June 10, 2025

Submitted via the Federal eRulemaking Portal: http://www.regulations.gov

Dr. Mehmet Oz
Administrator
Centers for Medicare and Medicaid Services
Department of Health and Human Services
7500 Security Boulevard
Baltimore, MD 21244

RE: Medicare Program; Hospital Inpatient Prospective Payment Systems for Acute Care Hospitals and the Long-Term Care Hospital Prospective Payment System and Policy Changes and Fiscal Year 2026 Rates; Requirements for Quality Programs; and Other Policy Changes [CMS-1833-P]

Dear Dr. Oz:

The College of Healthcare Information Management Executives (CHIME) appreciates the opportunity to comment on the Department of Health and Human Services' (HHS) Centers for Medicare and Medicaid Services (CMS) hospital inpatient prospective payment system (IPPS) proposed rule for fiscal year (FY) 2026, as published in the *Federal Register* on April 30, 2025 (Vol. 90, No. 82).

Background

CHIME is an executive organization dedicated to serving chief information officers (CIOs), chief medical information officers (CMIOs), chief nursing information officers (CNIOs), chief innovation officers (CIOs), chief digital officers (CDOs) and other senior healthcare IT leaders. With more than 3,000 individual members in 58 countries and two U.S. territories and 200 CHIME Foundation healthcare IT business and professional service firm members, CHIME and its three associations provide a highly interactive, trusted environment enabling senior professional and industry leaders to collaborate, exchange best practices, address professional development needs, and advocate for the effective use of information management to improve the health and care in the communities they serve.

Key Recommendations and Takeaways

In our comments, CHIME provides responses to address the proposals included in this Notice of Proposed Rulemaking (NPRM). Specifically, we are providing comments on proposed new requirements and revision of existing requirements for eligible hospitals and critical access hospitals (CAHs) participating in the Medicare Promoting Interoperability (PI) Program.

Additionally, we offer feedback and recommendations to constructively improve the final rule. CHIME believes the following areas are especially important for CMS to consider when finalizing the provisions in this important proposed rule, and our detailed recommendations are included below:

Proposed Changes to the Medicare Promoting Interoperability (PI) Performance Program

- CHIME opposes the proposal to modify the Security Risk Analysis Measure beginning with the EHR reporting period in calendar year (CY) 2026.
    - We believe that the proposal would add significant additional financial burden on our members, without improving or strengthening their cybersecurity posture.
    - CHIME members are extremely concerned that diverting resources and funds from meaningful cybersecurity investments is a threat to national security and patient safety.
- CHIME appreciates CMS and the Assistant Secretary for Technology Policy/Office of the National Coordinator for Health IT (ASTP/ONC) for undertaking the update of the SAFER Guides; our members remain staunch champions for promoting safety and the safe use of EHRs.
    - We respectfully request that CMS consider a step-wise approach (i.e., glidepath) before requiring our members to attest to the 2025 SAFER Guides.
    - At minimum, CMS should provide an additional two-year period – without penalty – before a review and annual self-assessment of the 2025 SAFER Guides is required for eligible hospitals and CAHs to attest "yes" to the SAFER Guides measure.
    - Eligible hospitals and CAHs have grown familiar and spent millions of dollars and hours to complete the complex process of attesting to each of the nine 2016 SAFER Guides; therefore, we recommend that CMS offer flexibility with future attestation requirements.
- It is critical that regulations do not inadvertently create overly duplicative requirements, penalize healthcare providers unfairly, and add burden.

By establishing a meaningful and continuous opportunity for stakeholder engagement – particularly from those with specialized expertise in healthcare information technology (IT) – we believe that CMS will benefit from informed, pragmatic, and technically sound input. Such engagement throughout the policy development and implementation process is essential to ensuring that resulting final regulations are both operationally feasible and aligned with the complex realities of modern healthcare delivery.

Proposal To Modify the Security Risk Analysis Measure Beginning With the EHR Reporting Period in Calendar Year (CY) 2026

CMS is proposing "to modify the Security Risk Analysis measure to require eligible hospitals and CAHs to attest "yes" to having conducted security risk management as required under the HIPAA Security Rule at 45 CFR 164.308(a)(1)(ii)(B) beginning with the EHR reporting period in CY 2026."

CMS states, "While we are proposing to require eligible hospitals and CAHs to attest "yes" to having conducted security risk management, the costs associated with performing security risk management required under the HIPAA Security Rule are currently approved under OMB control number 0945-0003 (expiration date July 31, 2027). We do not believe this provision results in any additional economic impacts."

CHIME members are deeply concerned that duplicative security risk management requirements – under both HIPAA and CMS programs – are in direct conflict with this Administration's stated goal of reducing regulatory burden and instead redirect limited healthcare system resources away from real cybersecurity improvements.

CMS is proposing to require eligible hospitals and CAHs to attest "yes" to having conducted security risk management under the Medicare PI Program, which would be a new requirement that is duplicative of obligations already mandated under the HIPAA Security Rule[1] and approved under OMB Control Number 0945-0003. Imposing parallel requirements, particularly under separate statutory authorities (e.g., HIPAA and the Medicare PI Program), does not align with the Administration's commitment to reducing unnecessary regulatory burden, as outlined in Executive Order 14192, titled "Unleashing Prosperity Through Deregulation," and reinforced by CMS's Request for Information (RFI) *Unleashing Prosperity Through Deregulation of the Medicare Program*[2] – which was released in tandem with this proposed rule.

Hospitals and healthcare systems are already subject to comprehensive and enforceable security risk assessment obligations under HIPAA, enforced by HHS' Office for Civil Rights (OCR). These assessments must be conducted routinely, documented, and updated as part of a broader security management process. Introducing an additional attestation requirement under a distinct CMS program – backed by the risk of penalties or audit failure – amounts to regulatory layering, not streamlining.

Moreover, imposing parallel but independently administered requirements increases the likelihood of conflicting interpretations and audit standards across federal agencies, such as CMS and the Office of Inspector General (OIG). This divergence creates legal uncertainty for regulated entities – hospitals and healthcare systems – and heightens the risk of inconsistent enforcement actions. Providers could face differing 'grading scales' or thresholds of compliance under separate audit regimes, despite operating in good faith under a unified cybersecurity posture.

Of notable concern, this redundancy has real operational costs which CMS does not account for in this proposed rule. For example, CHIME members would have to dedicate additional time and resources to interpret, align, and document compliance under multiple overlapping frameworks; develop new internal audit trails and processes solely for CMS programmatic reporting (distinct from HIPAA compliance); and face potential financial penalties or reputational harm from discrepancies in reporting, even when security risk assessments have been properly conducted under HIPAA. Therefore, CHIME members strongly oppose this proposed requirement.

Moreover, the Paperwork Reduction Act (PRA)[3] prohibits duplicative federal information collections unless justified by clear, demonstrable benefit. Requiring hospitals to re-attest to security risk management under the Medicare PI Program – without substantive difference from HIPAA's requirements – may run afoul of the PRA's purpose, particularly if the only function of the CMS attestation is enforcement signaling.

Many health systems operate multiple electronic health record (EHR) platforms across their enterprise, and the assumption that all providers rely on a single, unified EHR does not reflect the operational reality. As a result, attesting to the proposed cybersecurity requirements across a multi-EHR environment introduces significant technical complexity and risk, making it difficult for providers to do so safely and without issue.

CMS's proposal to layer a duplicative attestation on top of existing HIPAA requirements does not reduce regulatory burden – it increases it. This requirement forces hospitals to divert limited resources away from proactive strengthening of their cybersecurity posture in favor of

[1] 45 C.F.R. §§ 164.302–164.318
[2] Medicare Regulatory Relief | CMS
[3] 44 U.S.C. § 3506(c)(3)(B))

compliance bureaucracy, contrary to the stated intent of both HIPAA's security standards and the CMS Medicare PI Program.

Additionally, in this proposed rule, under the "Background on the Security Risk Analysis Measure" regarding the "Proposal to Modify the Security Risk Analysis Measure," CHIME is concerned with CMS's rationale for modifying the Security Risk Analysis (SRA) measure under the PI Program. Specifically, CMS cites the Biden administration's proposed rule *HIPAA Security Rule to Strengthen the Cybersecurity of Electronic Protected Health Information* (90 FR 898) as justification for its revised framing of the SRA measure.

CMS states, "The Health Insurance Portability and Accountability Act of 1996 (HIPAA), as implemented in the HIPAA Security Rule (45 CFR part 160 and subparts A and C of 45 CFR part 164) contains, among other things, the administrative safeguards that covered entities and business associates (45 CFR 160.103) must implement, such as the standard and implementation specifications for security management process." Within this statement, CMS includes a footnote citation (numbered 399 in the proposal) after the phrase "in the HIPAA Security Rule," which states:

> ***The Department has proposed to modify the HIPAA Security Rule to strengthen the cybersecurity of electronic protected health information, including proposals to revise the existing requirements to conduct a risk analysis and risk management. See generally HIPAA Security Rule To Strengthen the Cybersecurity of Electronic Protected Health Information proposed rule (90 FR 898). [emphasis added]***

CHIME is alarmed that CMS may by reliant on the Biden administration's proposed rule titled *HIPAA Security Rule To Strengthen the Cybersecurity of Electronic Protected Health Information* (90 FR 898), as cited in the footnote accompanying its background discussion. **If this is accurate, the proposal is procedurally flawed and raises substantial legal concerns.** The proposed rule referenced is not final and has not been adopted by HHS as binding regulation. As such, it does not have the force or effect of law and cannot serve as a legally sufficient basis for regulatory modification or reinterpretation of current program requirements.

It is a well-established principle of administrative law that proposed rules do not create enforceable obligations or justify the reinterpretation of existing legal requirements. Courts have consistently held that "a proposed rule is a tentative position, not a final agency action."[4] Under the Administrative Procedure Act (APA)[5], agencies may not implement or enforce policy based on speculative regulatory outcomes. In other words – agencies are not permitted to act as though proposed rules are final or to rely on them as if they reflect binding policy.

CHIME and numerous other stakeholders submitted detailed comments to OCR requesting that this proposal be rescinded due to a multitude of operational, financial, technical, and legal concerns. The proposal remains unresolved, with no final rule issued. CMS's decision to rely on an unfinished rulemaking process is not only procedurally inappropriate – it may also prejudice the outcome of OCR's ongoing rulemaking, undermining the transparency and integrity required under the APA.

---

[4] *See Nat'l Wildlife Fed'n v. U.S. Army Corps of Engineers*, 170 F. Supp. 3d 6, 15 (D.D.C. 2016)
[5] 5 U.S.C. § 553(b)–(d)

Moreover, our members – along with the Healthcare and Public Health Sector Coordinating Council (HSCC) Cybersecurity Working Group (CWG)[6] – have formally requested that HHS rescind the proposed HIPAA Security Rule, due to the above concerns raised by stakeholders across the healthcare sector. Until such time as HHS completes the rulemaking process, including responding to public comment and issuing a final rule consistent with the APA, the proposal remains just that – a proposal. Or, as HSCC CWG has requested, the Trump Administration initiate a one-year consultative process with leaders of the healthcare sector as an alternative to the proposal – CMS cannot reasonably or legally predicate changes to existing program requirements on a rule that is neither final nor adopted.

Therefore, CHIME strongly urges CMS to not move forward with this proposal and remove any reliance on the referenced proposed rule from this regulatory action. To do otherwise would not only undermine the integrity of the rulemaking process but also create legal risk by preemptively incorporating elements of a non-final regulation into an existing and enforceable CMS program framework.

CMS cannot incorporate speculative regulatory changes through the back door of an unrelated program update. Doing so would unlawfully conflate separate rulemaking processes, violate fundamental principles of administrative procedure, and expose the agency to potential legal challenge. CHIME believes that CMS must refrain from basing substantive changes to the SRA measure on a non-final OCR proposal that is still under review and subject to significant opposition.

Furthermore, as CHIME discusses in both our letter to the Administration Requesting HIPAA Proposal Rescission as well as our comments on the proposal submitted to Regulations.gov, the proposal directly conflicts with existing law. The proposed rule imposes numerous new mandates without acknowledging P.L. 116-321, which President Trump signed into law on January 5, 2021.

This law – supported by CHIME – explicitly requires HHS to consider a regulated entity's adoption of recognized security practices when enforcing the Security Rule. Yet, the proposed regulation fails to address or incorporate that legal requirement, directly contradicting existing statute. By overlooking this statutory framework, the proposed rule fails to account for existing legal provisions that encourage proactive cybersecurity measures, thereby creating potential misalignment with established federal policy. Our members strongly believe that we need to continue with this approach, rather than impose unreasonable mandates. Given these deficiencies, CHIME continues to urge HHS to focus on policies that support flexible, evidence-based security frameworks that align with industry best practices and the rapidly evolving cyber threat landscape.

Therefore, we strongly urge CMS to withdraw this proposal. CHIME also urges CMS to withdraw any reference to, or reliance on, the HIPAA Security Rule proposal in connection with this rulemaking, and ensure that the PI Program remains grounded in current law – not assumptions about a future that may never – and should not -comes to pass. CHIME believes that moving forward with the "Proposal To Modify the Security Risk Analysis Measure Beginning With the EHR Reporting Period in CY 2026" could be a serious procedural and legal misstep. Crucially, it would impose a financial and operational burden on hospitals and healthcare systems across the country – which would be especially detrimental in rural America.

[6] HSCC Statement on Healthcare Cybersecurity Policy - Health Sector Council

Proposal To Modify the Safety Assurance Factors for EHR Resilience (SAFER) Guides Measure

In January 2025, ASTP published an updated set of SAFER Guides (hereafter referred to as the 2025 SAFER Guides).[7] The 2025 SAFER Guides consist of eight guides organized into three broad groups of Foundational Guides, Infrastructure Guides, and Clinical Process Guides. CMS states that, "All guides have been edited and contain new recommendations as well as the comprehensive consolidation of recommendations that were similar and overlap in function or intent with the 2016 SAFER Guides." CMS is proposing to modify the SAFER Guides measure by requiring eligible hospitals and CAHs to attest "yes" to completing an annual self-assessment using the SAFER Guides that ASTP published in January 2025 beginning with the EHR reporting period in CY 2026.

In last year's rulemaking (IPPS/LTCH FY 2025), CMS anticipated that updated versions of the SAFER Guides may become available as early as CY 2025, and they would consider proposing a change to the SAFER Guides measure for the EHR reporting period beginning in CY 2026 to permit use of an updated version of the SAFER Guides at that time. In response, CHIME commented that, "while we are appreciative that CMS is updating the SAFER Guides, and believe it is a positive step – we are concerned that the above timeline and uncertainty could present challenges for our members."

Therefore, we must respectfully request that CMS reconsider the proposal for eligible hospitals and CAHs to conduct an annual self-assessment using all eight of the 2025 SAFER Guides at any point during the calendar year in which the EHR reporting period occurs, beginning with the EHR reporting period in CY 2026 and subsequent years. CHIME members remain steadfast in their commitment to being partners with their patients to facilitate greater – and safer – interoperability. CMS's proposal to require eligible hospitals and CAHs to conduct the annual SAFER Guides self-assessments and attest a "yes" response accounting for a completion of the self-assessment for all eight guides, is counter to the Administration's goal of reducing regulatory burden.

CMS states that, "we estimate no change in information collection burden associated with our proposed policies and updated burden estimates for the EHR reporting period in CY 2026 and future years compared to our currently approved information collection burden estimates." CMS also states, "We do not believe this provision results in any additional economic impacts beyond those previously discussed in the FY 2022 IPPS/LTCH PPS and FY 2024 IPPS/LTCH PPS final rules (86 FR 45609 and 88 FR 59432 through 59433, respectively)."

However, in previous IPPS/LTCH PPS rulemaking referenced by CMS:

> *Across 4,500 eligible hospitals and CAHs, we estimate that our proposed changes for the Medicare Promoting Interoperability Program in this proposed rule would not result in a change to the information collection burden for the CY 2024 EHR Reporting Period and subsequent years. We estimate additional* ***annual costs*** *[emphasis added] associated with our proposed modification to the SAFER Guides measure to range from a minimum of $8,916,278 to a maximum of $108,976,725 beginning with the CY 2024 EHR Reporting Period.*

[7] https://www.healthit.gov/ topic/safety/safer-guides

The vast range of impacted annual costs to implement the singular proposed SAFER Guides measure, from a minimum of nearly $9 million up to $109 million, each calendar year – provides a shocking glimpse on just how substantial this proposal will financially impact our members. Our members are committed to best practices regarding EHR implementation, safety and effectiveness, and take their responsibility to protect not only the privacy, security, and accuracy of patient data – but most critically – their patient's overall safety and well-being very seriously.

Furthermore, as CMS stated in the FY 2024 IPPS/LTCH PPS final rule: "With regard to the estimated annual costs associated with the proposal, […] we acknowledge that while an upfront investment of resources and staff time may be needed to conduct a SAFER Guides self-assessment, we believe the cost is outweighed by the potential for improved healthcare outcomes, increased efficiency, reduced risk of data breaches and ransomware attacks, and decreased malpractice premiums."[8]

As stated in the proposed rule:

> *Executive Order 14192, titled "Unleashing Prosperity Through Deregulation," was issued on January 31, 2025, and requires that "any new incremental costs associated with new regulations shall, to the extent permitted by law, be offset by the elimination of existing costs associated with at least 10 prior regulations. This proposed rule, if finalized as proposed, is expected to be an E.O. 14192 deregulatory action. We estimate that this proposed rule would generate $17.5 million in annualized cost savings at a 7 percent discount rate, discounted relative to year 2024, over a perpetual time horizon.*

In this proposed rule, CMS does not provide specific cost estimates and alludes to the belief that the financial impact is expected to be minimal and manageable within existing hospital resources. CHIME members strongly disagree with the assertion that this proposal, if finalized as proposed, would be an E.O. 14192 deregulatory action. Further, CHIME believes that reducing regulatory burden by reducing the substantial time providers must spend navigating regulatory changes and their evolving requirements would "unlock" countless hours of time. In turn, this time could be used to improve patient care and innovate new workflow and care processes.

CHIME members, even those that are larger and have more resources than most other hospitals and healthcare systems, shared that they find the requirement to perform a self-assessment using all nine SAFER Guides with one "yes/no" attestation statement to be a massive, onerous undertaking. This is an extremely concerning indication for our members that are rural and under-resourced. These are precious dollars and resources that could be going to investments in interoperability and to enhance hospital and healthcare systems' cybersecurity posture and safeguard patient care and patient data. Any investment in cybersecurity for the healthcare sector will be an investment not just in patient safety – but also national security.

Furthermore, under this proposal, an attestation of "no" would result in the eligible hospital or CAH not meeting the measure and not satisfying the definition of a meaningful EHR user under existing statute,[9] which would subject the eligible hospital or CAH to a downward payment adjustment. A downward payment adjustment creates a penalty approach resultant to this rulemaking.

[8] https://www.federalregister.gov/d/2023-16252/p-5367
[9] 42 CFR 495.4

Each hospital must involve individuals from a wide swath across an organization, beginning with the local governance committee and a multi-disciplinary team including, but not limited to, health IT specialists, technical support, application support, safety and quality, operations, health information specialists, clinicians, medical administration, and both Artificial Intelligence (AI) and EHR vendors and developers. Simply getting all these individuals from these teams together in the same room, at the same time – is an extremely burdensome undertaking and requires significant time and effort. Furthermore, EHR developers and vendors are not regularly "on-site", and having to rely on their participation makes an accurate, thorough self-assessment of the guides nearly impossible.

Additionally, our members have expressed concern that their EHR vendors would not assume responsibility for assisting providers in attesting to performing the self-assessment for each of the SAFER Guides – due to potential liability concerns. While vendors may offer general implementation guidance or reference materials, the burden of demonstrating compliance – including configuring, testing, and documenting technical capabilities – ultimately rests with the provider. This dynamic was evident during the Meaningful Use program, where vendors disseminated baseline standards, but providers were responsible for resolving implementation challenges – such as Admission, Discharge, and Transfer (ADT) exchange – unless a vendor-specific technical defect could be clearly identified.

When attestation was first required for the 2016 SAFER Guides, CMS offered eligible hospitals and CAHs a two-year period to begin the process, without penalty for not being able to complete the self-assessments. Additionally, this two-year period without penalty offered eligible hospitals and CAHs time to review available resources, work with staff and vendors on establishing an annual review process, where they would not be penalized for not having completed the self-assessments. **Before CMS requires the complex process of attesting to each of the 2025 SAFER Guides, CHIME is recommending CMS provide this same two-year period without penalty. We respectfully request that CMS require eligible hospitals and CAHs to conduct an annual self-assessment using all eight of the 2025 SAFER Guides at any point during the calendar year in which the EHR reporting period occurs, beginning with the EHR reporting period in CY 2028 without facing a downward payment adjustment.**

Further, CMS could require the annual self-assessment and attestation in a stepwise fashion (e.g., three guides per year). In the meantime, eligible hospitals and CAHs will continue to "familiarize" themselves with the use of the 2025 SAFER Guides. Our members are committed to best practices regarding EHR implementation, safety and effectiveness, and take their responsibility to protect not only the privacy, security, and accuracy of patient data – but most critically – their patient's overall safety and well-being very seriously.

CHIME also urges CMS to take into consideration the increasingly complex cybersecurity landscape hospitals and health systems must navigate and urge the agency to reconsider the timeline CMS has established for eligible hospitals and CAHs to attest to the 2025 SAFER Guides. Hospitals are spending an increasing amount of time, energy and resources navigating this highly challenging and evolving environment, which is an issue we have identified in several previous comment letters and during conversations with HHS, CMS, ASTP/ONC and other agencies.

Eligible hospitals and CAHs are spending between nearly $9 million and up to nearly $110 million dollars to conduct the 2016 SAFER Guides self-assessment and attest "yes" to the measure. These are precious dollars and resources that could be going to investments to enhance hospital and healthcare systems' cybersecurity posture and safeguard patient care and

patient data. Any investment in cybersecurity for the healthcare sector will be an investment not just in patient safety – but also national security.

Conclusion

In closing, we would like to thank you for providing the opportunity to comment and CHIME appreciates the chance to help inform the important work being done by CMS. We respectfully request that CMS take our comments on this proposed rule into consideration. CHIME and our members remain committed to the successful implementation of the Medicare PI Program, with strong and meaningful data exchanges. Understanding the long-term ramifications of these proposed policies is critical, and CHIME urges CMS to ensure these proposals do not inadvertently create and impose additional regulatory burden onto hospitals and healthcare systems.

As discussed in detail above, CHIME has several recommendations and concerns. We cannot stress enough the importance of reducing burden on healthcare providers while promoting safety and effective use of EHRs. Our members are deeply committed to making sound investments in EHRs and cybersecurity resources to protect the patient data they are entrusted to protect.

CHIME members are executives and senior healthcare IT leaders; thus, we are offering to continue to serve as a resource to CMS as they continue towards the goal of enabling providers to make improvements to safety and safe use of EHRs as necessary over time, which CHIME members staunchly support. Our comments are not intended to be censorious – we wish to work with CMS as partners and share the goal of strongly promoting safety and the safe use of EHRs. However, we believe that it needs to be done judiciously, with a stepwise approach.

The investments that would be required to meet these proposals would decrease providers' ability to make truly meaningful cybersecurity investments and will drive up the cost of healthcare for everyday Americans. CHIME is concerned that these proposals would impose significant costs and burden without meaningfully improving security – while reducing efficiency and increasing vulnerability, especially for smaller and rural healthcare providers. CHIME members are continuously investing in robust data security and cybersecurity and will continue to do so without overly prescriptive, heavy handed, and burdensome regulation.

We look forward to continuing to be a trusted stakeholder and resource to CMS and continuing to deepen the long-standing relationship we have shared. Working together through the rulemaking process is just one way we can accomplish our shared goals and make meaningful changes in healthcare.

Should you have any questions or if we can be of assistance, please contact Chelsea Arnone, Director, Federal Affairs at carnone@chimecentral.org.

Sincerely,

Russell P. Branzell, CHCIO, LCHIME
President and CEO
CHIME