November 10, 2026

Secretary Robert F. Kennedy, Jr
U.S. Department of Health & Human Services
200 Independence Avenue SW
Washington, DC 20201

RE: Concerns Regarding HIPAA Privacy Rule Finalization – APA Compliance, Logical Outgrowth, and Provider Verification of Patient-Authorized Applications

Dear Secretary Kennedy,

The undersigned organizations are writing to you with our concerns regarding the forthcoming final HIPAA Privacy Rule: Changes to Support Coordinated Care and Individual Engagement and Reduce Regulatory Burdens (RIN 0945-AA00). While we have requested an Executive Order (EO) 12866 meeting on November 2, 2026, we have yet to hear back from the Office of Information and Regulatory Affairs (OIRA) or the Office of Management and Budget (OMB). We appreciate and support the Department of Health and Human Services' (HHS) Office for Civil Rights (OCR) efforts to advance patient access to health technology and support the use of health IT to facilitate patient engagement. However, we urge you to carefully consider significant concerns being raised by healthcare providers regarding the potential addition of new provisions under consideration by the Administration that would restrict a provider's ability to confirm that a third-party application has been authorized by the patient to receive their protected health information (PHI).

We are also concerned that a final rule restricting provider's ability to confirm patient authorization could raise significant concerns under the Administrative Procedure Act (APA).[1] The January 2021 Notice of Proposed Rulemaking (86 FR 6446) sought to reduce unreasonable identity verification barriers to individuals exercising their HIPAA rights, including directing electronic copies of PHI to third parties. It proposed prohibiting unreasonable verification measures and provided examples of practices that could constitute unreasonable burdens. Importantly, the proposal expressly stated that it was not intended to prevent covered entities from taking reasonable measures to verify the identity and authority of the individual or entity making a request.

A final rule that categorically prohibits providers from confirming whether a patient has authorized a third-party application to receive PHI would represent a material departure from the proposed approach. Section 553 of the APA requires agencies to provide adequate notice of proposed regulatory requirements and a meaningful opportunity to provide public comment. [2] Under the logical growth doctrine, a final rule may differ from the proposal only when affected

[1] 5 U.S.C. § 553 and 5 U.S.C. § 706
[2] 5 U.S.C. §§ 553(b)(3), (c)

parties reasonable could have anticipated the final regulatory approach and had an opportunity to publicly comment on its implications.

Here, the 2021 NPRM expressly preserved covered entities' ability to employ reasonable verification measures, signaling that the proposed restrictions were intended to address unreasonable barriers rather than eliminate legitimate safeguards. The ability to confirm patient authorization is not synonymous with imposing unreasonable verification requirements. Rather, it is a reasonable safeguard that helps providers fulfill their obligations to protect sensitive health information while honoring a patient's right to direct its disclosure. A final rule categorically prohibiting providers from confirming patient authorization would effectively reverse that approach by restricting conduct that the NPRM expressly contemplated permitting. Although the NPRM solicited comments on unreasonable verification practices, it did not clearly notify affected parties that OCR might prohibit reasonable confirmation of patient authorization altogether. Consequently, providers would not have had a meaningful opportunity to evaluate and comment on the operational, legal, privacy, and security implications of such a prohibition. Notably, courts have recognized that a final rule may fail the logical outgrowth standard where an agency adopts a materially different regulatory interpretation that interested parties could not reasonably have anticipated from the proposal. [3]

These concerns are further compounded by any presumption that presentation of an IAL2 credential, standing alone, satisfies all verification necessary to effectuate an application-initiated request for PHI. Identity proofing, patient matching, and verification of authority are analytically and operationally distinct functions. Although an IAL2 credential may provide sufficient assurance as to the identity of the individual, it does not necessarily establish that the individual has been accurately matched to the appropriate medical record, nor does it establish the nature, scope, duration, or validity of the individual's authorization or direction permitting a third-party application to obtain the requested information. Treating IAL2 credentialing as sufficient for all verification purposes, while restricting providers' ability to confirm patient authorization, would introduce additional substantive limitations that were not clearly contemplated by the 2021 NPRM.

A recent EO 12866 stakeholder meeting further underscores the importance of preserving this distinction. During this meeting, representatives of the application community recommended that OCR provide additional examples of what constitutes unreasonable verification requirements. We agree that additional clarity and practical examples would be helpful to both providers and application developers. However, providing examples of unreasonable practices is fundamentally different from prohibiting providers from taking reasonable steps to confirm that a patient has authorized an application to receive their information. Stakeholder requests for additional guidance should not become the basis for imposing a new substantive restriction that was not contemplated in the original proposed rule.

We respectfully request that OCR:

1. **Preserve provider discretion** to take reasonable, risk-appropriate steps to confirm that a patient has authorized a third-party application to receive their PHI, including directly confirming that authorization with the patient when appropriate.
2. **Reject any final language** that categorically prohibits such confirmation or otherwise expands the 2021 proposal beyond its reasonably foreseeable scope.

---

[3] *See Long Island Care at Home, Ltd. v. Coke*, 551 U.S. 158, 174 (2007); *See also Environmental Integrity Project v. EPA*, 425 F.3d 992, 996 (D.C. Cir. 2005).

3. **Provide clear examples and guidance** distinguishing unreasonable verification barriers from legitimate provider safeguards necessary to protect patient privacy and prevent unauthorized disclosures.
4. **Pursue additional notice and comment** if OCR intends to establish requirements that materially depart from the 2021 NPRM, rather than attempting to implement those requirements through the final rule.

The goal of improving patient access and supporting innovation should not come at the expense of providers' ability to responsibly protect patient information. Providers should not be placed in the untenable position of choosing between facilitating patient-directed data sharing and exercising reasonable diligence to confirm that the disclosure is authorized.

We strongly urge the OCR to pursue additional notice-and-comment rulemaking, consistent with the APA, before advancing any policy that materially departs from the scope of the 2021 NPRM. Providers must have a meaningful opportunity to evaluate and comment on the operational, legal, privacy, and security implications of any new requirements. We welcome the opportunity to work with OCR to develop an approach that advances patient access and innovation without undermining providers' ability to fulfill their independent obligations to protect patient information.

However, insofar as the Administration moves forward with a policy that, in practical effect, prevents providers from reasonably confirming patient authorization and places them in the precarious position of facilitating disclosures without adequate assurance that the receiving application has been authorized by the patient, OCR must also address the resulting and foreseeable risks to providers. Such a policy could compel providers to facilitate disclosures that result in unintended privacy or security incidents, while leaving providers exposed to regulatory scrutiny for circumstances they may have had limited ability to prevent or control. It is neither reasonable nor equitable to impose new restrictions on providers' ability to exercise reasonable safeguards without establishing corresponding protections against the regulatory risks those restrictions create.

Accordingly, if the Administration proceeds with this policy, we urge OCR to:

1. **Establish explicit, meaningful enforcement protections for providers acting in good faith.** OCR should clearly articulate that covered entities (CEs) that comply with applicable patient-directed disclosure requirements and exercise reasonable diligence within the constraints of the policy will receive appropriate enforcement discretion when an otherwise compliant disclosure results in an unintended privacy or security incident. Providers should not face disproportionate enforcement exposure for downstream misuse, unauthorized access, or security incidents attributable to an application or recipient over which they have no reasonable control, provided the provider has met its own applicable HIPAA obligations. These protections should expressly distinguish a provider's good-faith facilitation of patient-directed disclosures from independent misconduct or noncompliance by the receiving application.
2. **Work with Congress to codify durable statutory protections for providers.** Agency guidance and enforcement discretion alone do not provide the certainty necessary for providers to manage long-term compliance and liability risks. We urge OCR to work with Congress to establish statutory protections for covered entities that act in good faith and comply with federal patient-directed disclosure requirements, including appropriate limitations on liability for unintended privacy or security incidents arising from disclosures made in compliance with those requirements. Such protections must be narrowly tailored

to provider conduct and must not create a safe harbor, immunity, or exemption from applicable legal obligations for applications or other recipients of PHI.

Providers support patient access, patient choice, and responsible innovation. However, those objectives cannot be achieved by shifting the burden of risk onto healthcare organizations while restricting their ability to take reasonable steps to protect patients and their information. If the Administration intends to change the rules governing patient-directed disclosures, it must also ensure that providers are not left holding the regulatory liability for risks they are no longer permitted to reasonably mitigate.

Finally, we urge you to ensure that the final rule remains within the scope of the original proposal, complies with the APA, and appropriately balances patient access, privacy, security, and provider responsibilities.

CHIME members are executives and senior healthcare IT leaders; thus, we are offering to continue to serve as a resource to you. They remain committed to leveraging technology to deliver high-quality care and to enabling interoperable and secure access to records across the care continuum. Should you have any questions or if we can be of assistance, please contact Chelsea Arnone, Senior Director, Federal Affairs at carnone@chimecentral.org. Thank you for your consideration.

Sincerely,

College of Healthcare Information Management Executives (CHIME)
AdventHealth
Baptist Health (Jacksonville, FL)
Bryan Health
Claiborne Memorial Medical Center
Cleveland Clinic
Fisher-Titus Medical Center
Fulton County Health Center
Genesis HealthCare System
Helio Health
MedStar Health
OrthoVirginia
RiverSpring Living
Sharp HealthCare
The University of Kansas Health System and Medical Center
Trinity Health
Trinity Rehabilitation Services
Wooster Community Hospital

cc:

Paula Stannard, Director, Office for Civil Rights (OCR)
Dr. Mehmet Oz, Administrator, Centers for Medicare and Medicaid Services (CMS)
Dr. Thomas Keane, National Coordinator for Health IT, Office of the National Coordinator for Health IT (ONC)