HHS FINALIZES HIPAA PRIVACY RULE CHANGES: WHAT EVERY HEALTHCARE ORGANIZATION NEEDS TO KNOW

Date: 19 November 2026

US Policy and Regulatory Alert

By: Jay E. Mitchell, Kevin L. Alonso, Nora E. Becerra, Sarah L. Carlins

On 16 November 2026, the US Department of Health and Human Services (HHS) Office for Civil Rights (OCR) finalized significant amendments to the HIPAA Privacy Rule. Key changes focus on strengthening individuals' rights to access their protected health information (PHI), including electronic PHI through personal health apps; improving information sharing for care coordination and case management; and reducing regulatory and administrative burdens on covered entities.

The final rule also reflects a broader shift in how HHS is adapting HIPAA to a healthcare environment in which individuals increasingly expect their health information to move electronically, including through applications and services that may sit outside the traditional HIPAA ecosystem. This shift has important practical implications for health systems, health plans, and digital health companies.

KEY DATES

- *Effective Date*: 18 January 2027 (60 days after the planned 19 November 2026 publication in the Federal Register).
- *Compliance Date*: 17 July 2027 (240 days after Federal Register publication).
- *Business Associate Agreements (BAAs)*: 18 January 2028, at the latest. Existing BAAs that are not renewed or modified before the compliance date are deemed compliant until they are renewed or modified, subject to the final rule's transition provisions.

WHAT THE FINAL RULE CHANGES

The final rule amends the HIPAA Privacy Rule in three principal areas:

1. Expands the Individual Right of Access

Response Time

Cuts the deadline for acting on a request for copies of PHI from 30 to 15 calendar days, with one 30-day extension if the individual is notified in writing within the first 15 days. Shorter deadlines under other state or federal law still apply.

©2005-2026 K&L Gates LLP. All Rights Reserved.

Personal Health Apps

Confirms that an individual may obtain electronic PHI through a personal health application, newly defined in the rule, when the covered entity can produce it in that form and format. The rule also defines “electronic health record” (EHR).

Access Fees

Revises permissible access fees, specifies when copies of PHI must be free, and requires advance notice of fees.

Transmission To Third Parties

Implements the individual's right to direct a covered entity to send an electronic copy of PHI in an EHR to a designated person, a right limited by Ciox Health, LLC v. Azar to electronic copies of PHI maintained in an EHR.

Identity Verification

Bars identity verification steps that impose unnecessary effort or expense on individuals exercising their access rights.

2. Supports Individual-Level Care Coordination

Health Plans

Confirms that health plans may use and disclose PHI for care coordination and case management for specific individuals, not only populations.

Community and Social Services Partners

Expressly permits disclosures to social services agencies, community-based organizations, and similar third parties for individual-level care coordination and case management.

Limits

The final rule leaves intact applicable requirements under 42 C.F.R. Part 2 and more protective state consent laws.

3. Lightens Administrative Requirements

Notice Acknowledgments

Eliminates the good-faith effort to obtain written acknowledgment of receipt of the Notice of Privacy Practices. Providers must still furnish and post the notice.

Telecommunications Relay Services

Permits disclosures to Telecommunications Relay Services (TRS) providers and communications assistants for individuals who are deaf, hard of hearing, deaf-blind, or who have a speech disability, and excludes TRS providers from the definition of business associate.

Uniformed Services

Extends the armed forces command-authority disclosure permission to US Public Health Service and NOAA Commissioned Corps personnel for mission readiness.

©2005-2026 K&L Gates LLP. All Rights Reserved.

WHAT THE FINAL RULE SIGNALS

Comparing the final rule with OCR's January 2021 proposed rule offers insight into OCR's priorities and how it is likely to approach compliance and enforcement:

Patient Access Is Not Negotiable

The 15-day response time, app-based access, free electronic access, and limits on burdensome identity verification survived largely intact. OCR gave ground only on the mechanics of compliance, most notably by keeping the 30-day extension it had proposed to cut to 15 days. Covered entities should expect enforcement to focus on whether patients actually get their records, in the format requested, on time.

OCR Expanded Patient Control, Not Provider Discretion

OCR dropped proposals that would have given covered entities more latitude to disclose PHI on their own judgment, including a minimum necessary exception for health plan care coordination, a “good-faith” standard for disclosures to family members and caregivers, and a lower threshold for disclosures to avert a threat. Information is meant to move at the patient's direction, not the provider's.

The Burden Relief Is Modest

The deregulatory framing rests largely on limited relief, such as eliminating notice acknowledgments, while the heavier lift in access workflows, fee practices, and app connectivity falls on providers, health plans, and their vendors.

Identity Verification Is the Issue to Watch

Shortly before issuance, health systems urged HHS to preserve their ability to confirm that a patient actually authorized an app to receive records. How the final standard and preamble address that concern will shape app-based access in practice and may be where providers and digital health companies feel the rule most directly.

IMPLICATIONS FOR DIGITAL HEALTH

The rule is particularly significant for organizations in the digital health space. By expressly addressing an individual's ability to obtain electronic PHI through a personal health application when the covered entity can provide the information in the requested form and format, HHS is underscoring the reality that health information no longer moves only from one HIPAA-regulated provider to another. Patients increasingly interact with health information through portals, applications, Application Programming Interfaces, remote-monitoring platforms, connected devices, and other consumer-facing technologies, and not every company receiving health information is a HIPAA business associate.

That distinction is important because HIPAA applicability does not turn solely on whether an organization handles health information. As such, the useful compliance question is not simply, “Is this health information?” Instead, it is: Who is receiving the information, on whose behalf do they act, why is it being transmitted, and what happens to it after the transfer? That analysis has become increasingly important as the boundaries between traditional healthcare technology and consumer health technology have blurred.

©2005-2026 K&L Gates LLP. All Rights Reserved.

WHAT THIS MEANS FOR COVERED ENTITIES

The new rule is straightforward from a requirements standpoint. The more complex question covered organizations will need to wrestle with is what it will take to comply operationally and how the rule implicitly reshapes the analysis around digital health.

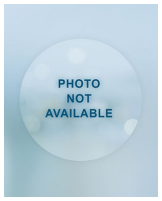
For example, reducing the access period from 30 days to 15 days sounds like a straightforward compliance change. However, a medical record request often crosses several systems and business functions—it may begin with health information management, involve identity verification, require retrieval from an EHR or another clinical system, and depend on a third-party records vendor before the information reaches the patient. Because existing processes were designed around a 30-day requirement, simply updating the policy may not result in operational compliance. In addition to updating their policies, organizations may also need to reexamine their access process and their data governance and ecosystem.

Most organizations will update their access policies before the July 2027 compliance date. Fewer will test whether the people, systems, and vendors behind those policies can actually deliver records in 15 days, or decide in advance how they will respond when a patient asks to send a full record to an unfamiliar app. Those gaps are where the rule is most likely to generate patient complaints and, in time, OCR scrutiny, and closing them depends on each organization's own data flows, vendor relationships, and contracts. Organizations that address these questions now will be far better positioned than those that discover the gaps with a request already on the clock.

ABOUT THE FIRM

The firm's healthcare practice routinely assists health systems, hospitals, and other providers, pharmaceutical manufacturers, and digital health and healthcare-adjacent companies with legal advice and strategic considerations, including providing advice on compliance with HIPAA and other state and federal privacy and data security laws. Please contact a member of our Healthcare and FDA practice group if you have questions about the final rule or how the new requirements may affect your business.

KEY CONTACTS



JAY E. MITCHELL
PARTNER

WASHINGTON, DC, CHICAGO
+1.202.661.3703
JAY.MITCHELL@KLGATES.COM



KEVIN L. ALONSO
PARTNER

NASHVILLE
+1.615.514.1847
KEVIN.ALONSO@KLGATES.COM



NORA E. BECERRA
PARTNER

CHICAGO
+1.312.807.4222
NORA.BECERRA@KLGATES.COM



SARAH L. CARLINS
OF COUNSEL

PITTSBURGH
+1.412.355.6548
SARAH.CARLINS@KLGATES.COM

©2005-2026 K&L Gates LLP. All Rights Reserved.

This publication/newsletter is for informational purposes and does not contain or convey legal advice. The information herein should not be used or relied upon in regard to any particular facts or circumstances without first consulting a lawyer. Any views expressed herein are those of the author(s) and not necessarily those of the law firm's clients.

©2005-2026 K&L Gates LLP. All Rights Reserved.