

MEDICARE COMPLIANCE

Weekly News and Compliance Strategies on Federal Regulations,
Enforcement Actions and Audits

Contents

Page 3

OCR's Model Notice for
Part 2 Patients

Page 5

Exclusions, Vendors, AI:
Mitigation Tips for Top 10
Compliance Risks

Page 7

New MOON Is Out; One
QIO Pushed Back on a
Different Expired Notice

Page 7

CMS Transmittals and
Federal Register Regulations,
Feb. 13-19, 2026

Page 8

News Briefs

OCR Said It's Coming After Part 2 Violations As SUD Patient Confidentiality Rule Takes Effect

Fifty years after HHS's first version of the Confidentiality of Substance Use Disorder (SUD) Patient Records regulation (42 C.F.R. Part 2), enforcement is coming to town. The HHS Office for Civil Rights (OCR) on Feb. 13 announced a "new program to implement and enforce statutory and regulatory requirements that protect" Part 2 records and opened a portal for complaints—an apparent attempt to communicate that without enforcement, regulations are just words on paper.¹

The enforcement announcement coincides with the Feb. 16 compliance date for the latest amendments to Part 2.²

Until now, the U.S. Department of Justice (DOJ) was responsible for enforcing Part 2 as a crime but no cases were ever brought. Now its civil enforcement rests with the HIPAA police. "If there's no consequence, then it's not high on anybody's compliance radar," said attorney Robert Trusiak, with Trusiak Law.

'Treat Part 2 as HIPAA-Plus'

OCR's enforcement role seems to fit with the Part 2 rule because it harmonizes more now with HIPAA and the Health Information Technology for Economic and Clinical Health Act. The Part 2 rule, which was finalized in 2024, allows a one-time consent form that mirrors HIPAA's and redisclosure of Part 2 records. It also builds a fortress around so-called SUD counseling notes and prohibits the release of Part 2 records to law enforcement without patient consent or a court order and subpoena.

"Treat Part 2 as HIPAA-plus," Trusiak said. "The operational model resembles HIPAA, but enhanced protections remain."

Part 2 programs are now subject to the breach notification obligations of HIPAA and its penalties. Between breach notification and the complaint portals, complaints about potential violations may fall in OCR's lap and unleash penalties on covered entities (CEs). "OCR investigations conducted under the new program may be resolved through a range of civil enforcement mechanisms," OCR said. "These include OCR entering into resolution agreements, securing monetary settlements, obtaining commitments for corrective action, or imposing civil money penalties for the failure to comply."

OCR Posts New, Revised Notices

OCR has also posted the first-ever Part 2 model notice for patients (see box, p. 3)³ and updated its HIPAA Notice of Privacy Practices (NPP) with new SUD language.⁴ CE's are required to add a statement to their NPPs that they will comply with state laws that are stricter than HIPAA, said attorney Jennifer Pike, with Alston & Bird. NPPs also must now include a statement that protected health information (PHI) disclosed pursuant to the HIPAA Privacy Rule may be redisclosed and lose its HIPAA protection. "This is generally meant to cover the disclosures of PHI a covered entity might make under 45 C.F.R. 164.512," Pike said. "We're used to seeing that in the HIPAA authorization, but it should be in the NPP as well."

One example: a CE shares PHI in response to a request for an organ



Managing Editor

Nina Youngstrom
nina.youngstrom@hcca-info.org

Copy Editor

Jack Hittinger
jack.hittinger@hcca-info.org

and tissue donation from an organ procurement organization. “The organ procurement organization isn’t subject to HIPAA, and so the PHI that has been shared is no longer protected by HIPAA,” Pike said.

OCR also started accepting complaints Feb. 16 about potential Part 2 violations and breaches in its portal.⁵

‘We Will See Them Acting Pretty Quickly’

Pike anticipates OCR enforcement actions in short order. “We will see them act pretty quickly if and when they receive a complaint or notice of a breach,” she said. “It’s a good opportunity to have fresh eyes on your policies and procedures.”

But there’s some question about whether OCR will be able to put its money where its mouth is. “OCR staff has dropped considerably,” said attorney Dori Cain, with Faegre Drinker Biddle & Reath. The Part 2 enforcement announcement reminds her of the September 2025 HHS alert on the high priority of information blocking enforcement.⁶ “We have not seen anything on information blocking” since, Cain noted.

That doesn’t change the fact that Part 2 now has a parallel complaint and penalty structure to HIPAA. “The dynamic has changed here,” Trusiak said. “The fact that Part 2 complaints can flow into OCR the way HIPAA complaints flow into OCR means they will be on somebody’s desk.” If they’re on someone’s desk, he assumes enforcement will follow.

Report on Medicare Compliance (ISSN: 1094-3307) is published 45 times a year by the Health Care Compliance Association, 6462 City West Parkway, Eden Prairie, MN 55344. 888.580.8373, hcca-info.org.

Copyright © 2026 by the Society of Corporate Compliance and Ethics & Health Care Compliance Association. All rights reserved. On an occasional basis, it is okay to copy, fax or email an article from *RMC*. Unless you have HCCA’s permission, it violates federal law to make copies of, fax or email an entire issue; share your subscriber password; or post newsletter content on any website or network. To obtain permission to transmit, make copies or post stories from *RMC* at no charge, please contact customer service at 888.580.8373 or service@hcca-info.org. Contact Paule Hocker at paule.hocker@corporatecompliance.org or 888.580.8373 if you’d like to review our reasonable rates for bulk or site licenses that will permit weekly redistributions of entire issues.

Report on Medicare Compliance is published with the understanding that the publisher is not engaged in rendering legal, accounting or other professional services. If legal advice or other expert assistance is required, the services of a competent professional person should be sought.

Subscriptions to *RMC* include free electronic delivery in addition to the print copy.

To order an annual subscription to **Report on Medicare Compliance** (\$665 for HCCA members; \$895 for nonmembers), call 888.580.8373 (major credit cards accepted) or order online at hcca-info.org.

Subscribers to this newsletter can receive 20 nonlive Continuing Education Units (CEUs) per year toward certification by the Compliance Certification Board (CCB). Contact CCB at 888.580.8373.

‘This Helps Them Think About It in a HIPAA Way’

Aligning Part 2 with HIPAA should make compliance easier for Part 2 providers, Cain said. “This helps them think about it in a HIPAA way.” Part 2 records can, for the most part, be treated as PHI, she said.

The final Part 2 rule for the first time allows patients in SUD programs to sign one consent form that allows all future disclosures for treatment, payment and operations (TPO), similar to HIPAA’s authorization. Patients also have the right to say no to the broader consent in favor of a limited consent that only lets Part 2 providers disclose SUD information to a specific health plan, for example. “It allows that alignment so covered entities aren’t operating under two separate workflows,” Cain said.

There are limits: Even if the patient signs a consent for all future uses of TPO, the rule requires the Part 2 program to get a separate consent from the patient before their SUD records may be used in a civil, criminal or administrative proceeding against them unless there’s a court order and a subpoena. It’s the biggest difference with HIPAA, Cain said.

Part 2 also lifts the prohibition on redisclosures of patient information. “A patient may now provide a single written consent permitting future disclosures for TPO, and that consent may allow downstream HIPAA-covered entities and business associates to redisclose consistent with HIPAA,” Trusiak said. When that happens, Part 2 providers must include the consent with the SUD data, along with a disclaimer saying, “You can’t use this for any other purpose,” Pike noted.

The rule offers extra protection for SUD counseling notes, which are analogous to psychotherapy notes under HIPAA. SUD counseling notes must be “separated from the rest of the part 2 and/or medical record” and “afforded additional privacy protection,” according to the rule. Pike recommends keeping counseling notes separate from other records because “in almost all circumstances, you will need a special consent for disclosing counseling notes.”

Does Part 2 Apply to You?

Trusiak cautions organizations not to fall into the trap of thinking they don’t have Part 2 risk because they have no behavioral health care. “Part 2 risk isn’t limited to behavioral health departments,” he said. An acute-care hospital, emergency department (ED) and a primary care or specialty practice “may touch Part 2 data” through ED consults, toxicology screens, overdose follow-ups, referrals for medication-assisted treatment, discharge planning, care coordination, case management and outside records from community

continued on p. 5

OCR's Model Notice for Part 2 Patients

The HHS Office for Civil Rights (OCR) posted this model notice for use by Part 2 programs, which must comply with the Confidentiality of Substance Use Disorder Patient Records regulation effective Feb. 16, 2026. OCR on Feb. 13 announced a “new program to implement and enforce statutory and regulatory requirements that protect” Part 2 records and opened a portal for complaints, and posted this notice and an updated HIPAA Notice of Privacy Practices (see story, p. 1).¹

Your Information. Your Rights. Our Responsibilities.

Notice of Privacy Practices of [Name of Part 2 Program]

This notice describes:

- HOW HEALTH INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED
- YOUR RIGHTS WITH RESPECT TO YOUR HEALTH INFORMATION
- HOW TO FILE A COMPLAINT CONCERNING A VIOLATION OF THE PRIVACY OR SECURITY OF YOUR HEALTH INFORMATION, OR OF YOUR RIGHTS CONCERNING YOUR INFORMATION

YOU HAVE A RIGHT TO A COPY OF THIS NOTICE (IN PAPER OR ELECTRONIC FORM) AND TO DISCUSS IT WITH [ENTER NAME OR TITLE] AT [PHONE AND EMAIL] IF YOU HAVE ANY QUESTIONS.

In this notice, your health information means your substance use disorder patient record.

Your Rights

You have the right to:

- Consent to most uses and disclosures of your health information
- Ask us to limit the information we share
- Get a copy of this privacy notice
- Discuss this notice with someone in our program
- Get a list of those with whom we've shared your electronic records²
- Get a list of health care providers who have received your information through certain third parties
- Choose in advance whether to receive fundraising communications
- File a complaint if you believe your privacy rights have been violated

Your Choices

- With your consent, we can use and share your information as we:
- Treat you
- Run our organization
- Bill for our services
- Fulfill your requests to share information with your consent
- Prevent multiple program enrollments
- Report about court-referred treatment
- Report to prescription drug monitoring programs

Our Uses and Disclosures

We may use and share your information without your consent as we:

- Communicate within our program and with our contractors
- Help with medical emergencies
- Help with public health
- Report crimes (and threats of crimes) on our premises and suspected child abuse and neglect
- Aid scientific research
- Respond to audits and evaluations of our program
- Assist cause of death inquiries
- Respond to court orders
- In all these circumstances, we must protect your information and limit how we use and share it.

Your Rights

When it comes to your health information, you have certain rights.

This section explains your rights and some of our responsibilities to help you.

Provide consent when we use or share your information for most purposes

- You may provide a single consent for all future uses or disclosures for treatment, payment, and health care operations purposes.

- [SUGGESTED OPTIONAL LANGUAGE: You may provide consent for more limited purposes (for example, to only disclose information to another health care provider for your treatment); however, doing so may affect the services we can provide you or how you pay for services.]
- [SUGGESTED OPTIONAL LANGUAGE: You may provide a general consent to share your information through certain third parties, such as a health information network or a research institution, where your treating health care providers can access it.]

Ask us to limit what we use or share

- You can ask us not to use or share certain health information for treatment, payment, or our health care operations after you have provided consent for all those purposes. We are not required to agree to your request, and we may say “no” if, for example, it could affect your care. If we agree to your request, we may still share this information in the event that you need emergency treatment.
- If you pay for a service or health care item out-of-pocket in full, you can ask us not to share that information for the purpose of payment or our health care operations with your health insurer. We will say “yes” unless a law requires us to share that information.

Get a copy of this privacy notice

You can ask for a paper copy of this notice at any time, even if you have agreed to receive the notice electronically. We will provide you with a paper copy promptly.

Discuss this notice with someone in our program

You can ask questions or obtain more information about this notice and our privacy practices by calling or emailing the contact person at the top of this notice.

Choose in advance about fundraising

You have the right to a clear and obvious notice in advance of, and a choice about whether to receive, fundraising communications for our program.

File a complaint if you feel your rights are violated

- You can complain if you feel we have violated your rights by contacting us using the information on page 1.
- You can file a complaint with the U.S. Department of Health and Human Services' Office for Civil Rights by sending a letter to 200 Independence Avenue, S.W., Washington, D.C. 20201, calling 1-877-696-6775, or visiting <https://www.hhs.gov/hipaa/filing-a-complaint/index.html>.
- We will not retaliate against you for filing a complaint.

Your Choices

How do we typically use or share your health information?

With your consent, we typically use or share your health information in the following ways.

Treat you

We can use your health information and share it with other professionals who are treating you.

Example: A doctor treating you for a chronic condition asks a doctor at our program about your health condition and medications you are taking, for example, to avoid complications.

Run our organization

We can use and share your health information to run our program, improve your care, and contact you when necessary.

Example: We use health information about you to manage your treatment and services.

Bill for your services

We can use and share your health information to bill and get payment from health plans or other entities.

Example: We give information about you to your health insurance plan so it will pay for your services.

With your consent, we may also use and share your information in the following ways:

- To whomever you name in a consent to share your information
- To prevent multiple enrollments in withdrawal management or maintenance treatment programs
- To report participation in treatment required by the criminal justice system
- To report prescribed substance use disorder treatment medications to a state prescription drug monitoring program when required by law

You can choose someone to act for you.

If someone has authority to act as your personal representative, such as if someone has your medical power of attorney or if someone is your legal guardian, that person can exercise your rights and make choices about your health information.

We will make sure the person has this authority and can act for you before we take any action.

Our Uses and Disclosures

How else can we use or share your health information?

We are allowed or required to share your information in certain ways without your consent – usually in ways that contribute to the public good, such as public health and research. We have to meet many conditions in the law before we can share your information for these purposes.

To communicate within our program and with contractors

We can share your information within our program, with an organization that has administrative control over our program, and with contractors who help us run our program.

For medical emergencies

We can share your information during a bona fide medical emergency with the personnel and health care providers responding to your emergency, even when you are unable to consent because of the emergency.

We can also share your identifying information to assist the federal Food and Drug Administration in notifying you or your doctor about unsafe products you may be using.

Help with public health

We can share health information that does not identify you for certain situations such as:

- Preventing disease
- Reporting adverse reactions to medications

Aid scientific research

We can use or share your information to conduct or help with health research. Researchers cannot include any patient identifying information in their reports about the research.

Respond to management and financial audits and program evaluations

We can use or share your information to improve the quality of our services, obtain needed credentials, and cooperate with oversight agencies for activities authorized by law, as long as those who view or receive the information agree to destroy or return the information when they are finished and agree not to use it against you.

Assist with cause of death inquiries

We can share patient identifying information about a deceased patient as required or allowed by laws that collect information relating to cause of death.

Report suspected child abuse and neglect

We will only report the information required by law.

Prevent or reduce crime in our program

We may report to law enforcement when a patient commits or threatens to commit a crime within our program or against our staff.

Redisclosure According to HIPAA

When you consent to uses and disclosures for all future treatment and payment purposes and to run our business, we may share your information with other substance use disorder treatment programs, doctors' offices, and health care businesses for those activities. If the person who receives it is subject to HIPAA, then they are allowed to use and share your information again without your consent for the purposes that HIPAA allows. Your information still cannot be used in legal proceedings against you unless (1) you consent or (2) based on a Part 2 court order and a subpoena (or similar legal requirement).

Legal Proceedings and Court Orders

We must follow certain procedures before using or sharing your information for investigations and legal proceedings.

- We will not use or share your information or provide testimony about your information in any civil, administrative, criminal, or legislative proceedings against you without your written consent or a court order.
- We will only respond to a court order to use or share your health information if it is accompanied by a subpoena or other similar legal mandate requiring us to comply.
- We will only use or share your information in proceedings against you based on a court order after we have received notice and an opportunity to be heard or you tell us that you have received notice.
- We may use or share your information to respond to legal proceedings against our program based on a court order and you may not be notified in advance. You have the right to seek to overturn or change the court order after you learn about it.

Our Responsibilities

- We are required to obtain your consent for most uses and sharing of your information.
- We are required by law to maintain the privacy and security of your information.
- We must let you know promptly if a breach occurs that may have compromised the privacy or security of your information.
- We must follow the duties and privacy practices described in this notice and give you a copy of it.
- We will not use or share your information other than as described in this notice unless you tell us we can in writing. If you tell us we can, you may change your mind at any time. Let us know in writing if you change your mind.

Changes to the Terms of this Notice

We are required to follow the terms of this notice that are currently in effect. We can change the terms of this notice, and the changes will apply to all information we have about you. The new notice will be available upon request in our office and on our web site.

Effective Date

This notice is effective as of [insert effective date of this notice].

Other Instructions for Notice

- Insert name or title of the privacy contact and his/her email address and phone number.
- Insert any special notes that apply to your entity's practices such as, "We will provide you with a summary of your treatment history upon request."
- Part 2 requires you to describe any state or other laws that require greater limits on disclosures. For example, "The information we can share about you for treatment is limited to admission forms, treatment/discharge forms, and discharge summaries." Insert this type of information here. If no laws with greater limits apply to your entity, no information needs to be added.

Endnotes

- 1 Nina Youngstrom, "OCR Said It's Coming After Part 2 Violations As SUD Confidentiality Rule Takes Effect," *Report on Medicare Compliance* 35, no. 7 (February 23, 2026).
- 2 The compliance date for this requirement will be set when the same right is revised in the HIPAA Privacy Rule.

continued from p. 2

SUD programs, outpatient treatment programs, detox programs or residential facilities.

Part 2 applies if an entity receives federal funding and creates, maintains, receives or transmits information that could qualify as a Part 2 record, Trusiak said. In other words, the medical records identify the person as having a SUD—such as a treatment note stating that the patient is diagnosed with an opioid use disorder—and were created or maintained by a SUD program that receives federal money. But Part 2 isn't triggered simply because an ED note mentions a patient's intoxication if there's no SUD program at that hospital. Pike added that when a SUD program rediscloses records to the patient's internist, that doesn't turn the internist into a Part 2 provider.

"The protected thing is often not a lab value or diagnosis code standing alone," Trusiak explained. It's the link between the identification of the patient; the SUD diagnosis, treatment or referral information; and federal funds.

Tips for Compliance Oversight

Part 2 should make its way onto the internal work plan, Trusiak said. "The greatest hazard a compliance officer has is you have to pivot now." He pointed to the fact that OCR put the spotlight on Part 2 days before the amended Part 2 rule took effect. He recommends CEs:

- ◆ Confirm their NPP is updated (e.g., explains Part 2's confidentiality protections and redisclosures);
- ◆ Ensure SUD data is incorporated into breach response (e.g., "incident response playbooks flag Part 2 data and apply HIPAA breach analysis and notification standards," Trusiak said);
- ◆ Review redisclosure protocols (e.g., electronic health record permissions and consent workflows have new language about redisclosures without "legacy blanket consent language");
- ◆ Update vendor agreements (e.g., business associate agreements and qualified service organization contracts should include Part 2 obligations vis-à-vis SUD data); and
- ◆ Revisit staff training (e.g., make sure employees know when SUD records may be used for TPO versus when a separate consent is required).

Contact Trusiak at robert@trusiaklaw.com, Pike at jennifer.pike@alston.com and Cain at doriann.cain@faegredrinker.com. ✨

Endnotes

- 1 U.S. Department of Health and Human Services, Office for Civil Rights, "Office for Civil Rights Announces Civil Enforcement Program for Confidentiality of Substance Use Disorder Patient Records," news release, February 13, 2026, <https://bit.ly/4kTz6lb>.

- 2 Confidentiality of Substance Use Disorder (SUD) Patient Records, 89 Fed. Reg 12,472 (Feb. 16, 2024), <https://bit.ly/3wpt20l>.
- 3 U.S. Department of Health and Human Services, Office for Civil Rights, "Model Part 2 Patient Notice," content last reviewed February 13, 2026, <https://bit.ly/4qJfxn4>.
- 4 U.S. Department of Health and Human Services, Office for Civil Rights, "Model Notice of Privacy Practices for HIPAA Covered Health Care Provider," content last reviewed February 13, 2026, <https://bit.ly/3OlstSU>.
- 5 U.S. Department of Health and Human Services, Office for Civil Rights, "Understanding Confidentiality of Substance Use Disorder (SUD) Patient Records or 'Part 2,'" content last reviewed February 13, 2026, <https://bit.ly/3ZKlx2Y>.
- 6 U.S. Department of Health and Human Services, Office of Inspector General, Assistant Secretary for Technology Policy, "Enforcement Alert: Information Blocking," September 4, 2025, <https://bit.ly/41xoKp6>.

Exclusions, Vendors, AI: Mitigation Tips For Top 10 Compliance Risks

Although hospitals typically screen employees for exclusion from federal health care programs, they may overlook the ordering and prescribing physicians who don't have medical-staff privileges.

That's a mistake, said Miriam Murray, a senior manager at PYA. They should "screen anyone who is ordering a service from your hospital." It's necessary to sweep physicians who only order and prescribe (e.g., diagnostic tests) into the exclusion screening process because Medicare and other federal health care programs don't pay for services provided by people who have been thrown out of them, although "sometimes you don't have a good line of sight to them" until the physicians send an order, Murray said at a Feb. 18 PYA webinar. "They're not on the medical staff, so they haven't gone through exclusion screening and credentialing."

Hospitals face the same exclusion minefield with vendors. Hospitals and other providers may be held responsible for a vendor's excluded employee, said Katie Crowell, a manager at PYA. Exhibit one: In July 2025, Kidspeace National Centers of New England Inc., a behavioral health care company in Maine, agreed to pay \$44,736 in a settlement with the HHS Office of Inspector General (OIG) over allegations it employed an excluded person through a contractor. "OIG alleged that the excluded individual, a speech pathologist, provided items or services that were billed to Federal health care programs," according to OIG's website.¹ Billing for services provided directly or indirectly by excluded people or entities invites civil money penalties and possibly false claims allegations. Running employees, vendors, prescribing providers and others every month through OIG's List of Excluded Individuals and Entities will help reduce the risk, Murray said.

Exclusions are one of the top 10 risks that compliance teams, operational managers, compliance committees

and board members should keep their eyes on, said Shannon Sumner, principal and chief compliance officer at PYA. “Compliance is everyone’s responsibility.” But she noted that “so many risks could be added to it.” A brand-new one: the 2026 Consolidated Appropriations Act requires hospitals to attest to the compliance of their off-campus provider-based departments and obtain separate Medicare identifiers for them.

Nine Other Top Compliance Risks

- ◆ **Outsourced arrangements.** Organizations increasingly delegate a host of services to outside companies, including clinical services, medical directors, technology/software, recruitment, coding and billing, Sumner said. Although they may do the work, the compliance buck stops with the organization. The agreements with outsourced entities should document expectations of “confidentiality, audit rights and contract termination if the vendor’s performance is unacceptable,” she said. The departments that use the services should monitor the vendor’s performance. “Many times, we see wonderful contractual relationships defined in the written agreement, but where we see things fall short is upon execution,” Sumner said.
- ◆ **Vendor oversight.** A third-party risk management lifecycle, which is almost a mini-compliance program for vendors, helps mitigate the risk. The lifecycle in a nutshell: onboarding (e.g., due diligence); risk assessment (e.g., evaluating possible compliance, financial and operational risks); monitoring (e.g., ongoing oversight of vendor’s performance and risk indicators); performance evaluations (e.g., reviewing the vendor’s deliverables against expectations); and offboarding (e.g., quickly ending the vendor’s access to your systems). Keep in mind that the U.S. Department of Justice’s *Evaluation of Corporate Compliance Programs* puts a premium on third-party risk assessment, Sumner said.
- ◆ **Administrative compensation and stacking.** Compliance should always have administrative agreements with independent physicians on their work plan. Risks include incomplete time sheets, services that aren’t performed and compensation “for administrative duties that are part of their other duties” (e.g., the hospital pays the physician for hours devoted to education or service line meetings), Sumner said. “You don’t get paid extra for those.” Stacking—paying physicians under multiple administrative agreements—is another risk area. Even if compensation for each one is fair market value, the total compensation may be over the top. Impossible hours also may be a problem. Sumner worked with the president of a heart hospital who also had their own private practice and was receiving compensation for two administrative agreements. “There was no way this person could do all of that,” she noted.
- ◆ **Cybersecurity and data breaches.** In addition to technology-related threats, such as ransomware and cloud-based server vulnerability, humans open the door to threat actors (e.g., they succumb to phishing), Murray said. “Human error is still the number one cause” of breaches, she noted. “Ensure team members are aware of company policies and reporting requirements.” Compliance should update cybersecurity and information system policies and ensure business associate agreements are updated and enforced. Organizations also need strong controls, such as multifactor authentication. All that also applies to vendors because “hackers have pivoted to go after third-party vendors,” she noted.
- ◆ **AI.** To mitigate AI risks, start with an inventory of AI tools in use, who is using them, how access is configured to ensure it’s the minimum necessary and what technical safeguards are in place—and then consider an AI-specific risk assessment, Murray said. For example, if your organization uses AI tools to review medical records and suggest coding, “periodically you will want to have an independent audit of that system to ensure it’s appropriately giving the suggestions and there’s not bias in the tool.” Also high on the list: making sure security protocols are in place and “prioritizing patient safety by understanding the risks and embedding compliance in every stage of AI adoption,” Murray said.
- ◆ **Data transformation and digital care.** This includes electronic health record systems, telehealth, ambient AI and remote patient monitoring. “Integrate compliance into daily digital care operations,” Murray said.
- ◆ **Health care real estate.** This is a bigger risk area than people may realize. Common challenges include below fair market value hospital leases with physicians; long leases without rent escalators; expired leases where the physician stays on; hospitals providing free staff to independent physicians; and space creep, where, for example, the physician uses a closet that’s not part of the lease to store equipment. Murray recommends several mitigation strategies,

such as a centralized contract management system, which flags when leases expire, among other things.

- ◆ **EMTALA.** Winter is a good time to retrain staff on EMTALA because people with respiratory viruses are packing emergency departments, Croswell said. Reiterate the definition of EMTALA and the requirement to provide medical screening exams for people with emergency medical conditions. “Make sure staff is not turning patients away,” she urged. Questions to ask: Are call coverage physicians showing up when summoned and as fast as required by hospital policy? Are patients discharged with instructions for follow-up care? Is there a process for clinical and registration staff to communicate about prior authorization as soon as stabilizing care begins?
- ◆ **Reimbursement pressures.** There are many, Croswell said. Medicare and Medicaid reimbursement isn’t keeping up with inflation; value-based care is growing without funding for its infrastructure; supply, drug and labor costs are outpacing reimbursement; and payers are hot and heavy with audits and recoupment. The best offense is an effective compliance program because “it can help you retain the dollars you have rightfully earned,” Sumner noted.

Contact Sumner at ssumner@pyapc.com, Murray at mmurray@pyapc.com and Croswell at kcroswell@pyapc.com. ✧

Endnotes

- ¹ U.S. Department of Health and Human Services, Office of Inspector General, “Kidspace National Centers of New England Agreed to Pay \$44,000 for Allegedly Violating the Civil Monetary Penalties Law by Contracting with an Excluded Individual,” July 31, 2025, <https://bit.ly/3ZM8XkP>.

New MOON Is Out; One QIO Pushed Back on a Different Expired Notice

CMS on Feb. 20 gave hospitals the go-ahead to use the new Medicare Outpatient Observation Notice (MOON), which is posted on its website. The MOON, like other beneficiary notices, had expired, but hospitals continue to use the expired versions of the beneficiary notices with CMS’s blessing.¹ Even so, hospitals may run into trouble while the other forms are in limbo, as one hospital utilization review (UR) manager learned.

The MOON, which explains to hospital outpatients that they’re receiving observation services rather than inpatient care, is the only revised beneficiary notice posted on the CMS website. “The updated MOON is effective now and expires February 28, 2029,” CMS said. “Providers who have existing stock of the expired

MOON may continue to use the expired version until April 20, 2026, but must transition to the new form no later than that date.”

Other expired forms are the Detailed Notice of Discharge (DND), Advance Beneficiary Notice (ABN) and Important Message from Medicare (IM). For now, CMS says on its website “In the event the notice expires, providers and plans may continue using the current version of the notice after the expiration date.” Unlike the MOON, updated versions of these other forms are not available.

Apparently, one quality improvement organization (QIO) didn’t get the memo that hospitals are permitted to use the expired DND, leading it to side with a patient who appealed a hospital’s discharge order, according to the UR manager, who prefers not to be identified.

Even though the CMS website says in black and white that hospitals should continue to deliver the expired forms, the QIO insisted the hospital used an “invalid” DND during the appeal, the UR manager said.

Patients learn from the IM they may contact the QIO and appeal a discharge while they’re still in the hospital. With that process set in motion, the QIO informs the hospital of the appeal and asks for the medical records, and the hospital is required to fill out a DND and deliver it to the patient, said Ronald Hirsch, M.D, vice president

CMS Transmittals and Federal Register Regulations, Feb. 13-19, 2026

Transmittals

Pub. 100-04, Medicare Claims Processing

- File Conversions Related to the Spanish Translation of the Healthcare Common Procedure Coding System (HCPCS) Descriptions, Trans. 13,587 (Feb. 19, 2026)
- Quarterly Update to the Medicare Physician Fee Schedule Database (MPFSDB) - April 2026 Update, Trans. 13,648 (Feb. 19, 2026)
- Update to Claims Processing Instructions for National Coverage Determination (NCD) 20.4 Implantable Cardiac Defibrillators (ICDs), Trans. 13,641 (Feb. 13, 2026)

Pub. 100-03, Medicare National Coverage Determinations

- NCD 20.40- Renal Denervation (RDN) for Uncontrolled Hypertension, Trans. 13,640 (Feb. 13, 2026)

Pub. 100-20, One-Time Notification

- Prior Authorization Data - Add Medicare Beneficiary Identifier (MBI), Trans. 13,645 (Feb. 19, 2026)
- Updating Consistency Editing Logic for Provider-Based Department (PBD) Claims Processing, Trans. 13,644 (Feb. 19, 2026)

Federal Register

Notice, request for information

- Request for Information: 340B Rebate Model Pilot Program, 91 Fed. Reg. 7,287 (Feb. 17, 2026)

of R1 RCM. That's how patients learn their appeal is in process and why the hospital thinks it's time for them to go.

In this case, the hospital completed the expired DND—the only one that exists—and sent it to the QIO. But the QIO told the UR manager to download an updated DND from the CMS website even though there's no such thing (yet). The UR manager said she spoke to several customer service representatives and supervisors and got the same response.

"The whole process was incredibly frustrating," the UR manager said. "I kept hitting roadblocks."

The impasse had consequences. "What they were saying was because we didn't have a valid form, we couldn't hold [patients] liable," the UR manager explained. "We received a determination letter from the QIO on a discharge appeal, and on the discharge appeal, it referenced the DND was invalid."

Eventually, the UR manager heard from a supervisor. "She offered sincere apologies and is now reviewing all prior communications and interactions related to this case in order to provide education to the involved staff. She is also issuing an updated determination letter," the UR manager said. "While I appreciate her responsiveness and efforts to correct this, the amount of time and resources spent addressing this matter could have been avoided." The QIO's remit includes

beneficiary notices, and "I would hope we could look to them as experts," she said.

Other than making its case to QIO representatives, hospitals don't have much recourse when they get a denial based on a technicality, Hirsch said. Discharge appeals are usually based on substantive issues, such as whether there's a medical reason for the patient to stay in the hospital (e.g., a patient is febrile and continues to require IV antibiotics). The QIOs are generally fair, and they have no financial incentive to deny cases like some other program integrity contractors, he said, but the UR manager's experience is a reminder to be on guard.

Hirsch said hospitals often misunderstand that beneficiary notices are a Medicare condition of participation, not a condition of payment. They can get dinged on a survey if they drop the ball, but they will still get paid for the admission.

"This comes up quite often," he noted. "Hospitals say, 'We forgot to deliver the MOON or did it after 24 hours. Are we still allowed to bill for the care?'" The answer is yes, but as a condition of participation, "it's something you need to take seriously."

Contact Hirsch at rhirsch@r1rcm.com. ✦

Endnotes

- Centers for Medicare & Medicaid Services, "Beneficiary Notices Initiative (BNI)," accessed February 20, 2026, <https://go.cms.gov/4rtet8k>.

NEWS BRIEFS

◆ **Indiana physician Bethany A. Cataldi was sentenced to 97 months in prison and ordered to pay more than \$19.138 million in restitution after pleading guilty to health care fraud, the U.S. Attorney's Office for the Northern District of Indiana said Feb. 18.**¹ Cataldi, who owned the Center for Otolaryngology and Facial Plastic Surgery in Highland, billed Medicare and private insurers for thousands of balloon sinuplasty procedures that she never performed, the U.S. attorney's office said. Cataldi collected almost \$20 million in reimbursement and patient copays for the "non-existent procedures" after billing about \$50 million.

◆ **Top of the World Ranch Treatment Center (TWRTC), a substance use disorder treatment provider in Illinois, has agreed to pay \$103,000 and implement a corrective action plan in a settlement for a potential violation of the HIPAA Security Rule, the HHS Office for Civil Rights (OCR) said Feb. 19.**² OCR received a breach report from TWRTC

in March 2023 and began an investigation. TWRTC reported that an unauthorized third party accessed electronic protected health information (ePHI) through a workforce member's email account after a phishing attack. As a result of the attack, the ePHI of 1,980 patients was compromised. TWRTC didn't admit liability in the settlement.

◆ **The HHS Office of Inspector General has updated its work plan.**³

Endnotes

- United States Department of Justice, United States Attorney's Office for the Northern District of Indiana, "Highland Physician Sentenced to 97 Months in Prison," news release, February 18, 2026, <https://bit.ly/3OiwKlK>.
- United States Department of Health and Human Services, Office for Civil Rights, "HHS' Office for Civil Rights Settles HIPAA Security Rule Investigation with Top of the World Ranch Treatment Center," news release, February 19, 2026, <https://bit.ly/3ZIOUDY>.
- United States Department of Health and Human Services, Office of Inspector General, "Browse Work Plan Projects," February 17, 2026 <https://bit.ly/4k0Owh1>.