RE: TEFCA Individual Access Services (IAS) Exchange Purpose Changes Under Consideration 2026

To whom it may concern,

On behalf of the CARIN Alliance, we write today to clarify a number of important issues that were raised in various comment letters on the recently proposed updates to the SOP for Individual Access Services within the TEFCA Framework.

About the CARIN Alliance

The CARIN Alliance is a non-partisan multi-sector group of stakeholders representing numerous hospitals, thousands of physicians, and millions of consumers and caregivers. The CARIN Alliance is convened by David Blumenthal, David Brailer, Aneesh Chopra, and former HHS Secretary Mike Leavitt, to unite industry leaders in advancing the adoption of consumer-directed exchange across the U.S. Working collaboratively with government leaders, the group seeks to rapidly advance the ability for consumers and their authorized caregivers to easily get, use, and share their digital health information when, where, and how they want to achieve their goals.

Specifically, we promote the ability for consumers and their authorized caregivers to gain digital access to their health information via the standards-based APIs required under the 21st Century Cures Act rules, CMS 9115-F, CMS 0057-F, Information Blocking and HTI Rules, and others. We also believe that it is the patient's right to have that information sent to any third-party application they choose, consistent with HIPAA. With a membership composed of patients and caregiver organizations, health care entities, health information technology vendors and others, the CARIN Alliance is uniquely positioned at the intersection of public and private organizations to advance the development of person-centered, value-driven health care through the adoption of consumer-directed health information exchange.

In summary, we believe:

- Consumers and their authorized caregivers should easily be able to get, use, and share their digital health information when, where, and how they want it to achieve their goals.
- The use of whatever tool they choose, including third-party, consumer-facing applications, should be facilitated within and without the TEFCA framework, the CMS Health Technology Ecosystem, and individual API Connection.
- Consumer-directed exchange supports sharing of personal health information with non-covered entities, which are not regulated by HIPAA and therefore not subject to the same privacy and security rules as providers, plans, and clearinghouses.
    - Once data is shared, we agree with OCR and HHS that the original Covered Entity/data holder is no longer responsible for the exchange of the data.

We write now to challenge claims in the April 24, 2026 letter from the American Hospital Association (AHA) to Mariann Yeager, the RCE Program Lead for TEFCA, that provisions in TEFCA Individual Access Services (IAS) SOP 3.0 conflict with covered entity (hospital) obligations under the Health Insurance Portability and Accountability Act (HIPAA) regulations, as well as modifications to those rules enacted by Congress in the Health Information Technology for Economic and Clinical Health Act (HITECH).[1] Under the AHA's claims,

[1] https://www.aha.org/lettercomment/2026-04-24-aha-comments-tefca-individual-access-procedure.

HIPAA prevents individuals from using personal health applications to access their protected health information (PHI) through TEFCA, notwithstanding decades of federal law, regulation and policy.

As explained in more detail below, we find these claims to be without merit. The HIPAA Privacy Rule individual right of access provisions at 45 CFR 164.524 are the foundation for the IAS SOP 3.0. While most provisions of the Privacy Rule create the framework for the permissible use and disclosure of PHI without a valid HIPAA authorization from the individual who is the subject of the PHI, Section 164.524 establishes an affirmative obligation of covered entities to provide individuals (upon request) with copies of PHI from their designated record set, in the form and format that the individual requests, unless that form and format is not readily producible by the covered entity.[2] The HHS Office for Civil Rights, which enforces HIPAA, has endorsed in guidance the ability of individuals to use apps to access their health information through their HIPAA right of access (cited and discussed further below). Consequently, **the other provisions of HIPAA cited by AHA must be read by covered entities to facilitate exercise of the right of access, not to conflict with it.** It is surprising that the penultimate HIPAA provisions that govern IAS, and are a requirement for AHA member hospitals are not even cited once by the AHA.

Also not mentioned by the AHA are the information blocking rules issued pursuant to the federal 21st Century Cures Act ("Cures Act"), which double down on HIPAA's individual right of access requirements by creating an expectation that hospitals and other medical providers provide patients with seamless access to their electronic health information, including through the use of apps, with financial disincentives for providers who fail to do so.[3] Even before the Cures Act was enacted, Congress enacted the Medicare Access and CHIP Reauthorization Act of 2015 ("MACRA"), which introduced the quality reporting and incentive payment program for Medicare eligible providers. The "Promoting Interoperability" performance category for Medicare's Quality Payment Program incentivizes eligible clinicians to ensure that a patient's health information is available for the patient (or patient-authorized representative) to access using ***any application of their choice"***.[4]

Building off existing law, regulation and policy, the Centers for Medicare and Medicaid Services launched the CMS Interoperability Framework in July 2025 as a voluntary initiative whereby providers and data networks pledge to quickly facilitate the seamless digital access by patients using medical applications, without patients having to authenticate and authorize individual connections through their selected app with each responding data source (essentially, the pathway proposed in 2a and 2b of the SOP).[5] Critically, CMS launched this initiative on the following principle: Nothing in its framework is intended to contravene federal and state healthcare and privacy laws, including HIPAA and the Privacy Act.[6] Patient access to their health information, using modern technologies used by consumers in nearly every other aspect of their lives, is clearly a longstanding priority of federal legislative and executive branch policy, and current Administration initiatives.

The foregoing summary of federal law, regulation and policy illustrates a history spanning the last two decades where multiple Congresses and administrations have made clear policy decisions aimed at

---

[2] There are exceptions to this right, but they are rare. See 45 CFR 164.524(a)(2)-(3).

[3] See 45 CFR Part 171, as well as guidance from the HHS Office of the National Coordinator at 85 Fed. Reg. 25642, at 25790-25901 (May 1, 2020) (hereinafter, the "Final Information Blocking Rules").

[4] https://qpp.cms.gov/reporting-requirements/measures-activities/explore (select Promoting Interoperability category, and the Provider to Patient Exchange measure).

[5] https://www.cms.gov/health-technology-ecosystem/interoperability-framework.

[6] Id.

facilitating patient and consumer access to their health information. For this reason, we strongly assert that any action taken in the context of Individual Access Services must begin with the understanding that consumers must have easy access to their health information, through whatever tool they choose, without needing to undertake special efforts to access that information. Claims that policy-makers intended to limit consumer choice in what information they can access, or the tools through which they may access that information, are counter to both Congressional intent and administrative applications of law.

Supported by this long-standing bipartisan policy mandate, patient use of apps to aggregate, manage, and use their health information is growing. A recent study found that patients are increasingly using apps to access their medical records, growing from 38% in 2020 to 57% in 2024.[7] While use of apps to aggregate medical records from multiple providers still lags (7% in 2024), it is a significant increase from 2% in 2022.[8] The study author speculates that the reason for the slower uptake is patient lack of knowledge of the capability.[9] We posit that slower uptake is also due to the challenges with connecting and maintaining app connections to multiple portals (commonly referred to as "hyperportalitis"[10]), which this SOP, through approaches 2a and 2b, is attempting to address.

The evidence is clear that federal policy points in the direction of facilitating patient access through their chosen apps. Given this backdrop, and as explained further below, **we believe the provisions cited by the AHA - when read in concert with current law, policy and Administration priorities - can and should be interpreted to support what has been proposed in SOP 3.0 2a and 2b.** If anything, movement to 2a and 2b should be accelerated to advance patient access using apps.

We acknowledge there is some uncertainty today over whether an individual access request coming through an individual's chosen app is a request for the patient to access their PHI directly or is a request of the individual to have their PHI sent to the third party of their choice, per HITECH. But whether this is considered to be a request from an individual directly or a request by an individual to have PHI sent to a third party (the position taken by AHA), both pathways are part of the HIPAA Privacy Rule individual right of access.[11] To address this uncertainty, OCR has proposed changes to the HIPAA Privacy Rule right of access provisions to treat requests coming through personal health applications as individual access requests, with the "form and format" of that request being through their chosen app.[12] This rule is currently pending finalization.[13]

---

[7] Richwine, C. "Individuals' Access and Use of Patient Portals and Smartphone Health Apps, 2024," Office of the Assistant Secretary for Technology Policy Health IT Brief (posted online July 2025).
https://www.ncbi.nlm.nih.gov/books/NBK606034/

[8] Id.

[9] Id.

[10] According to Google AI, "'Hyperportalitis' is a term coined by The Sequoia Project in 2023 to describe the patient frustration caused by navigating too many separate, non-interoperable healthcare provider portals. It highlights the need for better health data interoperability, which the organization addresses through initiatives like TEFCA."

[11] "In applying section 164.524 of title 45, Code of Federal Regulations, in the case that a covered entity uses or maintains an electronic health record with respect to protected health information of an individual — (1) the individual shall have a right to obtain from such covered entity a copy of such information in an electronic format and, if the individual chooses, to direct the covered entity to transmit such copy directly to an entity or person designated by the individual, provided that any such choice is clear, conspicuous, and specific….". 42 USC 17935(3)(1).

[12] 86 Fed. Reg. 6446, at 6456-57 (Jan. 21, 2021).

[13] https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202504&RIN=0945-AA00.

Regardless of the outcome of the OCR final rule, **the state of the law today is that patients can use their HIPAA right of access to have their PHI, at least from an electronic health record, sent to the app of their choice**. OCR has endorsed this concept in guidance. For example:

> A written request meeting the required elements of a directed third-party request can be "**forwarded** to the covered entity by a third party on behalf and at the direction of the individual **(such as by an app being used by the individual)**."[14] (emphasis added)

> For example, a covered entity is not permitted to deny an individual's right of access to their ePHI where the individual directs the information to a third-party app because the app will share the individual's ePHI for research or because the app does not encrypt the individual's data when at rest.[15]

> [D]isagreement with the individual about the worthiness of the third party as a recipient of the PHI, or even concerns about what the third party might do with the PHI (except for express reasons listed in the Privacy Rule, such as in cases where life or physical safety is threatened), are not acceptable reasons to deny an individual's request.[16]

Similarly, guidance from the HHS Office of the National Coordinator (ONC) interpreting the Cures Act information blocking rules specifically endorse the right of patients to access their electronic health information using apps.

> The final rule supports an individual's ability to choose which third-party developer and app are best for receiving all or part of their EHI from a health care provider and to agree to clear and public terms of use on how that initial and ongoing engagement with the third-party developer and app occurs.[17]

> The rule supports patient access to their electronic medical record data. Patients will be able to use applications they authorize to receive data from their medical records.[18]

> Modern technology allows clinicians to easily provide patients with access to their information in a fully automated, low-cost manner. Patients will be able to access their health information from an app of their choice.[19]

The AHA claims 45 CFR 164.530(c) - general provisions in the Privacy Rule requiring covered entities to have "appropriate administrative, technical, and physical safeguards to protect the privacy" of PHI—would prevent them from responding directly with PHI to IAS requests from individuals conveyed through their apps via TEFCA. This claim is without merit. More than a decade ago, OCR made clear in guidance that individuals have the right to request their data using mechanisms that are convenient for them - i.e., obtaining their data

[14]https://www.hhs.gov/hipaa/for-professionals/faq/2033/when-do-the-hipaa-privacy-rule-limitations-on-fees/index.html.
[15]https://www.hhs.gov/hipaa/for-professionals/faq/3012/can-a-covered-entity-refuse-to-disclose-ephi.html.
[16]https://www.hhs.gov/hipaa/for-professionals/faq/2037/are-there-any-limits-or-exceptions-to-the-individuals-right/index.html
[17] The Final Information Blocking Rules, at 25815.
[18]https://web.archive.org/web/20200309144449/https://www.healthit.gov/curesrule/what-it-means-for-me/patients
[19]https://web.archive.org/web/20200309144500mp_/https://www.healthit.gov/curesrule/what-it-means-for-me/clinicians

in the form and format they request - even if complying with those requests might appear to be inconsistent with other provisions in HIPAA. For example, OCR has stated that if an individual requests their copy of PHI by unsecure means (regular e-mail, for example), the individual has the right to receive information in this way, even though the HIPAA Security Rule (as well as the Privacy Rule section cited by the AHA) would generally prohibit a covered entity from sending PHI unsecurely.[20] Individuals can request their PHI in the form and format that works best for them, as long as that form and format is "readily producible" by the covered entity. OCR has made clear in this same guidance that "readily producible" refers to the covered entity's technical capabilities, not willingness. If a hospital is connected to TEFCA for exchange of PHI for other purposes, that hospital has the technical capability to respond with payload to an IAS request submitted by a patient's chosen app.

The AHA also cites 45 CFR 164.514(h)(1) regarding their verification requirements to confirm the identity and authority of entities requesting PHI. There is an argument that the regulatory text of Section 164.514(h)(1) by its terms does not apply to right of access requests. Specifically, 45 CFR 164.514(h)(1) is required "[p]rior to any disclosure *permitted* by this subpart." (emphasis added), while disclosures pursuant to an individual right of access request are "required" under the Privacy Rule.[21] But given that transactions through TEFCA are all remote, we appreciate and support the need for identity proofing of the patient - but that identity proofing is taken care of by the app through a process that complies with NIST IAL and AAL level 2. An app, when querying TEFCA under any of the options in IAS SOP 3.0, must submit proof (through a token) that identity proofing of the patient was performed by an approved credential service provider. When OCR interpretive guidance has addressed verification of the identity of individuals requesting their health information, OCR has said the following:

> Under § 164.514(h) of the Privacy Rule, a covered entity is required to take reasonable steps to verify the identity of the individual making a request for access. The rule does not mandate any particular form of verification (such as obtaining a copy of a driver's license), but rather leaves the type and manner of the verification to the discretion and professional judgment of the covered entity. Further, covered entities may rely on industry standards in developing reasonable verification processes.[22]

The process outlined in the SOP is consistent with stakeholder consensus on this issue, and given OCR's flexibility in how identity proofing takes place, the claim by the AHA that the IAS SOP would contradict covered entity identity verification requirements in 164.514(h)(1) just doesn't hold water. Indeed, these verification standards have been foundational to TEFCA since ONC first published a draft framework in January 2018,[23] and reflect the National Coordinator's determination to implement TEFCA standards in collaboration with NIST standards, as required by the Cures Act.[24]

As for the authority of the app to request the information, the identity proofing process and manner by

---

[20] 78 Federal Register 5566 at 5634 (January 25, 2013); https://www.hhs.gov/hipaa/for-professionals/faq/2060/do-individuals-have-the-right-under-hipaa-to-have/index.html

[21] Compare 45 CFR 502(a)(1)(i) - disclosures to an individual, which are permitted by the Privacy Rule - and 45 CFR 502(a)(2)(i) - disclosures at the request of an individual under 45 CFR 164.524, which are required. That these disclosures are required is reinforced by 45 CFR 164.524(a)(1), which declares an individual's *right* (not permission) to access a copy of their PHI, except under the narrow exceptions.

[22] 79 Fed. Reg. 7290, at 7303 (Feb. 6, 2014).

[23] https://healthit.gov/wp-content/uploads/2018/01/draft-trusted-exchange-framework.pdf

[24] Section 4003(b) of the Cures Act, implementing Section 3001(c)(9) of the Public Health Services Act, 42 U.S.C. 300jj-11(c)(9).

which a secure identity token is shared demonstrate that the individual hired the app - and OCR has already stated in guidance that individual requests for access can be conveyed by the app.[25] Also see our discussion below about federal and state legal requirements on apps prohibiting the collection, use, disclosure or retention of health information without patient consent.

On another topic, we take issue with some of the rhetoric in the letter that just doesn't apply in the context of individual access through TEFCA. For example, AHA claims that proposals in the SOP would fail to comply with the aforementioned HIPAA provisions (which don't actually apply in the context of IAS) and therefore would "harm patient care by delaying delivery of care, impacting access to critical information for treating providers…."

It's hard to see how the prompt delivery to a patient's app of her requested data is going to delay medical care or prevent treating providers from getting the information they need. In fact, the opposite is true - users of consumer-facing applications frequently report in LinkedIn posts and elsewhere that their ability to access and use their health data from different sources in a non-HIPAA application has empowered them in their own health journey, in their efforts to navigate the health system, and even with conveying critical information to their treating providers. There is published evidence regarding the benefits of sharing notes with patients.[26]

While TEFCA is a voluntary network, the value of exchange is underscored by the volume of entities already exchanging (mostly for treatment purposes) on the network. It is hyperbolic at best to argue that allowing patients to access their data through TEFCA will undermine treatment exchange. In fact, one of the greatest threats of TEFCA is not individual access, but misuse of the treatment pathway. Exchange for individual access purposes is susceptible to less abuse because individuals are directly involved in making the request. Plus, the privacy regulation and enforcement frameworks that exist outside of HIPAA can and do hold individual access service providers accountable if they engage in unfair and deceptive practices and/or violate the FTC's Health Breach Notification Rule, applicable state consumer privacy laws, or voluntary standards like the CMS Interoperability Framework, which requires participating patient-facing apps to adopt the CARIN Code of Conduct and submit to independent validation of their compliance with CARIN Code of Conduct as a condition of participation.

The concerns about privacy and apps not being subject to HIPAA are ones we frequently hear. When we published the first CARIN Trust Framework and Code of Conduct in November 2018, there was only one state - California - with a comprehensive consumer privacy law. Even then, commercial personal health apps were (and still are) subject to FTC rules - for example, the prohibition on unfair and deceptive practices in the FTC Act, in addition to the Health Breach Notification Rule, which was amended and expanded in 2024.

The regulatory and enforcement landscape for protecting consumer privacy has matured significantly over the last eight years. FTC enforcement actions not only involve unsecured health information, but the unauthorized use and disclosure of health information. Also, since enactment of the path-breaking California Consumer Privacy Act, an additional 18 states have enacted robust health data privacy laws that layer on top of FTC requirements. By notable contrast, HIPAA covered entities enjoy exemptions from these laws and are not required by HIPAA to obtain express opt-in consent for many uses and disclosures of their PHI, or to

[25] https://www.hhs.gov/hipaa/for-professionals/faq/2033/when-do-the-hipaa-privacy-rule-limitations-on-fees/index.html.

[26] For example, see https://www.ama-assn.org/practice-management/digital-health/5-positives-sharing-clinical-notes-your-patients; https://www.opennotes.org/implementation/

honor a multitude of different consumer privacy rights so individuals can make meaningful choices involving their health data.

Indeed, an app from a non-HIPAA entity that "misrepresents consent for disclosure," is liable under federal and state law(s) and creates significant reputational risk for their business. Further, IASPs in TEFCA (like other participants and sub-participants) must agree contractually, through the Common Agreement flow-down provisions, to adhere to the HIPAA Privacy and Security rules - and this agreement can be enforced against apps by the FTC. Further, apps are voluntary for individuals to use, so apps have to earn and keep the trust of their users to remain viable. All of this is to say, apps have plenty of "incentive" - both from a business and legal risk perspective - to protect data and collect, use, and share it only with user authorization, as the meaning is understood under fair information practice principles, which guides the majority of sectoral and comprehensive consumer privacy regulatory frameworks.

AHA has asked that providers "not be held liable or obligated to undertake breach notification steps" if the providers are complying with the IAS process. While OCR already is on record with guidance stating that a provider is not responsible for what an app chosen by a patient does with PHI, we are sympathetic to concerns of providers and other covered-entities under the current enforcement climate.[27] With respect to further guidance on breach notification responsibilities, the CARIN Alliance is already on record asking OCR to clarify that a covered entity (or business associate operating on its behalf) can consider it to be a low probability of compromise when a wrong record is delivered to an app and the app intercepts it before it is seen by the wrong patient, particularly via TEFCA where apps are required to comply with HIPAA and there is enforcement (via FTC for non-HIPAA apps and via OCR for HIPAA covered entities).[28] We support additional OCR guidance underscoring the HHS-wide policy support for consumer access, including the use of consumer-facing applications, to give providers appropriate assurances when complying with their privacy and security responsibilities.

With regard to the AHA's concerns about the patient matching aspects of the IAS SOP 3.0, we agree the patient matching criteria need another look. However, our concerns are that these criteria, when tested by some of our members, have been shown to be ineffective in allowing sufficient true positive matches to be released. In our separate letter about SOP 3.0, we noted that the matching criteria advanced by the SOP do not consider the recommendations of CMS' draft Patient Matching and Response Proposal, which was developed through an open, multi-stakeholder effort.[29] Please see our prior letter for details, but we do not understand why this proposal was not advanced or even addressed in SOP 3.0. As a final note on patient matching, the concerns expressed by AHA that these match criteria, in the context of IAS, will increase risk

---

[27] https://www.hhs.gov/hipaa/for-professionals/faq/3009/does-a-hipaa-covered-entity-bear-liability.html. "Once health information is received from a covered entity, at the individual's direction, by an app that is neither a covered entity nor a business associate under HIPAA, the information is no longer subject to the protections of the HIPAA Rules. If the individual's app – chosen by an individual to receive the individual's requested ePHI – was not provided by or on behalf of the covered entity (and, thus, does not create, receive, transmit, or maintain ePHI on its behalf), the covered entity would not be liable under the HIPAA Rules for any subsequent use or disclosure of the requested ePHI received by the app. For example, the covered entity would have no HIPAA responsibilities or liability if such an app that the individual designated to receive their ePHI later experiences a breach."

[28] https://cdn.prod.website-files.com/66635361bd8176cd6413cb24/690d16750ce4bc9a27b90f59_CARIN_Wrong%20Record%20Scenario_09.24.2024.pdf.

[29] https://cdn.prod.website-files.com/66635361bd8176cd6413cb24/69fcbba13f30317544f50a89_CARIN_TEFCA%20IAS%20SOP%202026_v.2%20(002).pdf

for adverse events and result in "billing delays, duplicative testing, and claims denials," is another example of hyperbole, as those concerns do not arise with respect to sharing data with patient apps, which is the sole use case of SOP 3.0.

Finally, we agree with the AHA that it would be helpful for OCR to issue additional guidance (and regulatory clarification) to clarify some of these points. We know of individual providers, provider organizations and health plans inside and outside the CARIN community who strongly support the individual right of access and also would appreciate this guidance/clarification.

As set forth above, current law and policy support moving forward with 2a and 2b (arguably even more quickly than proposed). We are disappointed that, notwithstanding current law and policy priorities, we keep experiencing push back on efforts to assure patients can access their data using modern technologies of their choice and without undue barriers. While it may be helpful to move forward with additional guidance from OCR, it is not essential for moving forward with IAS on TEFCA.

We appreciate the ongoing work that the RCE and ONC have undertaken to advance access by individuals to their health information through TEFCA, as a floor for network-based exchange in ways that also advance the ONC's deregulatory agenda. We remain committed to supporting the RCE and ONC as they lift the entire ecosystem. We also support CMS in work to accelerate first-movers. The CARIN Alliance remains committed to collaborating with relevant stakeholders in advancing consumer choice, consumer privacy, and consumer access.

Sincerely,

Ryan Howells
Leavitt Partners
On behalf of the CARIN Alliance