the right to inspect PHI in person…*

WEDI Response:

-We are concerned that the proposal, which differs from current practice by eliminating any discretion by the CE and making access in this manner an individual right, **could have adverse consequences to both the delivery of care and the privacy of other patients**.

-Allowing such a right would, at a minimum, **disrupt workflow and divert resources** in the form of staff and equipment away from patient care.

-It would also **significantly increase the privacy risks to other patient records** since this risk could not be mitigated without substantial logistical and operational system redesigns. Released via social media or other mechanisms, these recordings pose significant threats privacy and security risks to patients, employees, and the security of the facilities.

WEDI Recommendation

- We urge HHS not to mandate this type of electronic access as an individual right but rather encourage CEs to designate a secure area and offer this service voluntarily.

4. Impeding Access

OCR Proposal*: The Department proposes to clarify that, while an entity may require individuals to make requests for access in writing (as currently provided in the second sentence of section 164.524(b)(1)), it would not be permitted to do so in a way that impedes access…*

WEDI Response:

–We concur that a CE employing a standard form containing the minimum information that is needed to process a request for access is a reasonable step.

–We also agree that a CE requiring the individual to complete a form requiring information that is not necessary to fulfill the request is unreasonable as is a requirement that the individual obtain notarization of his or her signature.

–CEs should not require individuals to submit requests only in paper form, only in person at the CE's facility, only through the CE's online portal, or impose unreasonable identity verification.

WEDI Recommendation:

This proposal is a positive step and should enhance the individual's ability to gain access to their PHI. We continue to oppose unreasonable barriers or processes that unfairly impact an individual's access to their health information and **recommend that HHS publish comprehensive guidance regarding acceptable and unacceptable request processes**.

5. Access

OCR Proposal: *If an individual makes a clear, conspicuous, and specific request that his or her covered health care provider or health plan (‘‘Requester-Recipient’’) obtain an electronic copy of PHI in an EHR from one or more covered health care providers (‘‘Discloser’’), Requester-Recipient would be required to submit the individual’s request to Discloser, as identified by the individual.*

WEDI Response:

This new right would be inserted within the right to direct an electronic copy of PHI in an EHR to a third-party. HHS also proposes technical clarifications to the Privacy Rule provision requiring business associates to disclose PHI as needed for the CE to fulfill its obligations under the right of access.

WEDI Recommendations:

1. WEDI supports permitting the individual to direct copies of PHI to a third-party but **recommends this right be limited to only electronic copies of PHI in an EHR**. We also support that the request to direct an electronic copy of PHI in an EHR to a third-party designated by the individual be made in a “clear, conspicuous, and specific” manner.
2. However, **we do not agree that this request should be permitted to be oral**. We recommend the final regulation exclude this provision, or in the alternative, provide specific guidance as to how a CE will be expected to appropriately verify oral instructions. Having a request submitted on paper will reduce any potential confusion and ambiguity related to the specific needs of the individual.

6. Fees

OCR Proposal*: The Department proposes to modify the access fee provisions to establish a fee structure with two elements based on the type of access request. The first element describes categories of access for which covered entities cannot charge a fee. The second element describes the allowable costs that may be included when an access fee is permitted.*

WEDI Recommendations:

1. **WEDI strongly supports individuals having access to their PHI and cost should not be a barrier to that access**. Today, CEs are very familiar with the current fee requirements and limitations, and we recommend **HHS retain the existing flexibility** with "reasonable cost-based fees" and permit CEs to determine whether to waive fees, especially for individuals who have limited financial means.
2. In addition, with so many potential form and format variations impacting cost, **we do not believe providing an advance estimate of fees and an itemized list of fees would be helpful** for the patient. CEs now can offer the patient an estimate of the cost tailored on their specific request. This in turn can lead to a discussion between the individual and the CE to determine and meet the specific needs of the individual.
3. Further, should HHS move forward with this requirement, the Department should **specify when the itemized list of charges must be provided** and whether a CE should be able to charge a reasonable cost-based fee for the preparation of the itemized list.

7. Identity Verification

OCR Proposal: *The Department proposes to modify paragraph (2)(v) of 45 C.F.R. 164.514(h) to expressly prohibit a covered entity from imposing unreasonable identity verification measures on an individual (or his or her personal representative) exercising a right under the Privacy Rule*

WEDI Recommendations:

1. **We concur with HHS's intention to expressly prohibit a CE from imposing unreasonable identity verification measures on an individual**. The challenge is balancing the requirement against an unreasonable verification demand and ensuring that appropriate verification takes place. As the nation moves forward with API-based interoperability, identity management will be critical.
2. WEDI shares the overall goal of ensuring that sufficient (and effective) verification is conducted to confirm the correct individual is getting PHI. **HHS should publish additional examples of what are considered reasonable and unreasonable CE requirements**.
3. Finally, we recommend CEs have the **flexibility they need to deploy appropriate identity verification policies**.

8. EHR Definition

OCR Proposal*: The Department seeks comment on the scope of this proposed definition for EHR, including billing records for health care.*

WEDI Response:

–Many providers have systems separate from the EHR (i.e., **practice management system or billing system software**) and in some providers are maintained by third-party billing vendors. Including billing records in the definition would require combining the records from different systems, in different formats, using different software, and even housed in different locations. Most importantly, billing records contain the same clinical information that would be maintained in the EHR.

WEDI Recommendation:

WEDI supports the HHS proposal to limit the definition of an EHR to records held by covered health care providers that have a direct treatment relationship with the individual, as this is consistent with the definition in the HITECH Act.

However, **we do not support expanding the definition of an EHR to include non-clinical records such as billing records**. Should HHS include billing records in the definition it would impose a significant administrative burden on providers.

9. Health Care Operations

OCR Proposal*: The Department proposes to clarify the definition of health care operations in 45 C.F.R. 164.501 to encompass all care coordination and case management by health plans, whether individual-level or population-based.*

WEDI Response:

–HHS proposes to modify the definition of "health care operations" to clarify that the **term includes care coordination and case management for individuals**. The current definition is sometimes read to cover only population-based activities, with the result that some CEs believe that health plans are not permitted to use and disclose PHI to coordinate care for individuals.

–This can result is situations where PHI is not transmitted, **and care delivery is therefore negatively impacted**. In addition, the rule proposes to add an exception to the minimum necessary standard for disclosures to, or requests by, a health plan or provider for care coordination and case management.

–As an increasing number of CEs are entering into Alternative Payment Models such as Accountable Care Organizations (ACOs) where the ability to exchange the full range of PHI is even more critical. **We note that an ACO may require access to the entire medical record of each of its attributed patients to efficiently conduct case management or care coordination.**

WEDI Recommendations

1. **WEDI supports HHS efforts to facilitate improved care coordination**. As the industry transitions increasingly to value-based care, we are hopeful that these revised policies will translate to enhanced care delivery and improved patient outcomes.
2. We recommend HHS **release guidance that provides specific case management and care coordination examples**.
3. Some CEs have adopted policies of refusing to release patient records, even for TPO purposes, without a signed patient authorization. **HHS should undertake an education and communication effort** aimed at informing patients and CEs of the right to disclose PHI for TPO purposes.
4. OCR must also **balance these modifications** with additional safeguards that will ensure that patient privacy is maintained.

10. Good Faith Belief

OCR Proposal*: Department proposes to amend five provisions of the Privacy Rule to replace ‘‘exercise of professional judgment’’ with ‘‘good faith belief’’ as the standard pursuant to which covered entities would be permitted to make certain uses and disclosures in the best interests of individuals.*

WEDI Response:

–We believe that modifying the current HIPAA Privacy and Security Rules **could impact the opioid crisis**. We believe that educating patients and CEs on issues regarding appropriate disclosures of PHI will also have an impact.

–Some assert that HIPAA prevents clinicians from exchanging information with family members or caregivers of patients suffering from an opioid-related illness. We do not believe this to be the case. **There is appropriate flexibility built into HIPAA-permitting clinicians to directly engage with those closest to the patient** and who can provide key data to assist the clinician in delivering care.

WEDI Recommendation:

Providing unfettered access to information **must be balanced with the wishes of the patient**. We discourage HHS from pursuing changes to the HIPAA Privacy Rule that would result in patients suffering from opioid-related illnesses losing control over their medical record. These patients, if they are to confide in and trust their clinician, must still have the reassurance that their record will not be disclosed inappropriately.

11. Personal Health Application

OCR Proposal: *Department's proposal to address the use of personal health applications in the right of access, the Department proposes to define personal health application in the HIPAA Rules as "an electronic application used by an individual to access health information about that individual in electronic form, which can be drawn from multiple sources, provided that such information is managed, shared, and controlled by or primarily for the individual, and not by or primarily for a covered entity or another party such as the application developer…*

WEDI Response:

–WEDI believes the PHA offers significant promise for sharing PHI with patients. As more providers adopt EHRs with API capabilities, the PHA can permit patients to gain rapid access to their health information. At the same time, **there are potential confidentiality concerns with allowing non-HIPAA covered entities unfettered access to PHI.**

–The proposed rule requests comment on whether **CEs should be required to educate or warn individuals** that they are transmitting PHI to an entity that is not covered by the HIPAA Privacy and Security Rules.

–We continue to be concerned that individuals could have their information inappropriately disclosed and **we do not feel it is appropriate to put the burden of warning the individual on the shoulders of the CE.** CEs will typically not be experts on app data privacy and security protocols and will have little time to warn patients of the potential dangers associated with transmitting ePHI to third-parties not covered by the HIPAA protections.

WEDI Recommendation:

HHS should clarify that a disclosure to a PHA equates to a disclosure of PHI to a third-party. As well, **HHS should consider developing model language that CEs could share with patients, warning of the potential dangers**.

12. NPP

OCR Proposal*: The Department proposes to eliminate the requirements for a covered health care provider with a direct treatment relationship to an individual to obtain a written acknowledgment of receipt of the NPP and, if unable to obtain the written acknowledgment, to document their good faith efforts and the reason for not obtaining the acknowledgment.*

WEDI Response:

- The process of **obtaining and storing a written acknowledgment of receipt of the CE's NPP can be burdensome**. For providers, new patients coming to a care delivery site will be required to complete multiple forms prior to being seen by clinical staff. The written acknowledgement of receipt of the NPP is typically included in this set of intake forms.
- There is also administrative **burden associated with storing the completed acknowledgement form**. CEs will typically store it in the patient's paper record or scan the document into the practice management system (PMS) or EHR. It must be kept with the patient record and accessible upon request.
- **More challenging is when the patient cannot or will not sign the acknowledgement of receipt**. In these cases, staff are currently required to make a good faith effort to obtain it.

WEDI Recommendations

1. One opportunity to reduce the burden associated with obtaining and maintaining the written acknowledgement of receipt of the CE's NPP would be to **waive this requirement should the CE post the NPP in a prominent and public area of their facility and on their website** (as they are currently required to do so). Having the NPP posted on the website allows organizations offering services that would not require the patient to be physically present at the time of service to have their NPP accessible to the patient.
2. Similarly, we urge HHS to **remove the requirement for health plans to seek permission to distribute the NPP electronically**. Health plans typically offer their members access the NPP via plan websites, and many send NPPs to members via email if an individual consents to receiving electronic communications.
3. We would also recommend **removing the obligation** to send a paper notice every 3 years.
4. Overall, we recommend that **HHS waive the requirement to obtain a written acknowledgement of NPP receipt**. This would allow for all HIPAA CEs to benefit from reduced administrative burdens and provide more flexibility to deliver NPPs to individuals who have a relationship with a CE.

13. Changing the Model NPP

OCR Proposal*: The Department requests comment on ways the model NPP could be changed to improve consumer understanding*

WEDI Response:

–WEDI **applauds HHS for its development of model NPPs**. These are colorful, easy-to-read documents that convey the necessary information to patients.

–We also appreciate the fact that the **model NPPs can be customized** to meet the specific needs of individual CEs. We have heard that the HHS model NPP has been well-received by CEs.

–In addition to modifying the required contents of the NPP to support the final rule, we would **recommend HHS engage with consumer and CE organizations to promote use of the HHS model NPP**.

WEDI Recommendations

Education for CEs is critical if patients are to be made aware of their rights under HIPAA (including NPP requirements). In many cases, patients often rely on the CE to provide this education. WEDI recommends HHS consider the following education opportunities for CEs:

1. HHS could **develop educational posters** and post these on its website.
2. Partner with WEDI, other stakeholder organizations, and patient advocacy groups on **webinars/educational sessions**.
3. Conduct "**open door**" type calls for impacted stakeholders and include a Q/A component.

14. RFI: Accounting of Disclosures

OCR Proposal*: The RFI sought information about implementing a requirement of the HITECH Act to include disclosures by a covered entity for treatment, payment, and health care operations through an EHR in an accounting of disclosures*

WEDI Response:

–HITECH changes the accounting of disclosures requirement to **include even disclosures for TPO**. Under HITECH, if a CE, such as a physician practice or hospital, utilizes an EHR, the organization will be required to account for TPO disclosures.

–Upon receiving a request for such a disclosure, the **CE will be required to provide individuals with an accounting of disclosures of PHI which occurred within the 3 years prior to the date of the request**.

–The Secretary is also required to determine the **administrative burden in providing the accounting**.

–HITECH stipulates that the TPO accounting is only required for those CEs that have adopted an EHR- **suggesting the government believes TPO disclosures would be stored on this one clinical system**.

–This is simply not the case. CEs typically store their clinical data in an **EHR, PMS with PHI also potentially housed in other computer systems (i.e., Clinical Trials)**. Satisfying an accounting of disclosures for TPO requests in most CEs will not a simple keystroke. Completing these types of reports requires a substantial amount of manual collection from multiple data sources. **Larger providers many have dozens of different electronic systems that store PHI.**

RFI: Accounting of Disclosures

WEDI Response:

–Should the accounting of disclosures be expanded to include TPO, the effort to produce a report would **increase exponentially**.

–Further, in cases where a patient may have been seen multiple times over the required reporting period at a larger organization (utilizing perhaps numerous services and locations), the document given to the patient could literally be **hundreds of pages** in length and virtually indecipherable for the patient.

–WEDI is also concerned that a potential accounting of disclosures report to the patient could include **specific names of individuals** within the CE and the action they took. Releasing this level of information raises important security concerns for those individuals who may become targets for discontented patients or family members.

–This could lead to **unwarranted threats, harassment, or even potential physical harm to workforce members**.

WEDI Recommendations

1. Overall, **we do not believe patients have interest in receiving a lengthy report** explaining which staff looked at their medical record for purposes of treating them, submitting their claim to insurance to limit their out-of-pocket expenses, or for performing health care operations such as quality measurement.
2. We encourage HHS to **focus on providing education** for patients and CEs on the right of the patient to request that their medical record **not be disclosed** to designated individuals.
3. We urge the Department **not move forward with requiring CEs to issue accounting of disclosure reports for TPO**.

Additional Issues

15. Compliance Dates

WEDI Recommendation*:*

We note that CEs are focused on meeting the challenges associated with implementing numerous other federal mandates. To facilitate a streamlined compliance glidepath for all CEs, **we recommend the compliance timeframe for any final rule be a minimum of 24 months from the effective date of any final rule**.

16. Addressing Ransomware

-HHS currently **considers a ransomware attack a data breach**, and thus CEs attacked by ransomware are subject to the same process for both notification and enforcement as laid out in the Breach Notification Rules contained in the 2013 HIPAA Omnibus regulation.

-We assert, however, **that this equating of ransomware with a traditional breach of PHI is inappropriate and should be changed**.

-Although the broad definition of a breach as an “impermissible use or disclosure of protected health information” may apply to certain ransomware attacks, we believe **there are inherent differences between the two threats to PHI**.

WEDI Recommendations

We recommend the following steps be taken to better address ransomware threats:

1. **Move from a culture of "blaming the victim"** to one focused on transparency and action.
2. **Continue developing reasonable ransomware transparency and enforcement policy**. HR 7898 (amending HITECH), known as the **HIPAA Safe Harbor amendment**, incentivizes health care organizations to adopt recognized cybersecurity best practices by potentially reducing penalties for breaches. This is a good start and a launching pad for additional measures.
3. **Create a process of voluntary real-time ransomware reporting**. Provide a platform where CEs can voluntarily report a ransomware cyberattack as it is occurring or if suspected. This disclosure should not prompt disciplinary action under HIPAA unless there is evidence of recklessness on the part of the CE. Rather, this action should begin an urgent, cooperative investigation to preserve the integrity of the extorted data and prevent further damage.

WEDI Recommendations

4. Develop an HHS website focused solely on cybersecurity for health care stakeholders. This website should: (i) Present the latest information on cybersecurity focused on the health care sector; (ii) Promote practical, easy-to-comprehend guidelines and best practices; and (iii) Compile cybersecurity educational resources from federal agencies.
5. Expand educational outreach. HHS should fully fund a cybersecurity educational outreach program, with specific emphasis on smaller and rural CEs. Communication vehicles could include “open-door” telephone forums, newsletters and bulletins, interactive webinars featuring cybersecurity experts, and face-to-face presentations.
6. Engage directly with WEDI and other appropriate organizations to solicit feedback regarding educational content and outreach strategies.

17. 2025 Cybersecurity NPRM

Key WEDI Recommendations:

1. Implement a national health care cyber "**Fire Drill**"
2. Encourage the development and support of private sector **accreditation/certification** programs
3. Develop a **centralized, comprehensive website** for educational materials and guidance to support covered entity compliance
4. Identify opportunities to **reduce industry implementation costs**
5. **Strike the appropriate balance** between promoting effective cybersecurity requirements and avoiding imposing undue administrative and financial burden on stakeholders

18. High Level Observations

1. The Privacy Modification proposed rule was released almost 5 years ago. **Considerable changes** have occurred in the health care industry since 2021, including:
   - **New rules and legislation** (national and state) have enhanced how information is accessed, exchanged, and used by patients, clinicians, and other stakeholders. Most importantly, OCR has published the Part 2 SUD final rule in 2024, and others, ASTP/ONC and CMS have implemented policies addressing information blocking, enhancing patient access to their records, and assisting real time decision-making informed by longitudinal medical information.
   - **AI, wearables, telemedicine and other technologies** are driving innovation. All have privacy and security implications.
   - **Cyberattacks are on the rise** and their impact on health care operations can be significant-even impeding the delivery of care to patients.

18. High Level Observations

2. Securing our health care infrastructure is a national imperative. We believe there is a **need for public sector investment to assist CEs improve cyber hygiene and closer collaboration** between the public and private sectors.
3. In the area of **Information Blocking**, we urge OCR to continue working with ASTP in the development of industry guidance.
4. Understanding the significant changes in the health care environment since the publication of the 2021 NPRM, we believe it best for the agency to **solicit additional industry input** with a lens on current technologies, etc. as a next step in their processes.

On behalf of WEDI leadership, the Board of Directors and our members, we thank OCR for the opportunity to provide input on this important regulation.