Report on
Medicare Compliance

Volume 34, Number 35 • September 29, 2025

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

Contents

HCCA

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

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

Stakes Are Raised for Monitoring Blocked Notes With Enforcement Alert; 'HIPAA Ties Into It'

After a child reveals he's being molested by a relative, the physician he told blocks the note in the patient portal to head off potential retribution from family members. Until child protective services intervenes, the physician isn't taking any chances, although he may unblock the note later. Note blocking in this situation is allowed by HIPAA, a reminder that the information blocking rule defers to the Privacy Rule under certain circumstances, something that's often misunderstood, a compliance officer said.

Providers may overlook the interaction between HIPAA and information blocking rules, said Brian Colonna, director of the compliance program at Renown Health in Nevada. "People forget how HIPAA ties into it," he noted. "If you're not following the HIPAA side of it, you could be subject to" information blocking penalties.

With HHS and the Office of Inspector General (OIG) turning up the heat on information blocking violations, it's a good time to nail down when blocking notes is acceptable. While the information blocking rule, which comes from the 21st Century Cures Act, essentially prohibits providers and other "actors" from standing in the way of patients' immediate access to their electronic health information (EHI) with some exceptions, HIPAA allows providers to block notes under certain circumstances.

continued on p. 6

Impending Federal Shutdown Threatens Telehealth Flexibilities, CMS Rules and Guidance

Hope is fading for an extension of COVID-19 telehealth flexibilities included in an embattled stopgap funding bill that would keep the government's lights on until Nov. 21. The looming failure of Congress to pass continuing appropriations legislation by Oct. 1 would end telehealth flexibilities on that date and partially shut down the federal government, affecting services considered discretionary. Layered on top is the existential threat to many federal employees because the Trump administration appears to be planning large-scale layoffs and possibly permanent terminations in the event of a shutdown.

"Everything is kind of at a standstill," said Teri Bedard, executive director of client & corporate resources at Revenue Cycle Coding Strategies. Although the U.S. House of Representatives passed a short-term funding bill Sept. 19, the Senate didn't follow suit.[1] Now the House is out of town, dimming the prospects of a deal between Democrats and Republicans before the government runs out of funding.

The likelihood of a shutdown is greater than it has been in recent years, said Claire Ernst, director of government relations and policy at Hooper, Lundy & Bookman. "We are at an impasse." But never say never. "It wouldn't be crazy for [a funding bill] to happen in a day or two," she noted.

This isn't your ordinary shutdown. The potential for mass layoffs accompanying it was outlined in a memo from Russell Vought, head of the Office of Management and

continued

Budget (OMB).[2] He told agencies "to consider Reduction in Force (RIF) notices for all employees in programs, projects, or activities (PPAs) that satisfy all three of the following conditions: (1) discretionary funding lapses on October 1, 2025; (2) another source of funding, such as H.R. 1 (Public Law 119-21) is not currently available; and (3) the PPA is not consistent with the President's priorities."

Although Medicare and Social Security payments are insulated from government shutdowns, a widespread RIF will affect the programs, Ernst said. For example, CMS has statutory deadlines for regulations, including the final Medicare Physician Fee Schedule (MPFS) and outpatient prospective payment system rules, which are due out Nov. 1. The proposed versions were already released late, so furloughs and layoffs could slow the process, Ernst said. But she added the 2026 MPFS rule just went to OMB for review. "They could have turned this around faster than usual, thinking that a government shutdown was likely."

Many CMS Activities Could Come to a Halt

To get a sense of how things might play out at CMS in the event of a shutdown, consider the contingency plan for fiscal year (FY) 2025.[3] It states that Medicare will continue "during a lapse in appropriations," including the Health Care Fraud and Abuse Control program and the Innovation Center. But activities that would have come to a halt are surveys, policy and rulemaking, contract oversight, outreach and education, and beneficiary casework.

A federal shutdown this time around would hit federal agencies harder because of the OMB's roadmap for the lapse in appropriations, which was first reported by Politico.[4] The OMB memo also states that "RIF notices will be in addition to any furlough notices provided due to the lapse in appropriation. RIF notices should be issued to all employees working on the relevant PPA, regardless of whether the employee is excepted or furloughed during the lapse in appropriations."

Consider Holding Telehealth Claims on Oct. 1

On the telehealth front, without another congressional extension, Medicare coverage will mostly revert to pre-COVID-19 times. Coverage will be limited to originating sites (e.g., hospitals, clinics, but not patient homes) in rural areas, with two exceptions: behavioral health and end-stage renal disease monthly assessments provided by telehealth to patients at home. Providers also will say goodbye to audio-only telehealth services and Acute Hospital Care at Home, among other things. Unrelated to telehealth, the geographic practice cost index will expire Sept. 30, which will result in relative-value payment reductions in certain states, Ernst said.

"We will wake up and there will no longer be telehealth flexibilities in place for a period of time and no one knows what that will look like," said attorney Thomas Ferrante, with Foley & Lardner LLP.

He predicts most providers will hold their claims and submit them if flexibilities return. Whether they ultimately will be able to bill for telehealth services provided on dates of service during a coverage lapse depends on whether legislation is retroactive, Ferrante noted. If the flexibilities don't materialize by Oct. 1, providers should look to CMS guidance (e.g., *MLN Connects*) on how to proceed, Ernst said.

Bedard noted there's a sliver of hope that Congress will pass a freestanding telehealth bill soon, such as the Permanent Telehealth from Home Act introduced in February.[5] Meanwhile, the Medicare telehealth cliffhanger doesn't necessarily affect commercial payer coverage, "although some commercial payers may mirror" what happens with Medicare. Providers should keep in mind that telehealth utilization isn't as high as perceived, according to data in the 2026 MPFS rule and earlier rules, Bedard said. "There's a disconnect in what people think is happening and what's reported."

Contact Ernst at cernst@hooperlundy.com, Bedard at teri.bedard@rccsinc.com and Ferrante at tferrante@foley.com. ✧

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.

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.

Endnotes

1 Continuing Appropriations and Extensions Act, 2026, H.R. 5371, 119th Cong. (2025), https://bit.ly/4mpbXfU.
2 Russell Vought memo, accessed September 26, 2025, https://bit.ly/4myC4ko.
3 U.S. Department of Health and Human Services, "Centers for Medicare and Medicaid Services: Summary of Activities that Continue," last reviewed, December 17, 2024, https://bit.ly/48G1vNE.
4 Sophia Cai, "White House to agencies: Prepare mass firing plans for a potential shutdown," Politico, updated September 24, 2025, https://bit.ly/47VCkGK.
5 Permanent Telehealth from Home Act, H.R. 1407, 119th Cong. (2025), https://bit.ly/4nrFdny.

AI May Be Force Multiplier for Compliance, but 'Human-in-the-Loop' Is Essential

Artificial intelligence (AI) can be a force multiplier for compliance, but it's not a replacement for the usual oversight and controls, including human reviews and traditional technology, experts say. It's a balancing act, with compliance officers having the opportunity to increase their effectiveness using AI tools while monitoring for the risks they introduce.

"You're not going to lose your jobs," said Melanie Standish, senior director at FTI Technology. "The human-in-the-loop factor is critical every step of the way." For example, if compliance overrelies on AI and doesn't check the work, hallucinations may distort audit findings. "The outcome of this is not great if you're not watching what the output is," she noted.

Some of AI's potential for compliance departments is available now and some is "more future casting," Standish said at SCCE's Compliance & Ethics Institute Sept. 17. "You can potentially develop risk forecasting models that will help you be able to get more of a prediction concept in place and that will help you move the compliance function from reactive to more of a strategic partnership with business leadership."

For example, AI helps compliance with reviews, but there are caveats, said Tom Barce, managing director of FTI Technology. To evaluate whether an organization's invoices were valid and should have been paid, Barce fed a package of them into an AI tool along with supporting material (e.g., time sheets, agreements). Could a large language model (LLM) answer the question? Barce gave the LLM a complicated prompt—which is helpful to AI tools rather than distracting—explaining he is a sophisticated compliance officer and asking whether the invoices were legit. It took only one minute for the LLM to respond that every invoice matched with timesheets and the contract rates and therefore payments were appropriate. Its use illustrates how a compliance team can supplement their resources with an AI assistant.

But Barce added a "plot twist" that reinforces why compliance must be on AI overwatch. He created a "fictional fraud scheme that would potentially bypass some compliance controls" with a phony company and altered materials, and yet the invoices still passed muster with the LLM. "You can lean into using generative AI to evaluate content at a greater scale than you were able to, but at the same time you need traditional methods that are human centers, supported by traditional technology" (e.g., ensuring people who sign contracts are real humans and that the address isn't fabricated), Barce said. "You won't use LLM in place of your existing compliance reviews, but you will supplement them."

Guarding Against 'Ethical Drift'

For example, AI can assist with oversight of the hundreds or thousands of vendors that have contracts with a typical hospital or health system. "If you're thinking about the ability to analyze contracts, AI provides a notable opportunity, Barce said. "I have heard from every contract owner, especially in the privacy arena, that there are more regulations that impact their contracts every day" and they can't keep up with the "clause analysis." AI provides the capacity to risk rank contracts with, for example, surgical providers. "You are using AI to shorten the time to value and that's what managers want while compliance and counsel need to control the risk," Barce said.

But there are many risks associated with AI and the guardrails don't always come easy. For example, in terms of bias, when Barce asked an AI tool in use at a large provider to generate an image of lawyers and technologists collaborating on a project, it produced a picture of white, grey-haired men. "When we examine bias, we try to examine how an engine is performing relative to a relevant population," he said. "It's one way to measure the risk but it's an endless discussion."

With hallucinations, keep in mind it may not be the AI generating inaccurate information, Barce said. Often the hallucination stems from a bad prompt, such as a poorly worded question or old policy fed into the system.

With data security, organizations may have a false sense of security with a contractual agreement that the LLM will only be trained using their prompts and data. But "it's impossible to keep that stuff off the perimeter of the model," Barce said. Organizations may need technology to monitor what goes into the LLM and policies and procedures to prevent employees from letting outside information in.

AI tools also should be routinely audited to ensure "there is no ethical drift," Standish said. "You can't set it and forget it." Suppose an employee asks a compliance training chatbot whether it's OK to query patients about certain sensitive

health issues. The chatbot should give the employee the same ethically sound answer today as it does in a year. The answer would only drift if there's been a policy or regulatory change.

Beware the Use of Shadow AI

Shadow AI, which refers to employees using AI tools (e.g., ChatGPT) without approval, also requires oversight. "Employees will use AI whether you like it or not," Standish said. Without a "walled garden" or internal AI, employees may put their own AI tool into action. "You don't want it to go externally," she said, with employees potentially inputting PHI or proprietary information (see box, p. 5).[1] Employees' unsanctioned use of AI isn't an easy thing to track, but organizations should have policies and procedures and staff training. "We can't put our heads in the sand and pretend they don't exist," Standish noted. "You can partner with IT and cybersecurity so you know what's leaving proprietary systems and going offline and make sure policies are in place to communicate with your team."

Also, IT can monitor website activity and look at what LLMs are in use, Barce said. "Training and telling people what they can and can't do with AI is key," he noted. Imagine this scenario: a well-meaning employee testifies under oath that a document written by AI led to the improper disclosure of protected health information. "Some liability will follow," Barce said. "The patient disclosure will come up in a deposition and the employee or an executive will be presented with it and they will say, 'That was written by AI brand X.'" They will be asked when it was written, what prompt generated the language, who verified its accuracy, and whether the organization has an AI policy and a human was in the loop. Things could go downhill from there in a lawsuit.

Standish also warned of looming fraud risks. People are already trained to identify phishing email in their inbox, but cyberthreats using AI are another story. They include videos purporting to be your CFO to discuss a contract you expect from a vendor. "With any advancement in tech, it's not just angels on our shoulders taking advantage of that," Standish said. "It's bad actors and they will become extremely sophisticated in making AI work for them." They could infiltrate compliance programs and modify elements of them "without you being aware. You need to develop internal partnerships and try to think one step ahead of bad actors and how risks may come down the pike and how you can mitigate them."

Contact Standish at melanie.standish@fticonsulting.com and Barce at thomas.barce@fticonsulting.com. ✧

Endnotes

1 Nina Youngstrom, "Tips for Managing the Risks of Shadow Artificial Intelligence (AI)," *Report on Medicare Compliance* 34, no. 35 (September 29, 2025): 5.

Hospitals May Have to Return Money to Patients From PRF Balance Billing

Hospitals should brace for the possibility of returning money to patients who were overcharged for COVID-19 services in connection with the Provider Relief Fund (PRF). According to a report from the HHS Office of Inspector General (OIG) posted Sept. 23, a majority of hospitals audited didn't jump through the balance-billing hoop required to accept PRF money during the COVID-19 public health emergency (PHE).[1]

But it may be easier said than done for hospitals to repay patients for balance billing after the fact. Patients may be hard to locate and calculating their refund could be tricky, said attorney Judy Waltz, with Foley & Lardner LLP.

OIG reviewed balance billing at 25 hospitals and concluded that 17 didn't comply or may not have complied with balance billing requirements, which was one of the terms and conditions of taking PRF money. Hospitals were prohibited from collecting out-of-pocket payments from insured COVID-19 patients that were higher than the patients would have paid if treated at an in-network hospital. In the event hospitals couldn't nail down the in-network rate, they were expected to use the ACA Marketplace out-of-pocket limitation, according to the report, which is the latest in a series of OIG audits of compliance with PRF requirements.

OIG recommended that the HHS Health Resources and Services Administration (HRSA) determine whether the audited hospitals have repaid patients in connection with balance billing and perform postpayment reviews of hospitals generally for compliance with the PRF requirement. HRSA agreed and said it will ask hospitals to repay patients.

This is a sad turn of events considering that mistakes happened against the backdrop of a pandemic, Waltz said. "For the most part, providers were really jumping in for the interests of public health in a very chaotic time, and some of them (as well as HRSA) didn't get it quite right," she said. "There is no doubt there was some fraud going on, and that should definitely be prosecuted, but most of these findings sound to me like some sloppiness in a very chaotic time that was not intentional fraud."

Waltz anticipates false claims lawsuits premised on noncompliance with the PRF terms and conditions, although OIG doesn't paint balance billing as fraud and some HRSA audits "have at least preliminarily characterized provider errors as opportunities for improvement rather than overpayments." Meanwhile, HRSA audits of the COVID-19 Uninsured Program (UIP) may have dried up because a lot of HRSA staff has been laid off, she said—even though a 2023 OIG audit found almost $784 million in improper UIP payments to

providers between March 1 and Dec. 31, 2020.[2] Overall, though, she expects COVID-19 fraud to continue to be a focus of auditors and enforcers and potentially whistleblowers.

Repaying Patients May Be an Uphill Battle

Although HRSA agreed to tell hospitals to return money to patients, that's often hard to do, especially because out-of-network hospitals that treated patients for COVID-19 probably don't have an ongoing relationship with patients, Waltz said. Patients may have moved since then or died, or some may have married and changed their names. It will require manual efforts to find many of the patients, "and that's after the hospital now goes back to figure out what actually should have been charged to/collected from the patient," she noted.

According to OIG, hospitals that accepted PRF money had to agree to terms and conditions, including the balance-billing requirement. To comply with this requirement, hospitals would bill patients in one of four ways: hospitals didn't bill patients at all because they waived the copays; hospitals didn't bill patients because insurers waived the copays; hospitals billed the in-network cost-sharing amount; or the hospital couldn't pin down the amount so it billed the ACA Marketplace out-of-pocket limitation.

For the audit, OIG chose a nonstatistical sample of 25 hospitals that admitted four or more out-of-network patients who had a positive COVID-19 test result or a COVID-19 diagnosis code. The findings: 17 hospitals didn't comply (or may not have complied) with the balance billing requirement. They variously billed patients even though their insurers waived copays, billed insurers the out-of-network rate and billed above the ACA marketplace limit, among other errors.

Hospitals laid some of the blame for balance billing at the door of HRSA, which managed the PRF, because it didn't provide adequate compliance guidance. But running the PRF show was outside HRSA's traditional wheelhouse, Waltz said.

Contact Waltz at jwaltz@foley.com. ✧

Endnotes

1 U.S. Department of Health and Human Services, Office of Inspector General, *Seventeen of Twenty-Five Selected Hospitals Did Not Comply or May Not Have Complied With the Provider Relief Fund Balance Billing Requirement*, A-02-22-01018, September 2025, https://bit.ly/46kXRr8.

2 Christi A. Grimm, *HRSA Made COVID-19 Uninsured Program Payments to Providers on Behalf of Individuals Who Had Health Insurance Coverage and for Services Unrelated to COVID-19*, U.S. Department of Health and Human Services, Office of Inspector General, A-02-21-01013, July 2023, https://bit.ly/46Stngi.

Tips for Managing the Risks of Shadow Artificial Intelligence (AI)

Shadow artificial intelligence (AI), which refers to employees use of AI tools (e.g., ChatGPT) without approval, requires oversight (see story, p. 3),[1] according to Melanie Standish, senior director at FTI Technology, and Tom Barce, managing director at FTI Technology. Contact Standish at melanie.standish@fticonsulting.com and Barce at thomas.barce@fticonsulting.com.

Employees Use Shadow AI to Generate or Optimize Code for Internal Systems

Employees use unauthorized AI assistants to write or modify code, which may bring efficiencies to development projects, but also significant risks.

USE CASE
- Employees use public AI tools to create or modify code snippets that are then deployed internally to systems, pipelines or as workarounds with IT or security authorization

TACTICS
- Monitor repositories, internal wikis or productivity platforms for "rapid" or unexplained code proliferation
- Educate employees on software development vs. acceptable business automation
- Implement approval workflows for new macros, code snippets, or AI-generated automations
- Apply code-scanning tools to flag AI-written or copy-pasted code with potential IP concerns
- Limit external AI plugins or browser extensions in enterprise environment

BENEFITS
- Using AI tools to write code can speed up efficiencies and enable employees to innovate without waiting for formal development cycles

RISKS
- AI-generated code can contain security vulnerabilities or trojan-style attributes
- Code can be copyrighted and using it without authorization can be an IP violation
- Code is untraceable or unsupported if employee leaves firm
- Regulatory risk

RISK MITIGATION
- Require all code used in internal systems, including code snippets, go through light peer review
- Establish approved AI coding tools with enterprise licensing or audit capabilities
- Deploy runtime security or observability tools to flag risky behavior
- Include GenAI in secure software development lifecycles (SSDLC)

Endnotes

1 Nina Youngstrom, "AI May Be Force Multiplier for Compliance, but 'Human-in-the-Loop' Is Essential," *Report on Medicare Compliance* 34, no. 35 (September 29, 2025): 3.

Tip Sheets on Note Blocking

Here are two tip sheets on note blocking to help employees comply with information blocking and related HIPAA requirements (see story, p. 1).[1] They were developed by Renown Health in Nevada. Contact Brian Colonna, director of the compliance program, at brian.colonna@renown.org.

Note Blocking

What is Note Blocking?

Blocking the disclosure of any information that would otherwise be released to the patient under HIPAA. **The act of blocking Electronic Health Information (EHI) from a patient should be rare, not standard practice. Each action of note blocking must be assessed on its own.**

Why is releasing EHI important?

- It is important that patients and healthcare providers have access and transparency to all their EHI.
- Patients have the right to view all progress notes, telephone encounter notes, history and physical notes, consult notes, procedure notes, discharge summary, etc.
- Any interference with its access, exchange, or use implicates the information-blocking provision.
- HIPAA specifically states that a note cannot be blocked because it would upset the patient or because the patient may not understand the information.

When can I block a note?

- Short-term block while a protective agency is notified (CPS/EPS/law enforcement).
- The information was provided by a third party other than the patient or healthcare provider.
- There is a potential for harm to the patient or another party if the information were disclosed.
  - ◊ This includes threats of physical harm to healthcare workers or their families.
- The information is expected to be used in litigation.

If you are unsure of when blocking a note is appropriate, compliance is available to help. Email us at xxxx@xxxx.org.

Behavioral Health Note Blocking

What is Note Blocking?

Blocking the disclosure of any information that would otherwise be released to the patient under HIPAA. **The act of blocking Electronic Health Information (EHI) from a patient should be rare, not standard practice. Each action of note blocking must be assessed on its own.**

Why is releasing EHI important?

- It is important that patients and healthcare providers have access and transparency to all their EHI.
- Patients have the right to view all progress notes, telephone encounter notes, history and physical notes, consult notes, procedure notes, discharge summary, etc.
- Any interference with its access, exchange, or use implicates the information-blocking provision.
- HIPAA specifically states that a note cannot be blocked because it would upset the patient or because the patient may not understand the information.

The "psychotherapy" note type is not releasable to the patient or other providers unless the documenting provider approves the disclosure. This note type is not considered part of the medical record and should not be commingled with the progress note type.

When can I block a note?

- Short-term block while a protective agency is notified (CPS/EPS/law enforcement).
- The information was provided by a third party other than the patient or healthcare provider.
- There is a potential for harm to the patient or another party if the information were disclosed.
  - ◊ This includes threats of physical harm to healthcare workers or their families.
- The information is expected to be used in litigation.

If you are unsure of when blocking a note is appropriate, Compliance is available to help. Email us at xxxx@xxxx.org.

Endnotes

1 Nina Youngstrom, "Stakes Are Raised for Monitoring Blocked Notes With Enforcement Alert; 'HIPAA Ties Into It,'" Report on Medicare Compliance 34, no. 35 (September 29, 2025): 1.

Stakes Are Raised for Monitoring Blocked Notes

continued from page 1

For two years, Renown's compliance team has been tracking blocked notes and engaging with the clinicians who write them "to understand why the information was blocked and provide education when the reasoning does not appear to align with HIPAA," Colonna said (see box above).[1] For example, imminent physical harm is a legitimate reason for note blocking under HIPAA, and the information blocking rule has an exception for patient harm as well. But worrying the patient will be upset by a note in the patient portal or won't understand it aren't reasons to block a note, he explained.

Although incidents of note blocking have steadily declined at Renown, some worrisome risks persist. One is whether a department has a standing policy to block all notes in certain areas, such as abuse allegations or behavioral health. "If you have a policy that says everything of this type is automatically blocked, you have a problem, even if there's a valid reason," Colonna said. "They have to be reviewed case by case." For example, a clinician could block a note from a father who expresses concern about his son's drinking, but it wouldn't be compliant to have a policy blocking notes every time a friend or family member calls the clinician about a patient's alcohol abuse.

Enforcement Front Was Quiet Until Now

All was quiet on the enforcement front until OIG on Sept. 4 posted an Enforcement Alert on Information Blocking, which came a day after HHS vowed to increase resources in this area.[2]

The enforcement alert came down about two years after OIG finalized an information blocking enforcement rule for health information networks, health information exchanges, developers of certified health information technology and entities offering certified health IT,[3] and CMS more than a year ago did the same for providers.[4] These "actors" are at the heart of the information blocking regulation itself, which was implemented by the HHS Office of the National Coordinator for Health Information Technology and took effect April 5, 2021. According to the rule, any action or inaction that knowingly interferes with the access, exchange or use of electronic health information is prohibited unless it's required by law or falls into one of eight exceptions. The exceptions include information blocking if the physician believes sharing the information would cause patient harm or information blocking to prevent interference with the privacy or the security of protected health information (PHI).

Pre-information blocking, providers withheld information because they wanted to review it before talking to patients, but sometimes test results fell through the cracks, he explained. Now they're supposed to be released immediately with or without the physician reviewing them.

The question is, do patients have to ask for it or simply log into their patient portal? "We went extreme one way and send out the results immediately," Colonna said. Final notes also are released to MyChart as soon as they're signed by the provider. The risk is that patients may misinterpret notes or test results they see before talking to the physician. To try to tamp that down, Renown includes a warning in MyChart that patients may be seeing results before their provider and encouraging them to reach out with questions.

At the same time, HIPAA makes allowances for blocking notes. "The Privacy Rule contemplates circumstances under which covered entities may deny an individual access to PHI and distinguishes those grounds for denial which are reviewable from those which are not," according to HHS.[5] The "unreviewable" reasons for denial are situations involving psychotherapy notes; information assembled for legal proceedings; some information in the hands of clinical labs; some requests by inmates; information from third parties who promise confidentiality; and information for research. "Reviewable"

CMS Transmittals and *Federal Register* Regulations, Sept. 19-25, 2025

CMS Transmittals

Pub. 100-03, Medicare National Coverage Decisions

- NCD 20.37 - Transcatheter Tricuspid Valve Replacement (TTVR), Trans. 13427 (September 22, 2025)

Pub. 100-04, Medicare Claims Processing

- Transcatheter Tricuspid Valve Replacement (TTVR), Trans. 13427 (September 22, 2025)
- Implement Operating Rules - Phase III Electronic Remittance Advice (ERA) Electronic Funds Transfer (EFT): Committee on Operating Rules for Information Exchange (CORE) 360 Uniform Use of Claim Adjustment Reason Codes (CARC), Remittance Advice Remark Codes (RARC) and Claim Adjustment Group Code (CAGC) Rule - Update from Council for Affordable Quality Healthcare (CAQH) CORE, Trans. 13420 (September 22, 2025)
- October 2025 Update of the Hospital Outpatient Prospective Payment System (OPPS), Trans. 13425 (September 22, 2025)
- 2026 Annual Update of Healthcare Common Procedure Coding System (HCPCS) Codes for Skilled Nursing Facility (SNF) Consolidated Billing (CB) Update, Trans. 13426 (September 22, 2025)
- Revised Start Date of the Expanded Outlier Reconciliation Criteria for the Inpatient Prospective Payment System (IPPS) and Long Term Care Hospital (LTCH) PPS, Trans. 13428 (September 22, 2025)
- October 2025 Update of the Ambulatory Surgical Center [ASC] Payment System, Trans. 13429 (September 22, 2025)

Pub. 100-20, One-Time Notification

- Patient Driven Payment Model (PDPM) Corrections to Interrupted Stay Edits to Include Prospective Payment System (PPS) Swing Bed Providers, Trans. 13433 (September 25, 2025)

Federal Register

Final rule

- Medicare and Medicaid Programs; Contract Year 2026 Policy and Technical Changes to the Medicare Advantage Program, Medicare Prescription Drug Benefit Program, Medicare Cost Plan Program, and Programs of All-Inclusive Care for the Elderly (PACE)—Finalization of Format Provider Directories for Medicare Plan Finder, 90 Fed. Reg. 45,140 (September 19, 2025)

Semiannual regulatory agendas

- HHS Semiannual Regulatory Agenda, 90 Fed. Reg. 45,510 (September 22, 2025)
- Department of Justice Semiannual Regulatory Agenda, 90 Fed. Reg. 45,532 (September 22, 2025)

grounds for denial are disclosures that could endanger the patient or others; when the PHI "refers to another and disclosure is likely to cause substantial harm"; and "requests made by a personal representative where disclosure is likely to cause substantial harm."

Unlike unreviewable notes, reviewable notes may be appealed by patients to another clinician who wasn't involved in the note blocking. "We typically talk with the author of the note and their leader," Colonna said. "We understand we aren't clinical and we want clinical folks to make the decision."

Reports Identify Problems With Blocked Notes

Blocking notes requires an explanation, Colonna said. Before physicians and other authors of the notes close them, they see a pop up that asks them to check a box if they want to block a note. When that's the case, clinicians pick from a list of reasons to explain the note blocking based on HIPAA and the information blocking exceptions, with the former pre-empting the latter, Colonna said.

Physicians have a binary choice between blocking the whole note or none of it. In the event physicians want to block an excerpt of the note, they would put it into a second note and only block it.

Renown's compliance team runs a monthly report on blocked notes and meets with authors of notes to talk "about why the note was blocked and provide education," Colonna said. Behavioral health providers tend to do a lot of note blocking and "we don't always understand why." Although psychotherapy notes are blocked under HIPAA, they're not considered part of the medical record. Psychotherapy notes are the therapist's subjective observations (e.g., Jane was disheveled when she came in today and looks like she's struggling with self-care) and distinct from progress notes, which are the basis for billing (e.g., We may need to make adjustments to Jane's plan of care because she isn't showing improvement). Epic already has a psychotherapy note type "and we educate providers to use the note in Epic for private musings," Colonna said.

Another risk identified is that notes sent to the patient portal contained the full name of the author. With the increase in violence against health care workers, Renown non-provider staff were blocking notes because they were afraid of patients having their full names. "It's an area of growing concern when we look at violence against health care workers," he said. But fearing angry patients isn't a justification for blocking the note. To make clinicians more comfortable, Renown releases MyChart notes with the first name and first initial of their last name. It takes the edge off although patients can see the clinician's full name if they request medical records from the health information management department.

Contact Colonna at brian.colonna@renown.org. ✧

Endnotes

1 Nina Youngstrom, "Tip Sheets on Note Blocking," *Report on Medicare Compliance* 34, no. 35 (September 29, 2025).
2 U.S. Department of Health and Human Services, Office of Inspector General, "Information Blocking," last updated September 4, 2025, https://bit.ly/4645u5i.
3 Grants, Contracts, and Other Agreements: Fraud and Abuse; Information Blocking; Office of Inspector General's Civil Money Penalty Rules, 88 Fed. Reg. 42,820 (July 3, 2023), https://bit.ly/42KR8V9.
4 21st Century Cures Act: Establishment of Disincentives for Health Care Providers That Have Committed Information Blocking, 89 Fed. Reg. 54,662 (July 1, 2024), https://bit.ly/3KFkyOb.
5 U.S. Department of Health and Human Services, Office for Civil Rights, "The HIPAA Privacy Rule's Right of Access and Health Information Technology," accessed September 25, 2025, https://bit.ly/4myhII2.

NEWS BRIEFS

◆ **The U.S. Department of Justice (DOJ) said Sept. 25 it has created a new office in the Civil Division dubbed the Enforcement & Affirmative Litigation Branch**.[1] DOJ said the new office will "strengthen the Civil Division's ability to advance the Department's enforcement priorities, including protecting women and children from pharmaceutical companies, health care providers, and medical associations profiting off of false and misleading claims related to so-called gender transition, and ending sanctuary jurisdiction laws, policies, and practices that impede federal immigration enforcement and make Americans less safe in their communities." There will be two sections in the new branch. The Enforcement Section will focus on protecting consumers "from unfair and deceptive trade practices of the largest technology companies in the world, defective consumer goods imported from China, or false and misleading claims about drugs and dietary supplements manufactured by pharmaceutical companies." DOJ said the Affirmative Litigation Section will represent the United States by suing states, municipalities and private entities that hinder federal policies.

◆ **Health First Urgent Care in Richland and Pasco, Washington, has agreed to pay $2,807,729 to settle allegations of fraudulently billing Medicare and Medicaid for diagnostic tests, the U.S. Attorney's Office for the Eastern District of Washington said Sept. 24**.[2] The urgent care center allegedly unbundled polymerase chain reaction respiratory and urinary tract infection panel testing.

Endnotes

1 U.S. Department of Justice, Office of Public Affairs, "The Department of Justice Creates New Civil Division Enforcement & Affirmative Litigation Branch," news release, September 25, 2025, https://bit.ly/4gEzKae.
2 United States Attorney's Office of the Eastern District of Washington, "Tri-Cities Urgent Care Clinic Agrees to Pay $2.8 Million to Resolve Claims of Overbilling for Diagnostic Tests," news release, September 24, 2025, https://bit.ly/4nVC1Ax.