# HIM Briefings

## Updated NPPs raise new compliance and documentation challenges

*by Dom Nicastro*

HHS recently released updated model notices of privacy practices (NPP), introducing changes that go well beyond revising standard privacy notice templates. The recent update includes revisions to the healthcare provider and health plan NPPs, as well as the Part 2 patient notice.

The revised guidance clarifies patient rights, expands disclosures related to sensitive health information, and aligns privacy notice requirements with recent regulatory updates involving reproductive health information and substance use disorder (SUD) records.

For HIM leaders, the changes could trigger reviews of multiple operational processes tied to patient access, documentation governance, complaint management, and release-of-information workflows. Although the model language issued by federal regulators is recommended rather than universally mandatory, organizations that continue using outdated notices may face increased compliance exposure if their privacy disclosures no longer reflect current regulatory requirements.

**Richard F. Cahill, JD,** vice president and associate general counsel for The Doctors Company, says the revisions represent a broad update to how organizations communicate patient rights and privacy protections.

“The new provisions took effect on February 16, 2026, and introduce significant updates to existing templates,” he says. “The changes address patient documentation practices, complaint processes for alleged violations, operational compliance requirements, and enhanced protections for reproductive health data.”

Because the updated guidance does not include standardized implementation language for covered entities to adopt verbatim, healthcare organizations must develop their own revisions to ensure notices reflect the new regulatory expectations. At healthcare organizations, that responsibility often falls across multiple departments, including HIM, compliance, privacy, and legal teams.

**Understanding what changed**

The NPP has long served as a foundational document explaining how healthcare organizations collect, use, and disclose protected health information (PHI). Patients receive the notice during initial visits or enrollment, and organizations must maintain public access to the document through websites and other channels.

Under the revised guidance, the notice must more clearly explain patient rights, complaint procedures, and the circumstances under which PHI may be disclosed. The changes also strengthen language related to sensitive information such as reproductive health data and SUD treatment records.

“The regulations are intended to improve patient understanding of their legal rights and enhance the healthcare experience,” Cahill says.

Covered entities must ensure that notices are written in clear language and made available to patients when requested. Organizations must also post their notices online and provide them during a patient’s first interaction with the provider. For health plans, notices must be distributed when an individual first becomes a subscriber and again every three years.

In addition to describing how organizations use and protect health information, the revised notices must outline security measures applied to certain sensitive records and clarify restrictions on how those records may be used in legal proceedings.

“These regulations are sweeping and require careful evaluation by healthcare organizations to determine their scope and applicability,” says Cahill.

**Operational implications for HIM**

Although privacy notices are often drafted by legal or compliance teams, the operational implications frequently fall under HIM departments. These teams are responsible for many of the processes described in privacy notices, including responding to access requests, managing documentation corrections, and maintaining records of disclosures.

If operational processes differ from what is described in the notice, organizations could face compliance concerns

during regulatory investigations. Cahill says organizations should approach the new requirements carefully and evaluate how the updated guidance applies to their existing systems and policies.

“Providers in both rural and urban settings are encouraged to consult legal counsel to ensure compliance and avoid potential penalties or unintended consequences as the rules are implemented across the industry in the coming months and years,” he says.

As part of the compliance process, healthcare organizations may also need to review how their privacy notices interact with broader regulatory obligations. Cahill notes that regulatory compliance may allow combined notices that incorporate multiple privacy disclosures into a single document.

“Internal protocols supporting compliance should reflect applicable community standards,” he says. “They should be reviewed and updated periodically as regulations evolve.”

**Sensitive data protections**

One of the most significant elements of the updated notice guidance involves protections for sensitive categories of patient data.

Recent HIPAA Privacy Rule updates introduced additional safeguards for reproductive health information, and the revised notices incorporate language explaining these protections.

Organizations must now ensure their privacy notices clearly describe how certain sensitive information is protected and under what circumstances it may be disclosed.

Another major area of change involves SUD records governed by the federal confidentiality regulations under 42 *CFR* Part 2.

**Christopher Maniscalco, Esq.,** an associate attorney in Frier Levitt’s Healthcare & Life Sciences departments, says aligning privacy notices with these confidentiality rules represents one of the most substantial changes in the new guidance.

“The most significant change is that, where a Part 2 program is involved, the NPP must be aligned with the requirements of the 42 *CFR* Part 2 final rule governing the confidentiality of SUD patient records,” he says.

Under the revised framework, privacy notices must explain how SUD records may be used or disclosed for treatment, payment, and healthcare operations, while still complying with confidentiality protections.

Required updates include expanded explanations of patient rights related to consent, disclosure restrictions, and the ability to revoke previously granted permissions.

Patients must also be informed that their records generally cannot be used in civil, criminal, administrative, or legislative proceedings without written consent or a court order.

“These are not cosmetic edits,” says Maniscalco. “They reflect a fundamental restructuring of how notices of privacy practices pertaining to SUD records are communicated to patients.”

**Compliance and enforcement risks**

Healthcare organizations that delay updating their notices may face increased regulatory scrutiny if their privacy disclosures fail to reflect current rules.

“Organizations that delay updating their NPP face a relatively straightforward enforcement risk because these updates are clearly required regulatory changes,” says Maniscalco.

Although the existence of an outdated notice alone may not trigger enforcement, the risk increases significantly if a privacy complaint or breach investigation occurs.

“In particular, entities subject to SUD confidentiality requirements under 42 *CFR* Part 2, as well as updated HIPAA Privacy Rule provisions, may face scrutiny if their NPP does not accurately reflect current patient rights and permitted disclosures,” says Maniscalco.

If an outdated notice contributes to improper disclosures or patient complaints, regulators may interpret the failure to update as evidence of broader compliance gaps.

Oversight and enforcement of privacy notice requirements generally falls under the HHS Office for Civil Rights (OCR), though other agencies may become involved depending on the nature of the violation.

Cahill notes that regulatory investigations can take time and may involve multiple stages of review.

“The OCR generally follows a multistep investigative process that includes complaint intake, evidence gathering, policy review, analysis of allegations, issuance of a report, implementation of corrective actions, and ongoing oversight until resolution,” he says.

Such investigations may last up to 18 months, and outcomes can include corrective action plans, financial penalties, or other sanctions depending on the severity of the violation.

**Preparing for implementation**

Because the rule was finalized in 2024 and took effect in early 2026, regulators may expect organizations to begin implementing changes soon, if they haven’t already. Maniscalco says healthcare facilities should prioritize revising their privacy notices to reduce compliance risk.

In practice, updating the notice will likely involve reviewing existing policies, drafting revised language, coordinating legal review, and aligning operational workflows with the new disclosures.

Determining ownership of the update process is another important step.

“HIM, compliance, and privacy departments will ultimately be responsible for implementing the updates,” says Maniscalco.

However, he notes that legal oversight remains essential.

“Having legal oversee the NPP revision process helps ensure that the covered entity’s changes are properly analyzed, drafted, and aligned with applicable legal and regulatory requirements,” he says.