

Molly VandeVoort

Associate
208.383.3964
Boise, Billings
MSVandeVoort@hollandhart.com

HIPAA Privacy Rule: Faster Access, New Fee and Notice Rules

A 15-day access deadline, posted fee schedules, no more notice acknowledgments, and new rules for personal health apps and community referrals

Insight — November 18, 2026

On November 16, 2026, the U.S. Department of Health and Human Services Office for Civil Rights (OCR) issued a final rule revising the HIPAA Privacy Rule. The rule cuts the outer deadline for responding to an individual's request for records from 30 days to 15, makes portal and app access free, and requires covered entities that charge for copies to post a fee schedule. It eliminates the requirement that providers with a direct treatment relationship seek a patient's written acknowledgment of the Notice of Privacy Practices. It also limits the barriers providers may place in front of personal health applications, expressly permits disclosures to community-based organizations for care coordination, and gives existing business associate agreements a limited transition period. This alert addresses each change, notes what OCR declined to finalize and what health plans should consider, and closes with next steps for leadership.[1]

The rule is scheduled for publication in the Federal Register on November 19, 2026. If publication occurs as scheduled, the effective date will be January 18, 2027, and the compliance date will be July 17, 2027. After the compliance date, the new requirements are enforceable, and violations may be subject to civil monetary penalties, as with other HIPAA requirements. Providers should confirm both dates against the published rule.[2]

Records teams will have less time to complete access requests

A covered entity must act on an individual's access request as soon as possible and no later than 15 calendar days after receipt. The current outer limit is 30 days. One extension of up to 30 calendar days remains available when the entity cannot act within the initial period, but only if the entity gives the individual, within that initial period, a written statement of the reasons and a completion date. Acknowledging receipt is not enough—an entity that grants a request must both inform the individual and provide the access within that period.[3]

Providers should map every route by which requests arrive, including portals, APIs, clinic desks, and records vendors, and assign responsibility for recording receipt and escalating delays. Vendor processing targets should leave the provider time to cure an incomplete production or an improper denial. The rule also bars unreasonable identity-verification measures and request procedures that impede access, such as accepting

requests only through a patient portal. Providers nonetheless retain discretion to select verification measures appropriate to their operational environment and are not required to use the least burdensome method when doing so would not be realistic for their operations. Providers should review their request forms and identification requirements and document why each chosen measure is reasonable.[4]

The 15-day period is an outer limit, not a waiting period. Where another federal or state law requires a covered entity to provide access in fewer than 15 calendar days, the rule treats that shorter period as achievable, so the shorter deadline effectively becomes the HIPAA deadline as well. A discussion with the individual about the scope or format of a request does not extend the time to respond.[5]

Fees must match the revised access process

The rule separates access that must be free from copies for which a provider may charge. A covered entity may not charge when an individual inspects records or obtains electronic records through an internet-based method, which OCR describes as an automated process such as a patient portal or a personal health application connection. Copies that require workforce labor may carry a reasonable, cost-based fee limited to copying labor, supplies, postage, and an agreed summary or explanation, so an emailed PDF is not necessarily free merely because it is electronic.

The rule also supersedes OCR's 2016 guidance on calculating fees, including the $6.50 flat-fee option, so fee tables built on that guidance must be rebuilt. A covered entity that charges for copies must post a fee schedule on its website, if it has one, and make the schedule available at the point of service and on request. The schedule must identify every type of access the entity provides free of charge. Where the entity generally charges, the schedule must also list its standard fees, in each available form and format, for copies an individual obtains through the right of access or directs to a designated person and for copies disclosed under the individual's authorization.[6]

Records teams should distinguish among a patient's own access request, a patient's direction to send an electronic copy of EHR information to a designated person, and a disclosure under authorization. Each has different legal conditions, and a fee schedule or request form that treats them the same way may apply the wrong fee or process.[7]

Providers no longer need a written acknowledgment of the Notice of Privacy Practices

Health care providers with a direct treatment relationship will no longer have to make a good-faith effort to obtain a patient's written acknowledgment of receipt of the Notice of Privacy Practices. The duties to deliver and post the notice continue, and the notice itself must be revised, including its explanation of access rights and of the right to discuss the notice with a designated contact. Providers should revise the notice together with intake forms and staff instructions and should preserve their

separate treatment consents and disclosure authorizations.[8]

What providers can and cannot require of personal health apps

The rule adds definitions of “electronic health record” and “personal health application,” and it confirms that an individual may have a copy of electronic PHI in a designated record set sent to the personal health application of the individual's choice, where the covered entity can produce the information in that form and format. OCR treats a request to send records to a personal health app as the individual's own access request, not a direction to a third party. A separate right to direct a copy to a designated person is limited to electronic PHI in an EHR and a designated record set.[9]

The rule and its preamble also limit how providers may gatekeep apps. A provider may not require a business associate agreement from a patient's app before disclosing the patient's information, because OCR treats that demand as an unreasonable measure. A provider may not prevent a patient's app from registering with an API that the provider makes public unless registration would pose an unacceptable level of risk to its electronic PHI, as informed by its Security Rule risk analysis, and it may not block an app because the app competes with a service the provider offers. Security teams should therefore document app-vetting criteria and keep the risk analysis supporting any app they restrict.[10]

Verification of app requests remains the hardest operational issue. In the preamble, rather than the regulation text, HHS identifies two scenarios in which it would be unreasonable for a provider to refuse an app's access request. The first is a request made through TEFCA to a provider that participates in TEFCA. The second is a request that comes through a CMS Aligned Network in which the provider participates, from a personal health application in the Medicare App Library. In either scenario, the request must carry a cryptographically signed token from a credential service provider certified to IAL2 and AAL2 under NIST SP 800-63, and the token's demographics must match the provider's records.[11] Until credential service providers are certified to SP 800-63-4, providers may rely on certification under SP 800-63-3.[12] Providers should align their identity-proofing, patient-matching, and authorization-confirmation steps with these examples and with their network participation.[13]

For requests to direct a copy to a designated person, the preamble encourages covered entities to contact the individual if they have questions or concerns about the request, including the authority of the designated person. The final rule does not create a safe harbor for erroneous disclosures.[14]

OCR did not finalize the proposal to require providers to accept oral requests to direct PHI to a third party. A request must be clear, conspicuous, and specific, and providers may require it in writing, including by email. A provider may, but need not, accept a verbal request that meets that standard. Intake tools and portal forms should be configured to capture a compliant request without adding barriers the rule prohibits.[15]

Community referrals are permitted, but minimum necessary still applies

New § 164.506(c)(6) expressly permits disclosures to social services agencies, community-based organizations, home- and community-based services providers, and similar recipients that provide health or human services to specific individuals. The disclosure must be for individual-level care coordination and case management activities for that individual, whether those activities are treatment or health care operations. The provision can support referrals for services such as nutrition or housing assistance, but it does not authorize unrestricted sharing of a patient's chart. OCR retained the existing minimum-necessary framework, including its application to treatment disclosures to recipients who are not health care providers.[16]

A referral procedure should identify the recipient's role, the information the recipient needs, and any consent requirement that applies. HIPAA's preemption provisions preserve qualifying state requirements that are more protective, and substance use disorder records subject to 42 C.F.R. Part 2 must be analyzed separately under that regulation. A community organization that acts independently for the patient does not automatically become a business associate, but an organization that performs functions on the provider's behalf is a business associate, and an agreement must be in place before the disclosure.[17]

Existing business associate agreements get a limited transition period

The rule provides a limited transition for business associate agreements that were in place before the rule's publication and are not renewed or modified between the effective date and the compliance date. The transition also applies to agreements between business associates and their subcontractors. Eligibility must be evaluated agreement by agreement. A qualifying agreement is deemed compliant until the earlier of its renewal or modification on or after the compliance date or January 18, 2028. The transition does not postpone the covered entity's access obligations for records held by a business associate.[18]

What OCR did not finalize

Several proposals from 2021 are not in the final rule. OCR retained the 30-day extension rather than adopting the proposed 15-day extension. It did not finalize a broad exception to the minimum-necessary standard, the proposed good-faith and foreseeable-threat changes, or individualized fee estimates and itemized statements. It also left unaddressed the proposed limits on fees for an individual's direction to send electronic EHR information to another person, stating that it will continue to monitor those fees, so providers should review directed-copy fees separately from fees for a patient's own access request.[19]

What payors should note

The access changes apply to health plans as covered entities. A plan must

meet the same 15-day deadline, fee limits, and fee-schedule posting requirement for requests from its members, and it must revise its privacy notice. The rule also revises the definition of health care operations to confirm that it covers care coordination and case management by health plans, whether individual-level or population-based. OCR did not finalize the proposed minimum-necessary exception for those activities, so a plan's requests to providers for care coordination and case management remain subject to the minimum-necessary standard.[20]

Next steps for leadership

The privacy officer should coordinate a single implementation plan with health information management, clinical operations, IT, and the records vendor. That plan should include the following steps.

1. Update request routing and escalation so that every request is recorded on receipt and completed within 15 calendar days.
2. Document the designated record sets, the electronic health records subject to directed-copy requests, and the offices responsible for handling requests.
3. Rebuild fee tables, including vendor tables based on the 2016 flat-fee guidance, and reconcile actual charges with the published fee schedule.
4. Revise the Notice of Privacy Practices and intake forms together.
5. Test community referral procedures against the minimum-necessary standard and business associate requirements.
6. Obtain written confirmation of vendor readiness and test representative requests before the compliance date.
7. Inventory API and app-access controls, remove any requirement that apps sign business associate agreements, and document risk assessments supporting any app restriction.

This alert reflects the public inspection version of the final rule as of November 17, 2026. Citations will be updated when the rule is published in the Federal Register.

---

[1] HIPAA Privacy Rule: Changes to Support Coordinated Care and Individual Engagement and Reduce Regulatory Burdens, FR Doc. 2026-23429 (scheduled for publication Nov. 19, 2026) (Final Rule); Press Release, U.S. Dep't of Health & Hum. Servs., HHS Issues New Final Rule to Modernize the HIPAA Privacy Rule to Support Coordinated Care and Individual Engagement and Reduce Regulatory Burdens (Nov. 16, 2026).

[2] Final Rule (Dates; § I.C); HHS Office for Civil Rights, Fact Sheet, HIPAA Privacy Rule: Changes to Support Coordinated Care and Individual Engagement and Reduce Regulatory Burdens Final Rule (Nov. 16, 2026) (HHS Fact Sheet); see generally 45 C.F.R. pt. 160, subpt. D.

[3] 45 C.F.R. § 164.524(b)(2) (as amended by the Final Rule); HHS Fact

Sheet.

[4] 45 C.F.R. §§ 164.514(h)(2)(v), 164.524(b)(1)(iii) (as amended); Final Rule § IV.B (identity verification); HHS Fact Sheet.

[5] 45 C.F.R. § 164.524(b)(2)(iii), (c)(3) (as amended).

[6] 45 C.F.R. §§ 164.524(c)(4), 164.525 (as amended); Final Rule § IV.A.7 (superseding the 2016 fee guidance).

[7] 45 C.F.R. § 164.524(c)(3), (d) (as amended); HHS Fact Sheet.

[8] 45 C.F.R. § 164.520(b)(1), (c)(2) (as amended); HHS Fact Sheet.

[9] 45 C.F.R. §§ 164.501 (definitions of "electronic health record" and "personal health application"), 164.524(c)(3), (c)(4)(ii)(B), (d) (as amended); Final Rule § IV.A.6; HHS Fact Sheet.

[10] Final Rule § IV.B (examples of unreasonable measures); 45 C.F.R. §§ 164.308(a)(1), 164.524(b)(1)(iii).

[11] Final Rule § IV.B.4 (preamble discussion of TEFCA and CMS Aligned Networks requests); see also 45 C.F.R. § 164.514(h)(1).

[12] Final Rule § IV.B.4 n.585.

[13] Final Rule § IV.B (identity verification).

[14] Final Rule § IV.B (identity verification), § IV.A.6 (right of access to direct).

[15] 45 C.F.R. § 164.524(d)(5)(i) (as amended); Final Rule § IV.A.6.

[16] 45 C.F.R. § 164.506(c)(6) (as added); Final Rule § IV.E; HHS Fact Sheet.

[17] 45 C.F.R. §§ 160.202, 160.203, 164.502(e); 42 C.F.R. pt. 2; Final Rule § IV.E.

[18] 45 C.F.R. § 164.532(e) (as amended); Final Rule § IV.J; HHS Fact Sheet.

[19] Final Rule §§ IV.A.4, IV.A.7, IV.A.8, IV.D, IV.F.

[20] 45 C.F.R. §§ 164.501, 164.520, 164.524, 164.525 (as amended); Final Rule §§ IV.C, IV.D; HHS Fact Sheet.

Subscribe to get our Insights delivered to your inbox.

This publication is designed to provide general information on pertinent legal topics. The statements made are provided for educational purposes

only. They do not constitute legal or financial advice nor do they necessarily reflect the views of Holland & Hart LLP or any of its attorneys other than the author(s). This publication is not intended to create an attorney-client relationship between you and Holland & Hart LLP. Substantive changes in the law subsequent to the date of this publication might affect the analysis or commentary. Similarly, the analysis may differ depending on the jurisdiction or circumstances. If you have specific questions as to the application of the law to your activities, you should seek the advice of your legal counsel.