Shumaker

NOVEMBER 23, 2026 | PUBLICATION

Client Alert: United States Department of Health and Human Services Finalizes Major HIPAA Privacy Rule Overhaul: What Health Care Businesses Need to Do Before Mid-2027

INDUSTRY SECTOR

Health Care
Technology

SERVICE LINE

Data Privacy
Health Law
Technology

RELATED PROFESSIONALS

C. Jade Davis
Mark Lehman

MEDIA CONTACT

Wendy M. Byrne
wbyrne@shumaker.com

On November 16, 2026, the United States Department of Health and Human Services (HHS) Office for Civil Rights (OCR) announced a final rule that rewrites key parts of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule. The rule cuts the deadline to respond to patient record requests from 30 days to 15, requires covered entities to send records to patient-chosen health apps, limits what may be charged for copies and requires posted fee schedules, restricts identity-verification practices that impede access, broadens care-coordination disclosures, and eliminates the signed Notice of Privacy Practices acknowledgment. The rule was published in the *Federal Register* on November 19, 2026. HIPAA Privacy Rule: Changes to Support Coordinated Care and Individual Engagement and Reduce Regulatory Burdens, 91 Fed. Reg. 74,848 (Nov. 19, 2026) (to be codified at 45 C.F.R. pts. 160, 164). The published rule states that it

takes effect on January 19, 2027, and that most requirements must be met by July 19, 2027. *Id.* at 74,848.

For business owners, the cost of this rule is operational: records-request workflows, patient-facing technology, fee schedules, and patient notices all must change by July 19, 2027. For in-house counsel, the work is policy and contract driven: updating HIPAA policies and the Notice of Privacy Practices, amending business associate agreements and release-of-information vendor contracts, and monitoring likely legal challenges to the rule. Organizations that start now have about eight months to finish. Those that wait until the January 19, 2027 effective date will have six.

A note on terminology: Although this rule has been described as a "security" update, it amends the HIPAA Privacy Rule (45 C.F.R. pt. 160 and pt. 164, subpts. A, E). It does not change the HIPAA Security Rule, which governs technical, physical and administrative safeguards for electronic protected health information (PHI). HHS proposed separate Security Rule amendments in 2025, and that rulemaking remains pending. See HIPAA Security Rule To Strengthen the Cybersecurity of Electronic Protected Health Information, 90 Fed. Reg. 898 (proposed Jan. 6, 2025) (to be codified at 45 C.F.R. pts. 160, 164). Organizations should track the two efforts separately.

Who Is Affected

The rule applies to HIPAA "regulated entities": covered entities (health plans, health care clearinghouses, and health care providers that conduct standard electronic transactions) and their business associates. If your business is a medical or dental practice, hospital, clinic, laboratory, pharmacy, health plan, or a vendor that handles PHI for one of these entities (billing, IT, cloud hosting, Electronic Health Record (EHR), practice management), the rule affects you. Several changes also reach business associates directly, including the business associate agreement provisions discussed below.

Key Dates

Milestone	Rule Text	Date
Federal Register publication	Published at 91 Fed. Reg. 74,848	November 19, 2026
Effective date	60 days after publication	January 19, 2027
Compliance date	180 days after the January 19, 2027 effective date	July 19, 2027
Business associate agreements	Additional transition period under revised 45 C.F.R. § 164.532(e) for qualifying agreements	Until the earlier of renewal or modification on or after July 19, 2027, or January 18, 2028, for qualifying agreements

Dates are as stated in the published rule. 91 Fed. Reg. at 74,848.

What Changes: The Individual Right of Access

1. **Faster response deadline: 15 days, not 30**

Covered entities must act on an access request as soon as practicable, and no later than 15 calendar days after receiving it. 91 Fed. Reg. at 74,965 (to be codified at 45 C.F.R. § 164.524(b)(2)(i)). That is half the current 30-day period. One extension of up to 30 calendar days remains available. For most practices, this is the most demanding operational change in the rule. Records-request workflows and staffing should be built around the 15-day deadline, and release-of-information vendor contracts should require turnaround times short enough for the covered entity to meet it.

2. **New definitions: "electronic health record" and "personal health application"**

For the first time, the Privacy Rule defines "electronic health record" and "personal health application" (personal health app). 91 Fed. Reg. at 74,877, 74,884–85 (to be codified at 45 C.F.R. § 164.501). A personal health app is an application an individual uses to access their own health information, including information drawn from multiple sources, and the information must be managed, shared, and controlled by or primarily for the individual, and not by or primarily for a covered entity or primarily for another person. HHS finalized the definition with modifications for clarity and readability and declined to limit it to apps that meet particular privacy and security standards. *Id.* at 74,884–85.

3. **Delivery through personal health apps**

The right of access now expressly includes the right to obtain a copy of electronic PHI through a personal health app when the covered entity can produce the PHI in that form and format. In practice, a provider that can transmit records to a qualifying app the patient chooses must do so. It may not be refused because the app is not covered by HIPAA. Once PHI reaches an app the individual controls, the covered entity's HIPAA responsibility for that copy generally ends. Even so, providers should document the request and the transmission carefully.

4. **Right to direct electronic copies to a third party**

Consistent with the D.C. federal court's 2020 decision in *Ciox Health, LLC v. Azar*, 435 F. Supp. 3d 30 (D.D.C. 2020), the right to direct a covered entity to send PHI to a designated third party is limited to electronic copies of PHI in an electronic health record. 91 Fed. Reg. at 74,877. Paper records and PHI held outside an electronic health record fall outside this directed-access right. They remain subject to the individual's own right of access.

5. **Summaries in lieu of copies**

A covered entity that offers a summary instead of a copy must now tell the individual that they keep the right to obtain the copy itself, or to direct an electronic copy to another person.

6. **Fees: free access in some cases, plus website posting**

The rule revises permissible access fees. Three points matter most in practice. First, a covered entity may not charge any fee when an individual inspects their own PHI or accesses electronic PHI maintained by or on behalf of the covered entity using an internet-based method, such as a personal health app or patient portal. 91 Fed. Reg. at 74,966 (to be codified at 45 C.F.R. § 164.524(c)(4)(ii)).

Second, where a fee is permitted, it must be a reasonable, cost-based fee that includes only the cost of labor for copying (paper or electronic), supplies for creating a non-electronic copy, postage when a non-electronic copy or a summary or explanation is mailed, and labor to prepare an agreed-upon summary or explanation. *Id.* (to be codified at 45 C.F.R. § 164.524(c)(4)(i)). Covered entities therefore may not charge individuals for

electronic media (such as a CD or USB drive) or postage when providing electronic copies; only labor may be charged for those copies. *Id.* at 74,902–04. The final rule also supersedes the 2016 access guidance's three fee-calculation methods (actual costs, average costs, or a $6.50 flat fee). *Id.* at 74,903, 74,905–06. HHS did not address fees for electronic copies directed to a third party under the right of access to direct. *Id.* at 74,904, 74,906.

Third, covered entities that charge for copies must post a fee schedule on their websites, if they have one, and make it available at the point of service and upon request. The schedule must list all types of access available free of charge and the standard fees for copies provided under the right of access (45 C.F.R. § 164.524(a)), the right of access to direct (§ 164.524(d)), and a valid authorization (§ 164.508). *Id.* at 74,908–10; *id.* at 74,966–69 (to be codified at 45 C.F.R. § 164.525). HHS did not finalize the proposals to require individualized fee estimates or itemized statements. *Id.* at 74,908–10. Practices that rely on per-page schedules or the $6.50 flat fee should review them now.

7. **Limits on identity verification**

Covered entities may not impose unreasonable identity-verification measures that impede access. One example is requiring an in-person visit when a remote verification method is available. Industry groups argued that relaxed verification creates fraud and misdirection risks, especially in confirming that a third-party app is authorized by the patient. HHS finalized the provision anyway. The practical result is a balancing act between OCR's access enforcement and the organization's own breach and impersonation exposure. Remote verification procedures should be reasonable, documented, and consistently applied, and staff should know when and how to escalate a suspicious request.

What Changes: Care Coordination

- **Health plans:** The definition of health care operations is amended to clarify that health plans may use and disclose PHI for population-based and individual-focused care coordination and case management.
- **Third-party social services:** Covered entities may expressly disclose PHI for individual-level care coordination and case management to social services agencies, community-based organizations, home and community-based services (HCBS) providers, and similar third parties that provide health-related services. 91 Fed. Reg. 74,848, pt. IV.E (to be codified at 45 C.F.R. § 164.506(c)(6)).

These are permissions, not mandates. The final rule does not create an exception to the minimum necessary standard, and the minimum necessary standard continues to apply where it applied before. 91 Fed. Reg. 74,848, pt. IV.D. HHS also did not finalize its proposed changes to the professional judgment and good-faith standards for disclosures involving substance use disorder, serious mental illness, and emergencies. *Id.* at 74,925–26. Businesses that want to use them should update policies and train staff on the new pathways, while still observing more protective state laws and 42 C.F.R. pt. 2 where it applies.

What Changes: Reduced Administrative Burden

- **No more signed Notice of Privacy Practices (NPP) acknowledgment:** Covered health care providers with direct treatment relationships no longer need to make a good-faith effort to obtain a written acknowledgment that the patient received the NPP. HHS identifies this as the largest source of the rule's projected savings.
- **Revised NPP content:** NPPs must be updated to explain individuals' rights and how to exercise them, including a new right to discuss the notice with a designated contact person or office. The prior exception that excluded inmates of correctional institutions from receiving an NPP is removed.

- **Telecommunications Relay Services (TRS):** Disclosures to TRS communications assistants for individuals who are deaf, hard of hearing, or deaf-blind, or who have a speech disability, are expressly permitted. TRS providers are excluded from the business associate definition, so no business associate agreement is required with them.
- **Uniformed Services:** The Armed Forces mission-readiness permission now covers all Uniformed Services, including the U.S. Public Health Service and National Oceanic & Atmospheric Administration Department of Commerce (NOAA) Commissioned Corps.

Business Associate Agreements

HHS recognized that 240 days may not be enough to implement the substantive changes and renegotiate business associate agreements. The rule therefore revises 45 C.F.R. § 164.532(e) to give qualifying business associate agreements a transition period beyond the compliance date. 91 Fed. Reg. at 74,936. An agreement qualifies only if, before November 19, 2026, the covered entity (or a business associate, as to a subcontractor) had entered into and was operating under a written contract or other written arrangement that complied with the HIPAA Rules then in effect, and the agreement is not renewed or modified from January 19, 2027, until July 19, 2027. *Id.* (to be codified at 45 C.F.R. § 164.532(e)(1)). A qualifying agreement is deemed compliant until the earlier of (1) the date it is renewed or modified on or after July 19, 2027, or (2) January 18, 2028. *Id.* (to be codified at 45 C.F.R. § 164.532(e)(2)). The transition period covers only the agreement's terms. A business associate that responds to access requests on behalf of a covered entity must meet the 15-calendar-day deadline by the July 19, 2027 compliance date, whether or not its business associate agreement has been amended. *Id.* at 74,936. Even so, business associates are directly subject to several provisions, including the revised rules on required disclosures of PHI by business associates. Covered entities and their vendors should inventory agreements now. They should identify which agreements qualify for the transition period and which need earlier amendment to address the 15-day access deadline, app-based delivery, and fee terms.

Costs and Litigation Risk

Press reports put HHS's estimate at roughly $784 million in first-year implementation costs, offset by approximately $703 million in annual net savings in years two through five. Businesses should confirm these figures against the rule's Regulatory Impact Analysis before relying on them for budgeting. HHS also included a detailed severability statement. It addresses particular provisions individually. For example, it states that the right of access to direct does not depend on the new electronic health record definition, that individuals would retain the right to request copies through a personal health app even if that definition were invalidated, that the existing fee provisions would remain intact if the new fee prohibitions were invalidated, and that all existing right of access provisions would remain in effect if new 45 C.F.R. § 164.525 were invalidated. *Id.* at 74,854–55. Given recent litigation over HIPAA rulemaking, including the 2025 Northern District of Texas decision in *Purl v. U.S. Department of Health & Human Services*, 787 F. Supp. 3d 284 (N.D. Tex. 2025), vacating most of the 2024 reproductive health Privacy Rule amendments, legal challenges are a realistic possibility. A pending challenge is a reason to monitor, not to delay. The severability statement means that a court ruling against one provision likely leaves the rest in force, and the compliance work described above takes months. Unless a court enjoins the rule, businesses should plan to comply on schedule.

Action Checklist for Business Owners and In-House Counsel

1. Map your records-request process end to end and re-engineer it to meet a 15-calendar-day deadline, including vendor service levels.
2. Assess your technical ability to deliver ePHI to personal health apps and adopt a written procedure for

app-based requests.
3. Revise your access fee schedule, identify no-charge scenarios, and prepare the required website posting of estimated fees for access and authorization requests, and make the schedule available at the point of service and upon request.
4. Update identity-verification procedures to offer reasonable remote options and remove in-person-only requirements.
5. Redraft your NPP to meet the new content requirements, and retire the signed-acknowledgment workflow.
6. Update policies and training on care-coordination disclosures to social services and community-based organizations. Confirm that policies continue to apply the minimum necessary standard, which the final rule does not change.
7. Inventory business associate agreements, determine transition-period eligibility, and schedule amendments before the January 18, 2028 outside date.
8. Track the separate, still-pending HIPAA Security Rule rulemaking, and do not assume this rule changes your security obligations.
9. Calendar January 19, 2027 (effective date) and July 19, 2027 (compliance date), as stated in the published rule, 91 Fed. Reg. at 74,848.

This article is for general informational purposes only and is not legal advice. For questions about how the final rule affects your organization, contact a member of the Shumaker Technology, Data Privacy Cybersecurity & AI Service Line.

© 2026 Shumaker, Loop & Kendrick, LLP. All Rights Reserved. Privacy Policy/Disclaimer

Shumaker