Now & Next
Healthcare Alert

November 20, 2026

HHS finalizes HIPAA Privacy Rule changes

By Valerie Breslin Montague, Rebecca Simone, Laurie T. Cohen, Jéna M. Grady, Meredith D. LaMaster, Grace Connelly, and Epiphany Ramirez[i]

New access, fee, and care coordination rules are reshaping requirements for providers and health plans. Here's what organizations need to know.

What's the impact?

- Covered entities must satisfy access requests for protected health information (PHI) maintained in a designated record set within a shortened 15 calendar day timeline.
- Policies, procedures, and business associate agreements (BAAs) should be reviewed and updated as needed, with workforce trainings on the changes.
- OCR clarifies that PHI may be disclosed without authorization to social services agencies, community organizations, home and community-based services (HCBS) providers, and similar third parties for individual-level care coordination and case management.

On November 16, the US Department of Health and Human Services (HHS) Office for Civil Rights (OCR) announced a final rule, "HIPAA Privacy Rule: Changes to Support Coordinated Care and

This newsletter is intended as an information source for the clients and friends of Nixon Peabody LLP. The content should not be construed as legal advice, and readers should not act upon information in the publication without professional counsel. This material may be considered advertising under certain rules of professional conduct. Copyright © 2026 Nixon Peabody LLP. All rights reserved.

Individual Engagement and Reduce Regulatory Burdens" (Final Rule), to modify the Standards for Privacy of Individually Identifiable Health Information (Privacy Rule) under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act. Published in the *Federal Register* on November 19, it finalizes many of the proposals in OCR's January 2021 Notice of Proposed Rulemaking.

The Final Rule shortens the timeframe in which a HIPAA-covered entity is required to respond to access requests for PHI, limits fees that may be charged for the provision of access, revises notice of privacy practices (NPP) requirements, and clarifies when PHI may be shared to coordinate care. Most of the changes impact healthcare providers and health plans, with contract and workflow updated requirements for some of their business associates. To comply with the Final Rule, HIPAA-regulated entities may need to amend policies, fee schedules, NPPs, BAAs, and workforce member training.

Who is affected

- Healthcare providers that are HIPAA covered entities, including hospitals, skilled nursing facilities, physician practices, pharmacies, and laboratories, which bear most of the right of access, fee, and NPP changes.
- Health plans, which receive clearer authority for care coordination and case management and must update NPPs.
- Business associates, including electronic health record (EHR) vendors and vendors charged with satisfying medical record requests, whose agreements and access workflows may need updating.
- Third parties, such as social services agencies, community-based organizations, HCBS providers, and personal health app developers, which may face fewer obstacles receiving PHI without an individual's authorization for care coordination and case management activities (except to the extent limited by other appliable law).

Key changes at a glance

- **Access to records timeframe:** Covered entities must provide individuals with copies of their PHI maintained within a designated record set within 15 calendar days of receiving the request, or as soon as practicable, shortened from 30 calendar days. The allowance for a one-time, 30-day extension remains.
- **Form and format of PHI**: Covered entities must provide individuals with access to their PHI in the electronic form and format requested, including through a personal health app, if readily producible.

- **Fees**: Fees for responding to access requests are limited to labor for copying the PHI (electronic or non-electronic form), supplies for creating a non-electronic copy, postage when the individual requests that the non-electronic copy, summary, or explanation is mailed, and labor for preparing an agreed summary or explanation of records. Covered entities are not permitted to charge a fee for in-person inspection or access via a portal or app. OCR did not add a limit on fees charged to access requests directing PHI to a third party, stating that it will continue to monitor fees charged in such circumstances.
- **Right of access to direct**: Individuals have the right to direct a covered entity to send an electronic copy of their PHI to a designated person; however, the right is limited to electronic copies of PHI in an EHR.
- **Notice of privacy practices:** Providers with direct treatment relationships are no longer required to seek written acknowledgment of receipt of the NPP from individuals. NPP content requirements are revised, including a new right to discuss the NPP with a designated person or office. The inmate exception to receiving an NPP is removed.
- **Care coordination**: The definition of "healthcare operations" was clarified to cover both individual-level and population-based care coordination and case management. Further, OCR clarifies that covered entities are permitted to disclose PHI for individual-level care coordination and case management to certain third parties, including social service agencies, community-based organizations, and HCBS providers, without authorization. These disclosures remain subject to the minimum necessary standard, where applicable.
- **Identity verification:** Covered entities may not impose verification measures that impede an individual's rights under the HIPAA Privacy Rule when a less burdensome measure is practicable.
- **Disclosures to Telecommunications Relay Services (TRS) communications assistants**: Disclosures to TRS communications assistants are permitted. TRS providers are excluded from the business associate definition.
- **Not finalized:** OCR declined to adopt the proposed exception to the minimum necessary standard for individual-level care coordination, the proposed "good faith" standard for disclosures to family and caregivers (including for individuals with substance use disorder or serious mental illness), the proposed "serious and reasonably foreseeable" threat standard, the expanded right to inspect, mandatory acceptance of oral requests to direct access, and individualized fee estimates and itemized statements. OCR also did not address fees for access requests directed to a third party.

Key dates

The Final Rule takes effect 60 days after publication, on January 19, 2027 (effective date). HIPAA-regulated entities must come into compliance within 240 days of publication, by July 19, 2027 (compliance date).

The Final Rule provides a transition period for existing BAAs. An agreement that complied with the current HIPAA regulations and is not renewed or modified between the effective date and the compliance date is deemed to be compliant until the earlier of two dates: (1) when it is renewed or modified on or after the compliance date or (2) January 18, 2028. BAAs with automatic renewal provisions are deemed compliant if they automatically renew between the effective date and compliance date but must come into compliance by January 18, 2028.

Business associates must comply with the other requirements in the Final Rule by the compliance date even if their BAA qualifies for the transition period.

Action items for HIPAA-regulated entities

Among other steps required to implement the Final Rule, covered entities and business associates should consider the following:

/ Review right-of-access procedures

The updated 15-day timeframe to respond to an access request begins upon receipt of the individual's request to access PHI maintained in a designated record set. Time spent verifying an individual's identity, seeking clarification about the request, or directing the request to another department or business associate counts against the 15-day clock. Extension notices must go out within the first 15 days, and shorter deadlines under other applicable federal or state laws still apply. Any right of access procedures, including intake, tracking, and escalation steps, that are designed around a 30-day deadline may not be feasible in a shortened 15-day period.

Covered entities should revise their access policy and procedures to address this new timeframe, as well as the Final Rule's modifications to the form and format and the right to direct access. They should also coordinate with IT and EHR vendors on the production of electronic PHI (ePHI) through personal health apps, consistent with information blocking obligations, as compliance with the HIPAA timeframe for access requests does not alleviate the risk of information blocking enforcement if a covered entity's practice delays access.

/ Conform access fees

Fees calculated under OCR's 2016 guidance, including the $6.50 flat fee, must be recalculated using the permitted cost categories under the Final Rule. Charges for in-person inspection or portal and app access are not permitted. Entities that charge fees for access to copies of records must post a fee schedule on their website (if they have one) and make it available at the point of

service and on request. Fees for access are limited to the cost of labor for copying the PHI, regardless as to whether it is in electronic or non-electronic form; supplies for non-electronic copies; the actual cost of postage and shipping for mailing non-electronic copies, summaries, or explanations; and the cost of labor to prepare an agreed summary or explanation.

/ Revise NPP and related procedures

Covered entities will need to update their NPPs to be consistent with the Final Rule, including by designating a person or office who can discuss the NPP with individuals and listing that contact's email address, changing "Medical" to "Health" in the required header, and describing how individuals can obtain records at limited cost or free of charge. Direct treatment providers can eliminate the process of securing written acknowledgments of receipt of the NPP.

/ Review identity verification policies and request forms

Where remote options are practicable, requirements such as notarization or in-person verification are the kind of identity verification measures prohibited by the Final Rule. Further, requests for access cannot be limited to a single channel, such as paper, in person, or via patient portal, when another method is practicable, and a request form cannot demand the information required in a full HIPAA authorization. Covered entities may still require written requests, but an email, portal message, or personal health app transmission can satisfy that requirement. Because verification time counts against the 15-day deadline for right of access, an overly restrictive verification policy may cause a delayed response to an access request.

/ Inventory and amend business associate agreements

BAAs with vendors that handle access requests may need to be updated to reflect the shorter deadline and fee limits. A BAA that complied with the HIPAA regulations prior to the Final Rule's publication date keeps its compliant status until January 18, 2028, only if it is not renewed or modified between the effective date and compliance date. If a BAA is renewed or modified between those dates, it must be brought into full compliance.

/ Review care coordination policies

The Final Rule's new express permission may allow disclosures to community-based organizations and similar third parties that HIPAA-regulated entities previously may have handled through patient authorizations. OCR did not adopt the minimum necessary exception mentioned in the proposed rule, so these disclosures remain subject to the minimum necessary standard, Part 2, and more stringent state laws.

/ Train workforce members

Workforce members receive access requests, quote fees, verify identities, and distribute NPPs, so revised policies are only effective if workforce members are properly trained on the changes.

Nixon Peabody's Healthcare team helps providers, health plans, and business associates navigate HIPAA requirements and translate regulatory developments into practical compliance

measures. For more information on the content of this alert, please contact your Nixon Peabody attorney or:

Valerie Breslin Montague
312.977.4485
vbmontague@nixonpeabody.com

Rebecca Simone
516.832.7524
rsimone@nixonpeabody.com

Laurie T. Cohen
518.427.2708
lauriecohen@nixonpeabody.com

Jéna M. Grady
212.940.3114
jgrady@nixonpeabody.com

Meredith D. LaMaster
312.977.9257
mlamaster@nixonpeabody.com

Grace Connelly
312.977.9292
gconnelly@nixonpeabody.com

---

[i] Epiphany Ramirez, a law clerk in Nixon Peabody's Healthcare Group, assisted with the preparation of this alert.