AMA
AMERICAN MEDICAL ASSOCIATION

JAMES L. MADARA, MD
EXECUTIVE VICE PRESIDENT, CEO

ama-assn.org
t (312) 464-5000

Executive Summary of AMA Comments on CMS' Proposed Rule

The American Medical Association (AMA) has submitted comments to the Centers for Medicare & Medicaid Services (CMS) regarding the proposed rule on Medicare and Medicaid Programs; Patient Protection and Affordable Care Act; Interoperability and Patient Access for Medicare Advantage Organizations and Medicaid Managed Care Plans, State Medicaid Agencies, CHIP Agencies and CHIP Managed Care Entities, Issuers of Qualified Health Plans in the Federally-Facilitated Exchanges and Health Care Providers (Proposed Rule).[1] Improved accessibility to health information has the potential to transform care delivery and improve patient outcomes, particularly as the U.S. health system transitions from a fee-for-service model to value-based payment. The AMA appreciates many of CMS' proposals, and has included suggestions for how to strengthen the proposals prior to finalization. In summary:

- The AMA supports the proposed requirement that payers provide patients with access to their health care data through an application programming interface (API). We agree with CMS that patients should have the ability to decide how their information will be used by consumer-facing apps, and we include ways CMS can incentivize app developers to keep patient health information private.
    - CMS should also require payers to provide prior authorization requirements to patients and physicians.
    - While physicians must provide information to patients free-of-charge, CMS has not indicated that the same requirement applies to payers. It is unclear who will absorb the associated costs.
        - CMS should ensure that beneficiaries and the individuals assisting them should have assurances that information provided across settings (e.g., online web portals, smartphone apps, payer policy booklets, etc.) contain consistent information.
    - The AMA supports the proposal that certain payers expose provider directory information through an API to current enrollees, prospective enrollees, and the public.
        - We recommend extending this requirement to qualified health plans (QHPs) in federally-facilitated exchanges (FFEs).
        - We also urge CMS to require payers to update their provider directories in real-time and expeditiously correct errors, and strongly encourage CMS to implement and enact enforcement actions for payers that demonstrate noncompliance.
- The AMA appreciates the importance of trusted exchange networks (TEN) for information exchange but recommends that CMS include language in its final rule preventing insurers from requiring TEN participation as a term of network contracts.

[1] Throughout the comments, unless otherwise noted, we use the term "Payer" to refer to all of the payers implicated by the proposed rule—the Medicare Fee-for-Service (FFS) Program, the Children's Health Insurance (CHIP) FFS program, Medicare Advantage (MA) Organizations, Medicaid Managed Care plans (managed care organizations (MCOs), prepaid inpatient health plans (PIHPs) and prepaid ambulatory health plans (PAHPs)), CHIP Managed Care entities (MCOs, PIHPs, and PAHPs), and issuers of qualified health plans (QHPs) in Federally-facilitated Exchanges (FFEs). We use the terms "beneficiary" and "patient" interchangeably.

- The AMA urges CMS to move away from additional punitive levers related to information blocking and increase its efforts to provide positive incentives that will continue to increase rates of interoperability and patient access.

    - The AMA agrees with the general goal of including digital health contact information in a national provider directory.

        - CMS should encourage the development of this directory through positive incentives as opposed to public shaming, Medicare enrollment/revalidation, or Medicare reporting programs.

        - The directory should be accessible only to the provider and payer community (as opposed to the public) or, alternatively, should utilize an industry solution that is selected via a transparent process with input from cross-industry stakeholders.

    - The AMA agrees with CMS that coordination of care across institutional and non-institutional settings of care, as well as timely, electronic exchange of health information to support patient admission, discharge, and transfer (ADT) is a desirable goal.

        - However, the proposal is vague and, as drafted, could place substantial burden on physician practices. It also goes too far by requiring such notifications as a Condition of Participation.

Additionally, the AMA has identified four overarching areas of concern related to physician contracting requirements, privacy, payer-to-payer exchange of clinical data, and payer overreach into a physician's electronic health record (EHR).

Physician contracting requirements

Because this rule will impose additional requirements on Payers to provide certain types of information to patients and exchange information with other entities (e.g., other Payers and trusted exchange networks), we are concerned that Payers may "pass down" similar requirements onto their network physicians through burdensome or coercive contractual requirements. For example, as explained in more detail below, a Payer may force a physician to participate in the same exchange in which the Payer participates so that it has access to the physician's clinical information. This would likely lead to physicians who contract with multiple Payers needing to comply with multiple network requirements and take on costs and administrative burdens associated with each network.

CMS anticipates—and in fact encourages—that Payers will impose contractual requirements on physicians. Recognizing that Payers' ability to provide data quickly will depend on providers submitting the data on a timely basis, CMS "urges payers to consider whether their contracts with network providers should include timing standards regarding the submission of claims and encounter data to comply with API requirements."[2] This suggestion fails to consider potential downstream consequences, including whether such tactics will narrow a Payer's provider network. Narrow network plans have become increasingly common in private health insurance markets, including Medicare Advantage. The AMA and other physician groups have raised concerns that narrow physician networks create challenges for patients

[2] 84 Fed. Reg. 7610, at 7632 (Mar. 4, 2019).

seeking care and pose potential patient protection issues. Payers have much more leverage in a physician-payer relationship than a physician—particularly a small physician practice—and they will point to CMS' comments to strong-arm physicians. If a physician refuses, a network narrows. To guard against this, **CMS should prohibit Payers from using these proposals to place additional contractual demands on physicians and impose meaningful penalties for Payer noncompliance with this new prohibition.**

Privacy

We wholeheartedly appreciate CMS' acknowledgement that "unscrupulous actors" could use apps to profit from an individual's information in ways that the individual did not authorize or understand. Unfortunately, stories and studies abound about how smartphone apps share sensitive health information with third parties, often without the knowledge of an individual.[3] If beneficiaries access their and their family's health data—some of which are likely sensitive—through a smartphone, a patient should have a clear understanding of the potential uses of that data by app developers. Otherwise, most patients will not be aware of who has access to their medical information, how and why they received it, and how it is being used (for example, an app may collect or use information for its own purposes, such as an insurer using health information to limit/exclude coverage for certain services, or may sell information to clients such as to an employer or a landlord). The downstream consequences of data being used in this way may ultimately erode a patient's privacy and willingness to disclose information to his or her physician.

To assist in preventing this scenario, the AMA has identified an opportunity for CMS to empower patients with meaningful knowledge and control over how apps use their health data. **CMS should require that Payers' APIs check an app's attestation to:**

- **Industry-recognized development guidance** (e.g., Xcertia's Privacy Guidelines)[4];
- **Transparency statements and best practices** (e.g., Mobile Health App Developers: FTC Best Practices[5] and CARIN Alliance Code of Conduct)[6]; and
- **A model notice to patients** (e.g., U.S. Office of the National Coordinator for Health Information Technology's [ONC's] Model Privacy Notice)[7].

The app could be acknowledged or listed by the API developer in some special manner (e.g., in an "app store," "verified app" list). We would urge CMS to limit its BlueButton 2.0 app listings to those apps that

[3] Citations to these examples are provided in the body of the letter: (1) The Wall Street Journal reported that Facebook collected sensitive health and demographic data from a user's cellphone apps, regardless of whether the individual had the Facebook app on his or her phone, and even if the individual had never signed-up for Facebook. (2) Studies reported in the British Medical Journal and Journal of the American Medical Association have demonstrated that most apps do not share privacy policies with patients, and when they do, sometimes do not adhere to them. (3) The Washington Post reported that a workplace wellness pregnancy-tracking app reports data to a woman's employer, including the woman's average age, number of children and current trimester; the average time it took her to get pregnant; whether the pregnancy is high-risk, conceived after a stretch of infertility, a C-section or premature birth; and her return-to-work timing. The app's privacy notice is 6,000 words.

[4] https://xcertia.org/app-privacy-survey/.

[5] https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health-app-developers-ftc-best-practices.

[6] https://www.carinalliance.com/our-work/trust-framework-and-code-of-conduct/.

[7] https://www.healthit.gov/sites/default/files/2018modelprivacynotice.pdf.

have replied "yes" to all three attestations or, at the very least, provide those apps with a special designation on the BlueButton 2.0 website.

We recognize that a "yes" attestation would not ensure apps implement or conform to their attestations. However, app developer attestations would be a powerful resource for the Federal Trade Commission (FTC) in its enforcement of unfair and deceptive practices. In other words, an app developer would be strongly motivated to attest "yes" and to act in line with their attestations. We do not believe that requiring an API check for an app developer attestation would be a significant burden on health IT developers. We also specifically note that this proposal does not ask CMS to regulate apps or app developers; rather it regulates the type of API technology that Payers must adopt.

CMS can implement this requirement even if ONC does not since CMS' proposal does not require Payers to use Health IT Modules certified by ONC. We firmly believe these sorts of "checks" on an app will provide a needed level of assurance to patients and would be greatly welcomed by users.

Payer-to-payer exchange of clinical data[8]

CMS is proposing to require Payers to coordinate care between plans by exchanging a set of clinical information (the U.S. Core Data for Interoperability, or USCDI) with another Payer upon a beneficiary's request. We support the proposal to the extent that it will promote continuity of care and prevent new prior authorization or step therapy requirements. However, we have significant concerns about whether excessive data access will lead to increased prior authorization and patient profiling—limiting coverage and access to care.

Historically, Payers have only had access to clinical information when necessary for payment. Physicians have acted as "gatekeepers" to determine what information is necessary for each individual to be covered and for the physician to be paid. However, automated access to the EHR would potentially remove that gatekeeper and grant the Payer access to information in the EHR beyond what it needs for a particular transaction. This could have negative downstream consequences for patients and physicians. For example, a Payer could determine that the patient had already received imaging or another service from another plan and automatically deny coverage of that imaging service or require unnecessary prior authorization requirements that delay needed care. Even when patients already have coverage, there are examples of payers making coverage decisions based on patient information that neither the patient nor the patient's physician knew the payer was receiving.[9]

Payers must be prohibited from using this information to discriminate against a beneficiary—both newly covered and those in the application process. **CMS should require that Payers (a) attest that USCDI exchange between plans cannot be used as a basis to deny or delay coverage, increase rates, or implement step therapy; (b) display information to that effect on their website and in coverage documents; (c) cannot require an applicant or enrollee to request that a previous payer send the information to the payer as part of the enrollment process; and (d) provide language to that effect on enrollment forms and websites.**

---

[8] To be clear, if a patient requests that his or her physician send his or her USCDI to a payer, we of course would support the fulfillment of that request under the Health Insurance Portability and Accountability Act (HIPAA) right of access (directed to a third party).

[9] Marshall Allen, *You Snooze, You Lose: How Insurers Dodge The Costs Of Popular Sleep Apnea Devices*, National Public Radio and ProPublica (Nov. 21, 2018), available at https://www.npr.org/sections/health-shots/2018/11/21/669751038/you-snooze-you-lose-how-insurers-dodge-the-costs-of-popular-sleep-apnea-devices.

Unfettered Payer access to an EHR

We have concerns about how Payers will obtain the clinical information necessary to comply with CMS' requirement that a Payer provide a beneficiary's full USCDI to another Payer at his or her request. The ultimate source of the USCDI's clinical data is a clinician; a Payer will not necessarily have a beneficiary's complete USCDI at any given point.

We anticipate that some commenters will suggest that Payers be allowed to pull information out of a provider's EHR via API to promote Payer compliance with this requirement while reducing burden on the patient and physician. In fact, some Payers are already automatically accessing a physician's EHR for other purposes, either as an elective offering or through contractual requirements. We envision Payers viewing this requirement as a logical use case for "tapping into" a physician's EHR. However, physician practices may not understand that access to this data could lead to selective, discriminatory reimbursement models and intrusion on physician medical decision-making power (e.g., lower reimbursement rates for certain types of care that a physician deems necessary or in the best interest of the patient). Furthermore, physician practices could be priced out of markets because a Payer determines that they are a "second- or third-tier" option based on the totality of the information in the EHR.

Accordingly, **CMS should clearly state that (a) Payers are not entitled to receive information from a health care provider if such information is protected by federal, state, or local privacy law; (b) physicians may use their best judgement in responding to a request from a Payer for clinical information to the extent allowed by law; and (c) Payers may not condition provider participation in a plan based on whether a physician will grant the Payer electronic access to the practice's EHR to fulfil requests for the USCDI.**

The AMA's full comment letter can be found here.