30 Years HCCA Report on
MEDICARE COMPLIANCE

Volume 35, Number 23 • June 22, 2026

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

Contents

Managing Editor
Nina Youngstrom
nina.youngstrom@hcca-info.org

Copy Editor
Jack Hittinger
jack.hittinger@hcca-info.org

In Paradox, Ambient AI May Bring Humanity Back to Patient Encounters, but 'Read the Notes'

When Vanderbilt University Medical Center in Tennessee replaced hundreds of human scribes with an AI scribe, some attending physicians who supervise residents and fellows stayed out of the exam room altogether. Instead of seeing the patients for an exam and medical decision making, the attending physicians let the residents and fellows take over. After the encounter, they turned on ambient AI for a briefing with the attending physicians, who signed the documentation and moved on.

"My problem with that? The attending never saw the patient," said Mark Jenkins, compliance officer at Vanderbilt University Medical Center. How did he know? There was no documentation of physician-patient interaction (e.g., asking about the patient's family). "They forget we can see all that," Jenkins said. As he told the physicians, "I can see exactly that there was no patient participation in the conversation—no personal interaction because it was between you and your resident. No, 'How is your grandbaby?'"

After this shortcut came to light, "we put in a policy banning it as an inappropriate activity," he said.

'The Risks Are Real for us'

That's an example of the two sides of the AI coin. It has the potential to shoulder some of the documentation burden, reduce physician burnout and increase face-to-face interaction with patients. But without human review of AI-generated documentation and other tools, AI might come back to haunt providers.

"The risks are real for us as compliance professionals," Jenkins said at HCCA's Compliance Institute April 28.

It's also another reminder why clinicians must read their notes when AI tools are in the mix, said Colleen Dennis, director of compliance at Children's Hospital Colorado. "From a compliance perspective, you can't be one of the lazy doctors. You can't just make the assumption that everything is OK" in the AI version.

'AI Is Bringing More Humanity Back'

The paradox of ambient AI is that it's technology that makes the patient experience more human. "AI is bringing more humanity back to the practice of medicine," Dennis said. Because AI records patient encounters, physicians are lifting their eyes up from their laptops and looking at patients again.

When they're not glued to iPads, physicians notice things about patients, such as having a flat affect, having trouble answering questions or having trouble crossing their legs because they're swollen, Dennis said. Otherwise, physicians may miss body language if they're glued to their iPads. "That engagement builds their trust and the bond that allows the provider to get [patients] involved in their care," she noted.

It's also a buffer against a sometimes-impossible workload.

"Our practitioners are being pushed every day to see more patients. As an academic medical center, often we have specialties nobody else has in the region," Jenkins said. "Pushing a specialist to see 20 to 30 patients a day has caused a lot of practitioner burnout. We have practitioners complaining they see patients from 7 a.m. to 5 p.m. and go home and document until 11 p.m."

But compliance professionals should help ensure there are guardrails to prevent AI-driven errors, such as

hallucinations and fabrications. If an error isn't fixed, it could be replicated again and again, he noted.

There's also the risk of speaker attribution error. Ambient AI could mistake a patient for a physician and vice versa. It also can't record a patient's slumped shoulders or watery eyes, Dennis said. "Someone has to say that [out loud]" or it won't be in the documentation.

Testing AI Tools: 'Refine' vs. 'Review'

Some clinicians use AI to prepare notes from their encounters. Dennis tested two AI tools to see how accurate they would be with varying commands.

She typed the information into the tools, starting with ChatGPT: A 45-year-old patient self-reported headaches two or three times a week, as well as being tired and having trouble sleeping. Her blood pressure was 140/90, her lungs were clear and her neck tender. Dennis's assessment identified stress headaches and anxiety and her plan called for rest, ibuprofen and more exercise.

Dennis told ChatGPT to refine her documentation and make it more readable. "It refined it all right," she said. There were things in the AI version she never mentioned.

"It added pain six out of 10, dull aching across forehead, she is sleeping five hours a night due to racing thoughts," Dennis said. "That wasn't in my notes." ChatGPT also added that the patient was alert and oriented per a neuro exam, her cranial nerves II-XII were intact and she had mild tenderness in her trapezius muscles.

"I didn't say any of that," Dennis noted. "So, my command was wrong."

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.

She took a different tact with another AI tool. Instead of telling Claude to refine the notes, she commanded it to "review and make more readable."

This time, Dennis typed in notes for a 58-year-old patient with hypertension and type 2 diabetes who reported home readings of slightly high blood pressure and fasting glucose 140 to 160.

Objective data for the patient was a blood pressure of 142 over 92, no edema and clear lungs, with a hemoglobin HbA1C test result of 7.8%. Dennis' assessment was hypertension and her plan called for increasing the patient's dose of Metformin and testing glucose again in three months.

Claude created a "pretty note" that was fairly clear and didn't take liberties for the most part. The only thing the AI tool changed was "lungs clear to auscultation. I just said lungs clear. And this said no peripheral edema. I just said edema."

Claude went a step further and suggested home monitoring the patient's blood pressure. "That's a good callout. I might want to think about having them monitor their blood pressure at home."

Her takeaway: "AI is really good to use. It will humanize medicine." But providers must review notes generated by the AI scribe. "Don't make assumptions," she said. "What if it's totally different" from what you said in the encounter? "You have to read the note."

Compliance and Revenue Cycle Are AI Partners

Between the risks and rewards of AI, compliance and the revenue cycle departments "will be good partners for AI," Dennis said. "That's an opportunity. Your revenue cycle is the first line of defense."

Compliance needs a seat at the table with leadership "as AI continues to reshape healthcare and transform our documentation."

Providers also should watch their backs. Payers are using AI to ferret out whether documentation is AI-supported. For example, AI can identify indications that the physician didn't write the note because they used medical terms that they didn't use in 99% of other notes, Jenkins said.

"Doctors do the same things over and over again" and AI will be able to flag a deviation, Dennis said.

"If you have AI, let them know, but reiterate the provider is the one who is treating [patients], making medical decisions, following them through their care," Dennis said. AI "just helps them document."

Contact Dennis at colleen.dennis@childrenscolorado.org and Jenkins at kenneth.m.jenkins@vumc.org. ✧

Proposed Shakeup of Federal Grants Paves Way for More Terminations

Research compliance officers will have to get very familiar with cost accounting principles if a proposed regulation on federal financial assistance is finalized.

The May 29 proposed rule from the Office of Management and Budget (OMB), which would overhaul grant management at HHS and other funding agencies, puts an end to fixed-amount awards and subawards in favor of "merit-based" discretionary grants.[1]

Although OMB frames it as a way to increase transparency and oversight, the shift "would increase the compliance burden related to grants accounting," said attorney Kate Heffernan, with Epstein Becker & Green.

Other sweeping changes to the Guidance for Federal Financial Assistance at 2 C.F.R Part 200 (known as the Uniform Guidance) would make it easier to terminate grants midstream; empower political appointees to review and reject grants before they reach a merit review; and prohibit grants that touch on diversity, equity and inclusion (DEI) and gender-affirming care.

And the rule tinkers with its name. Uniform Guidance would become Uniform Grant Regulations to drive home the point that the guidance is binding.

'They Want Clear, Item-by-Item Justification'

The way certain fixed-amount grants are awarded now gives researchers discretion in the way they budget. "You can get a lump sum and spend that money with flexibility so long as the aims of the award and agreed-upon deliverables are met. You don't have to do the same type of cost accounting for each expenditure," Heffernan noted.

That goes out the window if the rule is finalized because it ditches certain fixed-amount grants. "They want clear, item-by-item justification for how you are spending the grant funds," she said. "All grant funding will be subject to very rigid cost accounting principles." That's where the increased potential noncompliance arises for institutions without robust cost accounting programs.

Compliance officers would have to "get up to speed quickly on how to manage cost accounting principles," she noted.

Grants Can Be Pulled at Any Time

Like many Trump administration initiatives, the changes to the Uniform Guidance were set in motion by a 2025 executive order (EO)—in this case, it was the EO on "Improving Oversight of Federal Grantmaking."[2] It set the stage for the 2025-2026 termination of grant programs that don't align with administration priorities, although the basis for some terminations was unclear except possibly to cut spending, Heffernan said.

Ultimately, many of the grant terminations were reversed and reinstated because they didn't follow procedural requirements under the Uniform Guidance, as determined by several court cases. "The proposed rule is arguably a direct response to the setbacks the administration faced in court," she said.

Normally researchers operate on the assumption that they will continue to receive the money during a multi-year funding cycle although they're required to demonstrate every year they're performing the work compliantly and in furtherance of the award's aims, Heffernan said. If they want to terminate a grant, funding agencies must articulate the reason for the termination, which may be appealed, she said.

That will be history if the rule is finalized. Funding agencies would have another avenue to terminate grants in addition to terminations for noncompliance (e.g., fraud).

"It's giving a lot more flexibility and discretion to funding agencies to decide to terminate without specific cause," and grantees have no way to push back because there are no appeal rights.

Grants can be yanked at any time, even in the middle of a clinical trial. "That injects a certain degree of insecurity into funding continuity and puts grantees in a more challenging position with respect to raising objections to terminations," Heffernan noted.

Adding a Political Layer to the Process

Grant applications also could be cut off at the pass by political appointees. Currently, when applications are submitted to funding agencies, they're reviewed for compliance and then forwarded for peer review.

But OMB would require senior political appointees to do a "pre-issuance review" of discretionary awards. "It adds this layer of politicization to the funding decision-making that historically hasn't been there, at least not explicitly," Heffernan noted. "It's introducing this concept of oversight and screening from a political as opposed to a scientific standpoint."

Grave concerns about this proposed change were raised in a June 15 editorial in the *New England Journal of Medicine*.[3] "Giving political appointees ultimate authority to determine federal grant funding, as proposed by the OMB, would politicize and weaken biomedical research. Expert, independent peer review of grant applications is essential for directing [National Institutes of Health] dollars to research that has the greatest potential for advancing science and improving health," the editorial stated.

No Research Money for DEI

The rule telegraphs the administration's antipathy toward DEI, gender-affirming care and undocumented immigrants. OMB said it wants to move away from the days

when "Federal awards were often used during those years to promote a 'woke' policy agenda that did not reflect the values of the vast majority of the American public."

Assuming the rule takes effect, OMB would require funding agencies (e.g., HHS) to ensure federal grants aren't used to promote, subsidize or facilitate DEI policies and practices that violate federal anti-discrimination laws; "gender ideology"/"the so-called 'transition' of a child under 19 years of age from one sex to another"; Illegal immigration; or "any other initiatives that compromise public safety or promote anti-American values."

Assuming it's finalized, the rule will take effect Oct. 1, 2026, and apply to all new grants and awards issued starting in federal fiscal year 2027. Comments on the rule are due July 13.

Contact Heffernan at kheffernan@ebglaw.com. ✧

Endnotes

1 Regulation for Federal Financial Assistance, Proposed Rule, 91 Fed. Reg. 32,198 (May 29, 2026) (to be codified at 2 C.F.R. pts. 1, 25, 170, 175, 176, 180, 182, 183, 200, 300, 376, 382, 400, 417, 421, 600, 601, 700, 701, 780, 782, 801, 802, 901, 902, 910, 1000, 1104, 1120, 1122, 1125, 1126, 1200, 1201, 1326, 1327, 1329, 1400, 1401, 1402, 1500, 1532, 1536, 1600, 1800, 1880, 1882, 1900, 2000, 2001, 2200, 2205, 2245, 2300, 2336, 2339, 2400, 2424, 2429, 2500, 2520, 2600, 2700, 2701, 2800, 2867, 2900, 2998, 3000, 3001, 3002, 3185, 3186, 3187, 3254, 3255, 3256, 3369, 3373, 3374, 3474, 3485, 3513, 3603, 3700, 3701, 5800, 5801, 5900, 6000, 6100, 6200, 6300, 6400, 6500, and 6600), https://bit.ly/4eg9DHg.

2 Improving Oversight of Federal Grantmaking, Exec. Order No. 14,332, 90 Fed. Reg. 38,929 (Aug. 7, 2025), https://bit.ly/4vdpuMI.

3 The Editors, "The OMB and the Politicization of Science," *New England Journal of Medicine*, June 15, 2026, https://bit.ly/44gFMIR.

In Another Compliance Review, OIG Said Ark. Hospital Was Overpaid $4.7M

In a new hospital compliance review, the HHS Office of Inspector General (OIG) said Jefferson Regional Medical Center (JRMC) in Arkansas was overpaid $4.7 million in 2021.[1] The usual suspects, including the Two-Midnight Rule and inpatient rehabilitation facility admissions, drove the overpayment findings. OIG recommended the hospital refund the money.

The hospital disagreed with the bulk of OIG's findings and found fault with the way OIG's medical review contractor applied Medicare requirements to its claims. But the hospital wasn't allowed to make its case to the contractor.

This is the third hospital compliance review in the latest series from OIG. In a March report, OIG said Medicare overpaid Lehigh Valley Hospital in Pennsylvania $17.8 million for high-risk claims.[2] A month earlier, OIG said Sarasota Memorial Hospital in Florida received $12.1 million in overpayments.[3]

Because compliance reviews take on multiple risk areas at the same time, they provide a roadmap to the top billing risk areas. But there's not a lot of detail in the latest round, said Steve Gillis, director of compliance coding, billing and audit at Partners Healthcare in Boston, Massachusetts. "OIG is not really showing their cards."

The mystery of overpayments also deepens when OIG walls off the independent medical review contractors.

OIG: 33 Claims Had Errors

According to the report, OIG reviewed a stratified random sample of 100 claims in high-risk areas that generated $1.3 million in Medicare reimbursement.

The findings: JRMC didn't comply with Medicare billing requirements for 33 claims, resulting in net overpayments of $348,677 for the audit period, which OIG extrapolated to $4.7 million. The errors in a nutshell:

- Ten of the inpatient claims didn't comply with the Two-Midnight Rule, according to OIG. For example, one enrollee on medication for hypertension presented to the hospital with acute high blood pressure. The enrollee's blood pressure was brought down by oral medications, their cardiac enzymes were negative, and the electrocardiogram was unremarkable. "The enrollee was admitted for medication adjustment, and the admitting physician expected the enrollee could be discharged within 24 to 48 hours," OIG said. The documentation didn't support an expectation that the enrollee would require hospital care for at least two midnights.
- Four inpatient claims had an unsupported diagnosis code and three had the wrong discharge status code.
- Twelve related to IRF admissions. Mostly, OIG said there wasn't a "reasonable expectation that the enrollee required supervision by a rehabilitation physician."
- Six of the outpatient claims were billed with modifiers 59, XU or 59 "even though the services on the claim were not separate and distinct." One claim had a code with modifier XU, "which improperly unbundled the billing for compression dressings that were part of an unhealthy tissue removal procedure performed on the same anatomic area," according to OIG.
- Two outpatient claims lacked supporting documentation.

In its written response to the report, JRMC said OIG's medical review contractor misapplied CMS rules

and overlooked documentation supporting claims in several risk areas.

But the hospital wasn't allowed to make its case to the source. "Since we have been unable to have a substantive claim-specific discussion with the medical review contractor or OIG about the claims at issue, JRMC's response is based on the written information that has been provided by OIG and is informed by JRMC's expert reviews," the hospital said.

For example, JRMC said all 10 inpatient claims complied with the Two-Midnight Rule. The example of the enrollee with acute high blood pressure "fails to paint a complete picture," the hospital wrote.

The hospital said that OIG never mentioned the inpatient admission order estimated the enrollee would stay in the hospital at least two midnights, was treated in the ICU and "that the combination of the patient's acute congestive heart failure and uncontrolled hypertension typically requires at least 2 midnights of care to adequately diurese the patient and to lower blood pressure in a controlled fashion without compromising cerebral, coronary or renal perfusion."

And despite what OIG said, there was nothing in the chart about the physician expecting discharge in 24 to 48 hours, the hospital contends.

Contact Gillis at sjgillis@mgb.org. ✧

Endnotes

1 U.S. Department of Health and Human Services, Office of Inspector General, Office of Audit Services, "Jefferson Regional Medical Center Received at Least $4.7 Million in Medicare Overpayments," A-04-22-07101, June 2026, https://bit.ly/4aVVSey.

2 U.S. Department of Health and Human Services, Office of Inspector General, Office of Audit Services, "Lehigh Valley Hospital Received At Least $17.8 Million in Medicare Overpayments," A-03-23-00001, June 2026, https://bit.ly/43vN4bq.

3 U.S. Department of Health and Human Services, Office of Inspector General, Office of Audit Services, "Sarasota Memorial Hospital Received At Least $12.1 Million in Medicare Overpayments," A-04-23-08098, February 2026, https://bit.ly/44gJgLk.

CISOs: Beware Spoofed Applicants for Remote Jobs in the Latest AI Scam

Science fiction is becoming reality as offshore bad actors use AI to impersonate applicants for remote positions and try to gain in-house access to sensitive systems they then compromise, according to a panel of healthcare chief information security officers (CISOs).

"On the AI front and on the identity front, it used to be this theoretical thought where you could have real-time deep faking and spoofing kinds of attacks that were occurring," said Erik Decker, vice president and CISO at Intermountain Healthcare. "We thought it was science fiction." Unfortunately, these AI-generated attacks are happening at scale, he said at the 43rd National HIPAA Summit.[1]

There is currently "a very large active campaign by North Korea through their national operations to effectively use corporate America to fund their national defense and security programs," Decker explained.

"They're going after the very high-paying jobs that are 100% remote in corporate America," with North Korean nationals applying for these jobs fraudulently, he said. They're using a combination of stolen credentials from real people and fabricated credentials. "If one person can secure 10 jobs, then you have the potential for one person to be able to pull in about a million dollars of revenue if you assume a hundred thousand dollars a job. Put an army of people in place to do that across the board, and you've got a new threat," Decker said.

Real Experience, Fake Profiles

He said he has heard anecdotes from other CISOs who tell him that for every remote job posted, 30% to 40% of the applications are North Koreans "trying to subvert their way in and effectively become employed." These people can collect a paycheck to fund national defense programs in North Korea and ultimately extort their employers when they get caught, he said.

To do this, North Korea uses AI to fake profiles and the real work experience of an individual whose data was compromised to pass background checks, Decker said. They can use AI and available photos of the individual to generate an avatar for an on-camera interview "and you don't know that you're actually talking to somebody who's not the real person at the other end of that keyboard," he said.

These are sophisticated actors, and there's a tremendous infrastructure built around this capability, explained Chris Tyberg, CISO at Abbott. "There's money to be made, and they have organized around it." There's even a system to game the drug tests that might be performed as part of employment screening, he said.

To detect this type of AI-fueled scam, organizations can ask the person to turn off their background, which might reveal a call center, or pass their hand in front of their face, which causes AI artifacts to appear, Decker said. However, AI will continue to improve, likely rendering these clues moot.

To identify potential threats, Decker said he starts by considering who and what the threat actors are, their motivations, why they are targeting his organization and how they are targeting it.

In-Person Interviews Return

More organizations are requiring one in-person interview for certain roles, or requiring the person hired to pick up their company-issued device in person, Tyberg said.

In addition, organizations that use third-party entities in the hiring process need to communicate with their vendors about how they verify candidates, said Michael Bray, CISO at The Vancouver Clinic. "Are they aware of the faked LinkedIns? Are they aware of the North Korean groups? Are they aware of the other groups that are out there doing very similar work? What adjustments are they making to protect us?"

Vancouver Clinic recently started requiring some applicants to fly in, Bray said. "We're willing to pay that $1,200, $1,500, $2,000 to vet somebody in certain positions versus taking that risk that it's all virtual and it can be impersonated."

The clinic has also started a campaign, "See Something, Say Something," aimed at HR and hiring managers to educate them on these threats, Bray said.

For example, the campaign recommends looking at new employee orientation, which in Vancouver lasts two to three days, to see if the person was engaged and whether their camera was on throughout the entire presentation, he said. Team members are encouraged to flag someone who is "on your team, but they don't really call you, they don't engage with you," Bray said.

In one case, a candidate called the help desk to retrieve their original network credentials but didn't want to turn on their camera. "The help desk reported that. It went to the hiring manager, [and] the hiring manager called that person, who was on their second day. That person only wanted to text [and] did not want to get on the phone, so maybe they weren't prepared. And we ended up finding out that that was an impersonation of a candidate. We dodged a bullet on that one, but it's happening like crazy."

Financial, HR Roles Targeted

The bad actors are targeting financial positions and, in some cases, HR roles, because those are more likely to have access to sensitive information, Bray said.

The "mule" will be hired and will have enough knowledge to handle the role for several days or weeks, and then that mule will hand off the credentials to "the folks that really know how to do the damage," he said. "So, you might sometimes have a little bit of a window to catch it—maybe, maybe not—but it's all part of the vetting and the initial onboarding for these candidates."

To mitigate some of these risks, Tyberg recommended enabling multifactor authentication (MFA) and considering phishing-resistant MFA. Looking beyond MFA, high-risk roles should have more targeted controls.

There are additional places where bad actors are trying to find ways into organizations, the CISOs said.

For example, many attacks in recent years have involved social engineering targeting the service desk to obtain valid credentials, Tyberg said. "If you're not, I encourage people to run social engineering tests against your service desk, whether it's your team or a third party, to make sure they're following procedures." For organizations that outsource their service desk, Tyberg recommended repeated phishing tests. "One of the things we've done is monthly phishing tests. If a service desk person misses more than a couple in a 12-month rolling period, we require our third party to pull that person from the account."

Leadership Input Needed

The information security team needs to stay on top of all these threats in real time to protect the organization, the CISOs said. Bray said it's all about resiliency: "We can bend but not break." In addition, from a strategic perspective, it's key to get in front of the board and executive leadership team to make sure security has a seat at the table, he said.

For crisis management, it's important to ask if a leadership representative has been part of a crisis management tabletop plan, whether there's a crisis manager named and how that person will work with the legal and public relations departments in the event of an actual crisis, Bray said. "Do we understand those third party, fourth party, fifth party, sixth party relationships, what the impact is to clinical operations and our ability to serve our patients?"

Meanwhile, the cybersecurity team functions "like a volunteer fire department" where "at any given time they could be called into action." Recovery is an area that's sometimes overlooked as part of this equation, Bray said. "Recovery is the boring part, right? You do the tabletop, you want to hack, you want to get in, you want to see if you can stop them."

However, recovery is critical and often takes longer than administrators think it will, Bray said. "If we can get those recovery times down, we become more resilient." He recommended performing a tabletop exercise on recovery to see what issues it uncovers.

Cut Through the AI 'Hype, Magic'

AI also is being used in more pedestrian ways, Tyberg said. AI is driving "improvements" in phishing and social engineering attacks, such as an AI-generated "phone call from a senior leader asking you to do something." Fortunately, new tools are emerging that will help healthcare organizations educate and test their user populations about phishing and social engineering, he said.

"As with all things AI, there is a lot of hype and magic that's being discussed," Decker said. Still, he noted that AI should be used for good within healthcare organizations.

"One of the best ways you can start contemplating the use of AI on the good guys' side of the house

is to really get use case-specific," Decker said. He recommended looking for repeatedly problematic areas, such as data loss prevention.

Intermountain is considering giving agentic AI greater access to analyze data events to help give human analysts more context, Decker said. "If I see a phishing [attempt] then turn into a privileged escalation event, I think that we might be able to get some value there. It's theoretical that we would get value there, but I think there's opportunity."

AI can also help an organization's external attack surface, Decker said. "Today, when we do attack surface management work, we do have automated tools that will scan and look and start to see how things are changing." Using AI to analyze how changes, such as opening a port, might affect potential threats can help identify and mitigate them before they become an issue, he said.

Ongoing maintenance is also key, given that AI technology and the AI space are changing so quickly, Tyberg said. And AI can also help find bugs that represent security risks faster than humans can, he noted.

Governance Key to AI Use

Most organizations at this point have created governance capability for their AI use, Tyberg said. It's possible for a healthcare organization to use its existing IT steering or governance committee for AI issues, but some have developed separate panels to review AI uses, Bray noted. Regardless, "it's very important to have the governance clearly defined on who's going to be accountable for it, who oversees it and who's authorizing it from both the clinical side and the operations side."

Data security is the other "pillar" of the AI puzzle, Bray said. For example, "How does it map to HIPAA with the PHI [protected health information] data?"

Human oversight is key, Bray said. "We've got these droids out there working for us, which are incredible. But we have to have some human oversight with the hallucinations and the false positives. We wouldn't want a provider to provide patient recommendations on something specifically from the output of a droid without some sort of human oversight. And we wouldn't want a system engineer making decisions on blocking or taking action on an email or a firewall or a web portal without some human oversight."

A version of this article originally appeared in *Report on Patient Privacy*, *RMC*'s sister publication. For more information, visit http://bit.ly/2TJ1VcM. ✧

Endnotes

1 Michael Bray et al., "Cybersecurity Leader's Roundtable: Protecting Healthcare in a Rapidly Evolving Threat Environment," Virtual 43rd National HIPAA Summit, April 8, 2026, https://bit.ly/4tvddBZ.

CMS Transmittals and *Federal Register* Regulations, June 12-18, 2026

Transmittals

Pub. 100-04, Medicare Claims Processing

- July Quarterly Update for 2026 Durable Medical Equipment, Prosthetics, Orthotics and Supplies (DMEPOS) Fee Schedule, Trans. 13,805 (June 18, 2026)
- July 2026 Update of the Hospital Outpatient Prospective Payment System (OPPS), Trans. 13,832 (June 16, 2026)
- Update to Several Sections of the Internet-Only Manual (IOM) Publication (Pub.) 100-04, Medicare Claims Processing Manual, Chapter 23 - Fee Schedule Administration and Coding Requirements, Trans. 13,701 (June 16, 2026)
- October 2026 (2027 File) Update of the International Classification of Diseases, Tenth Revision, Clinical Modification (ICD-10-CM), Trans. 13,792 (June 16, 2026)

Pub. 100-07, State Operations Provider Certification

- Revisions to State Operations Manual (SOM), Chapter 5, Trans. 243 (June 12, 2026)

Pub. 100-05, Medicare Secondary Payer

- Creating Additional Medicare Secondary Payer (MSP) Error Codes to Better Identify Incoming MSP Claims that Conflict with MSP Records Found on the Common Working File (CWF), Trans. 13,833 (June 16, 2026)

Pub. 100-06, Medicare Financial Management

- The Fiscal Intermediary Shared System (FISS) Submission of Copybook Files to the Provider Statistical & Reimbursement (PS&R) System, Trans. 13,785 (June 12, 2026)

Federal Register

Final Rule with Comment Period

- Medicare Program; Strengthening Oversight of Accrediting Organizations (AOs) and Preventing AO Conflicts of Interest, and Related Provisions, 91 Fed. Reg. 36,370 (June 16, 2026)

Request for Information

- Request for Information; Comprehensive Review of the Essential Health Benefits Framework and Typical Employer Plan Standard, 91 Fed. Reg. 35,938 (June 15, 2026)
- Request for Information (RFI): Pharmacy Benefit Manager Compensation and Data Collection, 91 Fed. Reg. 36,776 (June 18, 2026)

Proposed Rule

- Medicare Drug Price Negotiation Program and Medicare Prescription Drug Benefit Program, 91 Fed. Reg. 36,236 (June 16, 2026)

Notice

- Agency Information Collection Activities: Proposed Collection: Public Comment Request; Information Collection Request Title: 340B Rebate Model Pilot Program Application, Implementation, and Evaluation, OMB Number 0906–NEW, 91 Fed. Reg. 35,989 (June 15, 2026)

Final Rule

- Reducing Bureaucracy and Burden for Human Services and Emergency Response Programs—Repatriation Program, 91 Fed. Reg. 36,542 (June 17, 2026)

Hospital, Payer Get on Same Sepsis Page in Show of Collaboration

Fed up with sepsis denials, a hospital tried another route to reverse them instead of the usual fistfights with payers. It collaborated with a payer to reduce the friction over sepsis denials and ease the administrative burden.

Like many others, the hospital had experienced an uptick in sepsis denials and was digging into why, said Erin Boyd, M.D., associate chief medical officer for Sound Advisory Services, who worked with the hospital. "We found a couple things," she said at a June 18 town hall sponsored by the American College of Physician Advisors (ACPA).

For starters, there was variation in clinical documentation and physician interpretations of a sepsis diagnosis. Some used Sepsis-2 criteria, others Sepsis-3 criteria and "some said we have no idea what sepsis is anymore," she recalled. "Some threw in the towel." Sepsis-2 is systemic inflammatory response syndrome due to infection and Sepsis-3 is life-threatening organ dysfunction caused by a dysregulated host response to infection.

Increasingly, the hospital's clinical validation denials were coming from a third-party auditor hired by the primary payer, said Boyd, chair of the ACPA Government Affairs Committee. "We saw a third party was auditing and denying cases that per the primary contracts should have been approved," she said. "It was an opportunity for the third party to have a better understanding of the contract."

Boyd gathered data because "it's more powerful than arguing about one denial at a time" and compared the denial rates to other payers. She had multiple conversations with the hospital, medical staff and payer about how to define sepsis with an eye on reducing the antagonism among them.

They settled on a definition of sepsis that's between Sepsis-2 and Sepsis-3. "We aren't going fully with" a definition of SIRS plus infection, but it's not limited to a sequential organ failure assessment score, where only certain types of organ dysfunction qualify.

With everyone on the same page, the payer automatically approved sepsis diagnoses that fit into their agreed-upon definition, Boyd said. "The insurer also had conversations with the third-party auditor and said, 'you need to follow the contract.'" Work is ongoing to have the payer review claims earlier, with a chance for discussion with the hospital before auto-denials of gray claims.

It took a year to accomplish this because of all the discussions between the hospital and its medical staff, as well as the hospital and the payer, but the hospital now gets only one-fifth as many sepsis denials as it used to.

"It's hard to see sometimes, but there are a lot of payers interested in collaboration," Boyd said. Although that may be hard to swallow with the slew of denials and peer-to-peer discussions, payers have an interest in easing the administrative burden of denials, reducing regulatory exposure and protecting their contracts with hospitals, she noted. "We all want to reduce administrative burden" and improve the patient and provider experience. ✧

NEWS BRIEFS

◆ **The HHS Office for Civil Rights (OCR) said June 18 that Spencer Gifts LLC Flexible Benefits and Welfare Benefit Plans (the Plan), the employer-sponsored group health plan of Spencer Gifts LLC, paid $450,000 in a settlement of potential HIPAA privacy and security violations.**[1] The settlement puts to rest an investigation opened by OCR after the plan filed a breach report on Jan. 24, 2022, in the wake of complaints from employees they were unable to connect to the virtual private network. The plan realized that in November 2021, "an unauthorized actor accessed the company's network and deployed ransomware, encrypting data on the company's systems, including servers storing the Plan's PHI, and demanding a ransom," OCR said. The protected health information (PHI) of 10,023 people was potentially affected. The plan didn't admit liability in the settlement.

◆ **A South Florida nursing school operator, Carleen Noreus, has pleaded guilty for her role in a scheme involving the sale of fake nursing diplomas and transcripts to people seeking nursing licenses and employment all over the U.S., the U.S Attorney's Office for the Southern District of Florida said June 18.**[2] The case is part of Operation Nightingale, which targeted fraudulent nursing diploma schemes operated by for-profit nursing schools in South Florida.

Endnotes

1 U.S. Department of Health and Human Services, Office for Civil Rights, "HHS' Office for Civil Rights Settles Ransomware Investigation with Health Plan," news release, June 18, 2026, https://bit.ly/4vUW4mo.

2 U.S. Department of Justice, U.S. Attorney's Office for the Southern District of Florida, "Owner of Two South Florida Nursing Schools Pleads Guilty in Fraudulent Nursing Diploma Scheme," news release, June 18, 2026, https://bit.ly/3Qu9UNN.