

May 31, 2019

The Honorable Seema Verma
Administrator
Centers for Medicare & Medicaid Services
U.S. Department of Health and Human Services
Hubert H. Humphrey Building, Room 445–G
200 Independence Avenue, SW
Washington, DC 20201

Re: CMS-9115-P

Dear Administrator Verma:

On behalf of the physician and medical student members of the American Medical Association (AMA), I am pleased to offer our 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.

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 (FFE). We use the terms “beneficiary” and “patient” interchangeably.

- 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.
- 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 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

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

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.

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 Practices⁵ 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 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.

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>.

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).

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.**

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.**

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>.

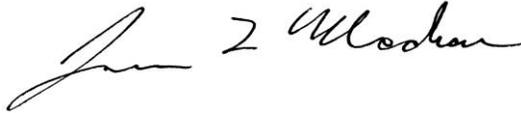
The Honorable Seema Verma

May 31, 2019

Page 6

In closing, we greatly appreciate this opportunity to share the views of the AMA regarding the proposals, issues, and questions which CMS has raised in its Proposed Rule. Our comprehensive comments are below. If you have any questions, please contact Laura Hoffman, Assistant Director, Federal Affairs, at laura.hoffman@ama-assn.org or 202-789-7414.

Sincerely,

A handwritten signature in black ink, appearing to read "James L. Madara". The signature is fluid and cursive, with a large initial "J" and "M".

James L. Madara, MD

Attachment

I. Contractual Requirements of Timing Standards Will Narrow Network Adequacy

We are troubled by the possibility that payers may use these proposals to impose contractual requirements onto their network physicians. Narrow network plans have become increasingly common in private health insurance markets, including MA. While traditional Medicare allows seniors to access any physician or hospital that accepts Medicare patients, MA access is limited to physicians and hospitals within plan networks. More than one in three MA enrollees is in a narrow physician network, which is defined as less than 30 percent of physicians in the county participating in the plan.¹⁰ On average, MA networks include less than half of all physicians in a given county.¹¹

Narrow networks give insurers greater leverage to negotiate physician payment rates and to select those providers that the insurer believes deliver high quality of care.¹² However, MA plans state that, because they already pay providers at or near Medicare fee schedule rates, negotiating lower payment rates is not a significant consideration.¹³ Instead, they achieve lower total costs by focusing on utilization.

The AMA and other physician groups have raised concerns that narrow physician networks create challenges for patients seeking care and pose potential patient protection issues. Specifically, a narrow network might have shortages of specific specialties, and plans may purposefully understaff specialties to avoid attracting enrollees with expensive pre-existing conditions like cancer and mental illness.¹⁴ Access to psychiatrists is more restricted than other specialties. On average, only 23 percent of psychiatrists in a county participate in MA plans, and 36 percent of plans include less than 10 percent of psychiatrists in their county.¹⁵ Limited access to specialists extends beyond psychiatry to cardiothoracic surgeons, neurosurgeons, radiation oncologists, and others.

In an acknowledgement 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."¹⁶ This recommendation is problematic. Physician practices have limited resources, including administrative staff, and have developed procedures and workflows to turn claims around quickly. The faster physicians submit claims, the faster they are paid, so there is already a built-in

¹⁰ Gretchen Jacobson, Matthew Rae, Tricia Neuman, Kendal Orgera, and Cristina Boccuti, Kaiser Family Foundation, *Medicare Advantage: How Robust Are Plans' Physician Networks?* (Oct 05, 2017), available at <https://www.kff.org/medicare/report/medicare-advantage-how-robust-are-plans-physician-networks/>.

¹¹ Id.

¹² Mark A. Hall, Paul B. Ginsberg, USC-Brookings Schaeffer Initiative for Health Policy, *A Better Approach to Regulating Provider Network Adequacy* (Sept. 2017), available at <https://www.brookings.edu/wp-content/uploads/2017/09/regulatory-options-for-provider-network-adequacy.pdf>.

¹³ Laura Skopec, Robert A. Berenson, Judith Feder, The Urban Institute, *Why Do Medicare Advantage Plans Have Narrow Networks?* (Nov. 2018), available at https://www.urban.org/sites/default/files/publication/99414/why_do_medicare_advantage_plans_have_narrow_networks.pdf.

¹⁴ Mark A. Hall, Paul B. Ginsberg, USC-Brookings Schaeffer Initiative for Health Policy, *A Better Approach to Regulating Provider Network Adequacy* (Sept. 2017), available at <https://www.brookings.edu/wp-content/uploads/2017/09/regulatory-options-for-provider-network-adequacy.pdf>.

¹⁵ Gretchen Jacobson, Matthew Rae, Tricia Neuman, Kendal Orgera, and Cristina Boccuti, Kaiser Family Foundation, *Medicare Advantage: How Robust Are Plans' Physician Networks?* (Oct 05, 2017), available at <https://www.kff.org/medicare/report/medicare-advantage-how-robust-are-plans-physician-networks/>.

¹⁶ 84 Fed. Reg. 7610, at 7632 (Mar. 4, 2019).

incentive to submit claims quickly. Furthermore, Payers have much more leverage in a physician-payer relationship than a physician—particularly a small physician practice—and they will point to comments like these to strong-arm physicians. **In an environment where there are already network adequacy problems, 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.**

II. Privacy

We appreciate CMS' discussions of privacy and security concerns in the context of APIs, including instruction that Payers comply with federal, state, and local privacy laws and provide consumers with information about the roles of the U.S. Office of Civil Rights (OCR) and FTC in protecting privacy rights. However, we are dismayed that CMS chose to identify privacy concerns as one of five “challenges and barriers” to interoperability, particularly when there are technological solutions to promote interoperability while protecting privacy. Such language indicates that CMS and covered entities should think of privacy as a burden rather than a cornerstone of the physician-patient relationship. Health care information is one of the most personal types of information an individual can possess and generate—regardless of whether it is legally defined as “sensitive”—and its privacy is critical regardless of where the data resides, how it is used, or why it is exchanged. CMS' proposal will affect data exchange both within and outside of the HIPAA-covered space, and both scenarios must respect patient privacy when evaluating how to encourage greater access. **We must always evaluate whether providing increased access to information to anyone other than the patient will encourage patients to seek care or potentially deter them.** Proper controls and consent mechanisms must be a part of any policy proposal, lest health data be shared without patients' consent.

Privacy risks include re-identification of patients through de-identified (or partially de-identified) data, misunderstanding or disregard of the scope of a patient's consent, patient perception of loss of their privacy leading to a change in their behavior, embarrassment or stigma resulting from an unwanted disclosure of information or from fear of a potential unwanted disclosure, perceived and real risks of discrimination including employment and access to or costs of insurance, and law enforcement accessing data repositories beyond their intended scope.

AMA approach to privacy

The first step of any ultimately successful privacy framework, legislative or regulatory, places the patient first. Each entity seeking access to patients' most confidential medical information must pass the stringent test of showing why its professed need should override individuals' most basic right in keeping their own information private. Moreover, citizens deserve a full and open discussion of exactly who wants their private medical information and for what purpose.

The AMA's approach to privacy is governed by our Code of Medical Ethics and long-standing policies adopted by our policymaking body, the House of Delegates, which support strong protections for patient privacy and, in general, require physicians to keep patient medical records strictly confidential. **AMA policy and ethical opinions on patient privacy and confidentiality provide that a patient's privacy should be honored unless waived by the patient in a meaningful way, de-identified, or in rare instances when strong countervailing interests in public health or safety justify invasions of patient**

privacy or breaches of confidentiality. These policies and ethical opinions are designed not only to protect patient privacy, but also to preserve the trust inherent in the patient-physician relationship.

This is particularly important in scenarios involving sensitive health information. For example, striking the correct balance is critical in encouraging individuals with mental illness and/or substance use disorders (SUD) to seek treatment. Consumers are also increasingly concerned with privacy in today's environment (e.g., the Facebook–Cambridge Analytica data scandal). In fact, many industries, states, and countries are moving towards increasing privacy rights and protections, not expanding ways in which information can be shared without an individual's full knowledge and clear consent.

Physicians take the Hippocratic Oath to “do no harm” and swear that “whatever I see or hear in the lives of my patients, whether in connection with my professional practice or not, which ought not to be spoken of outside, I will keep secret, as considering all such things to be private.”¹⁷ Physicians want to share patients' information where appropriate. However, maintaining trust between patients and physicians is fundamental to medicine. Patient trust in the health care system can only be assured when all entities that maintain a patient's health information have an obligation to maintain the confidentiality of that information and when patients truly have autonomy and control over decisions to disclose or retain their personal information.

Privacy controls in FHIR

CMS is proposing to require Payers to implement open APIs consistent with the API technical standards proposed by ONC in 84 Fed. Reg. 7424 (March 4, 2019), using content and vocabulary standards that include those proposed by ONC at 45 CFR 170.213.¹⁸ These standards include the use of HL7 Fast Healthcare Interoperability Resources (FHIR) referenced in 45 CFR §170.299. FHIR supports data controls like segmentation; however, we are concerned those controls are an afterthought in FHIR-based API design and will become “bolt-on” functions—drastically increasing their costs and limiting their usefulness. The AMA has been told that FHIR developer efforts are first focused on “just making the technology work” and that “patient data protections and privacy controls are outside their scope.” The downstream consequences of this approach will negatively impact physicians and patients. Developers need to address privacy concerns and incorporate privacy considerations as a part of the development process of any new technology. Mechanisms to monitor and control data access, patient consent and privacy, and ensure data provenance, governance, and enforce state and federal law must be inherent in FHIR development.

Fortunately, ONC names in its proposed rule the Consent2Share FHIR Consent Profile standard developed by the Substance Abuse and Mental Health Services Administration (SAMHSA). Consent2Share provides both physician and patient-facing services and the infrastructure to segment data and manage consent. **The AMA strongly supports the use of this standard and urges CMS to require Payers to use it.** Doing so would help both physicians and Payers to comply with local, state, and federal privacy laws while still facilitating patient access and interoperability. It also would assist with implementing recommendations from the physician-directed “*Consensus Statement: Feature and Function Recommendations to Optimize Clinician Usability of Direct Interoperability to Enhance Patient*

¹⁷ https://www.nlm.nih.gov/hmd/greek/greek_oath.html.

¹⁸ We direct CMS to our comments on ONC's rule for feedback on the proposed API standards.

Care,” which calls for system configurations that prevent the forwarding of information specifically protected by law.¹⁹

Consumer-facing apps

The AMA is also very concerned consumer-facing apps will monetize patient data without patient knowledge. We appreciate CMS’ proposal for Payers to provide consumers with their health and claims information through consumer-facing applications (apps). The AMA has long heralded the benefits of APIs and apps to both patients and physicians. Together they can offer better information usability, providing an enhanced view into a patient’s medical record repository. However, patient privacy is of utmost concern when non-covered HIPAA entities such as apps gain access to medical information. **To be clear, the AMA supports patients’ access to their entire record.** But there is a significant lack of attention on consumer education and patient control over the use of their information once his or her information has been downloaded onto a smartphone. Apps often do not provide patients with clear terms of how his or her data will be used. The app’s terms can be 6,000+ words in length, and can shield a developer’s activities by permitting a “royalty-free, perpetual, and irrevocable license, throughout the universe” to “utilize and exploit” an individual’s de-identified personal information for scientific research and “marketing purposes.” The terms may also permit a developer to “sell, lease or lend aggregated Personal Information to third parties.”²⁰

Many apps, particularly free apps, use advertisements to generate revenue. The advertisements collect and share an individual’s advertising ID—a string of numbers and letters that identify an individual and keep a log of his or her clicks, searches, purchases, and sometimes geographic location as he or she moves through various apps.²¹ While the information is often deemed anonymous, the information can be “shockingly easy to de-anonymize, and that hundreds of apps collect ‘anonymous’ real-time location data that needs only the slimmest additional context clues to tie to an individual person.”²² As National Public Radio and ProPublica report, “it isn’t hard to understand the appeal of all of this data to insurers”:

Merging information from data brokers with people’s clinical and payment records is a no-brainer if you overlook potential patient concerns. Electronic medical records now make it easy for insurers to analyze massive amounts of information and combine it with the personal details scooped up by data brokers.

Some insurance companies are already using socioeconomic data to help patients get appropriate care, such as programs to help patients with chronic diseases stay healthy. Studies show social and economic aspects of people’s lives play an important role in their health. Knowing these personal details can help them identify those who may need help paying for medication or help getting to the doctor. ... But experts said patients’ personal information could still be used for

¹⁹ Steven R. Lane et al., *Appl. Clin. Inform.* 2018; 9:205-220, available at <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5863061/>.

²⁰ Drew Harwell, *Washington Post*, *Is your pregnancy app sharing your intimate data with your boss?* (April 10, 2019), available at https://www.washingtonpost.com/technology/2019/04/10/tracking-your-pregnancy-an-app-may-be-more-public-than-you-think/?utm_term=.3b82122fec27.

²¹ Kaitlyn Tiffany, *Vox Media Network*, *Angry Birds and the end of privacy* (May 13, 2019), available at <https://www.vox.com/explainers/2019/5/7/18273355/angry-birds-phone-games-data-collection-candy-crush>.

²² Kaitlyn Tiffany, *Vox Media Network*, *Angry Birds and the end of privacy* (May 13, 2019), available at <https://www.vox.com/explainers/2019/5/7/18273355/angry-birds-phone-games-data-collection-candy-crush>.

marketing, and to assess risks and determine the prices of certain plans...[noting that short-term health plans] allow insurers to deny coverage to sick patients.²³

A recent Wall Street Journal report exposed just how much is at stake when patients share their personal health information with apps. Several apps feed users' personal health information to Facebook even if the individual does not have Facebook installed on his or her phone, or even possess a Facebook account.²⁴ A study published in the Journal of the American Medical Association (JAMA) found that many health apps created to track a user's progress in battling depression or quitting smoking are sharing the personal details they collect about an individual with third parties—like Google and Facebook—without the individual's knowledge or informed consent:

Transmission of data to third-party entities was prevalent, occurring in 33 of 36 top-ranked apps (92%) for depression and smoking cessation, but most apps failed to provide transparent disclosure of such practices. Commonly observed issues included the lack of a written privacy policy, the omission of policy text describing third-party transmission (or for such transmissions to be declared in a nonspecific manner), or a failure to describe the legal jurisdictions that would handle data. In a smaller number of cases, data transmissions were observed that were contrary to the stated privacy policies.²⁵

Apps are also being used as a powerful monitoring tool for employers and payers. Couched in corporate wellness, employers and payers have aggressively pushed to gather more data about their employees' lives than ever before.

Experts worry that companies could use the data to bump up the cost or scale back the coverage of health care benefits, or that women's intimate information could be exposed in data breaches or security risks. Although the data is made anonymous, experts also fear that the companies could identify women based on information relayed in confidence, particularly in workplaces where few women are pregnant at any given time.²⁶

Not only do these practices jeopardize patient privacy and commoditize an individual's most sensitive information, but they also threaten patient willingness to utilize technology to manage their health—a goal frequently expressed by the administration. In fact, a Rock Health 2018 National

²³ Marshall Allen, National Public Radio, *Health Insurers Are Vacuuming Up Details About You—And It Could Raise Your Rates* (July 17, 2018), available at <https://www.npr.org/sections/health-shots/2018/07/17/629441555/health-insurers-are-vacuuming-up-details-about-you-and-it-could-raise-your-rates>.

²⁴ <https://www.wsj.com/articles/you-give-apps-sensitive-personal-information-then-they-tell-facebook-11550851636>.

²⁵ Kit Huckvale et al., JAMA Netw Open. 2019;2(4):e192542, *Assessment of the Data Sharing and Privacy Practices of Smartphone Apps for Depression and Smoking Cessation* (April 19, 2019), available at [https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2730782?utm_source=For The Media&utm_medium=referral&utm_campaign=ftm_links&utm_term=041919](https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2730782?utm_source=For%20The%20Media&utm_medium=referral&utm_campaign=ftm_links&utm_term=041919).

²⁶ Drew Harwell, Washington Post, *Is your pregnancy app sharing your intimate data with your boss?* (April 10, 2019), available at https://www.washingtonpost.com/technology/2019/04/10/tracking-your-pregnancy-an-app-may-be-more-public-than-you-think/?utm_term=.3b82122fec27.

Consumer Health Survey found that just 11 percent of respondents said they would be willing to share health data with tech companies.²⁷

The survey noted that physicians are the most trusted entities with whom patients are willing to share information. However, it notes, confidence is dropping, possibly due to spillover from privacy and security breaches in other sectors and general distrust of “big tech.”²⁸ A 2017 Black Book survey reports that:

- 87 percent of patients were unwilling to comprehensively share all of their health information with their physicians;
- 89 percent of consumers who had visited a health care provider in 2016 said they had withheld some information during their visits;
- 81 percent were concerned that information about chronic conditions was being shared without their knowledge; and
- 99 percent were concerned about the sharing of mental health notes.²⁹

In other words, carelessness and lack of transparency in how consumer information is handled and used by technology has likely influenced what a patient is likely to share with his or her physician. This should serve as a warning to policy makers that consumers take privacy very seriously. **Privacy safeguards must be established concurrently with any health information exchange policies—particularly when consumer-facing technology is implicated—or patient health and safety will be jeopardized.**³⁰

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. To assist in preventing this scenario, the AMA has identified an opportunity for CMS to empower patients with meaningful knowledge and control over the use of 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 Guidelines³¹);
- **Transparency statements and best practices** (e.g., Mobile Health App Developers: FTC Best Practices³² and CARIN Alliance Code of Conduct³³); and

²⁷ Sean Day and Megan Zweig, Rock Health, *Beyond Wellness for the Healthy: Digital Health Consumer Adoption 2018*, available at <https://rockhealth.com/reports/beyond-wellness-for-the-healthy-digital-health-consumer-adoption-2018/>.

²⁸ Sean Day and Megan Zweig, Rock Health, *Beyond Wellness for the Healthy: Digital Health Consumer Adoption 2018*, available at <https://rockhealth.com/reports/beyond-wellness-for-the-healthy-digital-health-consumer-adoption-2018/>.

²⁹ Black Book Market Research, *Healthcare’s Digital Divide Widens* (Jan. 3, 2017), available at <https://blackbookmarketresearch.newswire.com/news/healthcares-digital-divide-widens-black-book-consumer-survey-18432252>.

³⁰ “Incomplete medical histories and undisclosed conditions, treatment or medications raises obvious concerns on the reliability and usefulness of patient health data in application of risk based analytics, care plans, modeling, payment reforms, and population health programming.” Doug Brown, Black Book Managing Partner, available at <https://www.prnewswire.com/news-releases/healthcares-digital-divide-widens-black-book-consumer-survey-300384816.html>.

³¹ <https://xcertia.org/app-privacy-survey/>.

³² <https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health-app-developers-ftc-best-practices>.

³³ <https://www.carinalliance.com/our-work/trust-framework-and-code-of-conduct/>.

- **A model notice to patients** (e.g., ONC’s Model Privacy Notice³⁴).

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 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 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. Additionally, if CMS does not believe that such a policy is a logical outgrowth of its proposal (despite multiple sections of the proposal being dedicated to privacy), it should issue a Supplemental Notice of Proposed Rulemaking to solicit feedback from the stakeholder community. 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.

We are aware there are some who believe requiring even this minimum level of privacy controls for patients is “paternalistic.” This characterization is perplexing given that patient privacy is a fundamental aspect of the 21st Century Cures Act, necessary for patients to safeguard themselves from data profiteering and discrimination, and promoted by the AMA Code of Medical Ethics and House of Delegates, which includes representation from state and territorial medical associations, national medical specialty organizations, and the federal government.

III. Technical Standards Related to Interoperability

Content and vocabulary standards

CMS proposes to require Payers to use API technology conformant with the USCDI v1 (proposed in ONC’s rule at 45 CFR 170.213). As for content and vocabulary standards for data available through the API, CMS proposes the following:

1. API standards and associated implementation specifications proposed in ONC’s rule at 45 CFR 170.213 where such standards are the only available standards for the data type or element;
2. Content and vocabulary standards at 45 CFR Part 162 (HIPAA Transactions) and 42 CFR 423.160 (NCPDP SCRIPT) where required by law or where such standards are the only available standards for the data type or element; or
3. The content and vocabulary standards in (1) or (2) as determined appropriate for the data type or element where a specific data type or element may be encoded or formatted using content and vocabulary standards in (1) or (2).

³⁴ <https://www.healthit.gov/sites/default/files/2018modelprivacynotice.pdf>.

We begin by noting that HIPAA standards cover communication between providers and health plans—not health plans and patients, which is the use case discussed in this rule. Payers are required under law to support the HIPAA Transactions, but just with providers—not patients. We are puzzled as to why CMS has indicated that such usage would be required by law. Still, given that the USCDI does not contain the data elements that CMS is proposing Payers must provide to patients, the HIPAA Transactions are currently the only way to relay such information and, as such, most of the information patients receive will be in HIPAA Transaction format unless it is translated for them. While we agree with CMS that both API technology itself and the data it makes available must be standardized to support true interoperability, the HIPAA Transaction content and vocabulary standards will not be useful for most patients, particularly those who need care “outside of their regular provider’s business hours, while traveling, or in the wake of a natural disaster,” as CMS suggests.

The HIPAA Transactions are not patient-readable. As shown in the image below, they are essentially strings of letters, numbers, and symbols; only by utilizing an app or other technology can patients make sense of the information such transactions contain.

```
TS3*6543210903*11*20021231*1*211366.97*****138018.4**73348.57~  
TS2*2178.45*1919.71**56.82*197.69*4.23~  
CLP*666123*1*211366.97*138018.4**MA*1999999444444*11*1~  
CAS*CO*45*73348.57~  
NMI*QC*1*JONES*SAM*O***HN*666666666A~  
MIA*0***138018.4~  
DTM*232*20020816~  
DTM*233*20020824~  
QTY*CA*8~  
LX*130212~  
TS3*6543210909*13*19961231*1*15000*****11980.33**3019.67~  
CLP*777777*1*15000*11980.33**MB*1999999444445*13*1~
```

Example of information contained in an ANSI ASC X12 835 (provider remittance) transmission³⁵

CMS has not proposed a way to make this information readable—and therefore useful—to the patient. We are therefore unsure of whether CMS expects each Payer to convert the information into a patient-readable format before sending it to a patient (as they do now with a written Explanation of Benefits) or whether CMS expects a proliferation of apps to be developed that will translate the information for their users.³⁶ To the extent that CMS envisions that an app will translate the information for the patient, it should state this in the final rule to avoid confusion.

Unfortunately, regardless of whether an app translates the information, physician burden will increase when a patient tries to share his or her claims information with his or her physician. Not only would

³⁵ Available at <http://www.x12.org/examples/005010X221/dollars-and-data-sent-together/>.

³⁶ As of April 3, 2019, CMS lists 17 apps on its website as compatible with Blue Button 2.0.

physicians, too, find the information unintelligible without the use of an app or other technology to translate it, but also their certified EHRs are read-only, meaning that even if a physician could make heads or tails of the information, he or she would still need to scan as a PDF or hand-input the information into the EHR. (Whether EHRs should have write capability must be fully considered outside of this Proposed Rule and comment letter as that would present serious security concerns, among others.)

CMS should continue to promote its Blue Button 2.0 sandbox to developers to increase the number of available apps that can digest information contained in the HIPAA Transactions. Simultaneously, we urge CMS to temper patient expectations about the utility of receiving claims information, as it has continued to publicly state that access to these administrative data sets will “[make] it easier for people to make more informed decisions about their healthcare needs.”³⁷ We also encourage CMS to work with ONC to add data elements related to administrative transactions to the USCDI, which will vastly expand the number of ways in which a beneficiary can access and utilize such information.

Data consistency

The AMA applauds CMS’ focus on the USCDI as the basis for information exchange within the health care system and is encouraging ONC to do the same in our comments on its information blocking proposal. Not only should a complete record be accessible, but also the data contained therein must also be consistent, understandable, and usable. For this to occur, data must be in a recognizable electronic package (data structure or syntax) and maintain a consistent meaning (data semantics). Just as the English language is built from words and grammar, the translation from data to knowledge can only occur if the meaning of data is consistent. However, levels of semantic interoperability vary greatly in the health care system. Physicians agree that the current level of interoperability is inadequate to support the necessary changes, reforms, and innovations desired in health care.³⁸ As a practical matter, the more data exchanged that lacks both semantic and syntactic interoperability, the less useful it is to physicians and patients.

This leads to another piece of the interoperability puzzle that the industry must address: data mapping. Mapping is needed so transmitted data can be used by the receiving EHR, not just viewed. For example, if a patient’s diagnosis includes the term “hypertension,” a simple interface can move this text to another system where it can be viewed. However, to be useful in automated alerts and care planning, mapping must translate this information so that it has the same “meaning” in the receiving system. To create the appropriate meaning, the “hypertension” text typically must be put into the correct part of the receiving EHR’s database so that the EHR “knows” the patient has this condition. Additionally, problems like hypertension often are comprised of many different attributes, all of which should be captured, stored, and transmitted in a common format. While this example may seem simple, the proprietary nature of EHRs and the lack of an agreed upon medical data model make this difficult—even with the increased use of standardized codes.

³⁷ CMS Fact Sheet, *CMS Advances Interoperability & Patient Access to Health Data through New Proposals*, available at <https://www.cms.gov/newsroom/fact-sheets/cms-advances-interoperability-patient-access-health-data-through-new-proposals>.

³⁸ Stanford Medical, *How Doctors Feel About Electronic Health Records National Physician Poll* by The Harris Poll, (June 2018), available at <http://med.stanford.edu/content/dam/sm/ehr/documents/EHR-Poll-Presentation.pdf>.

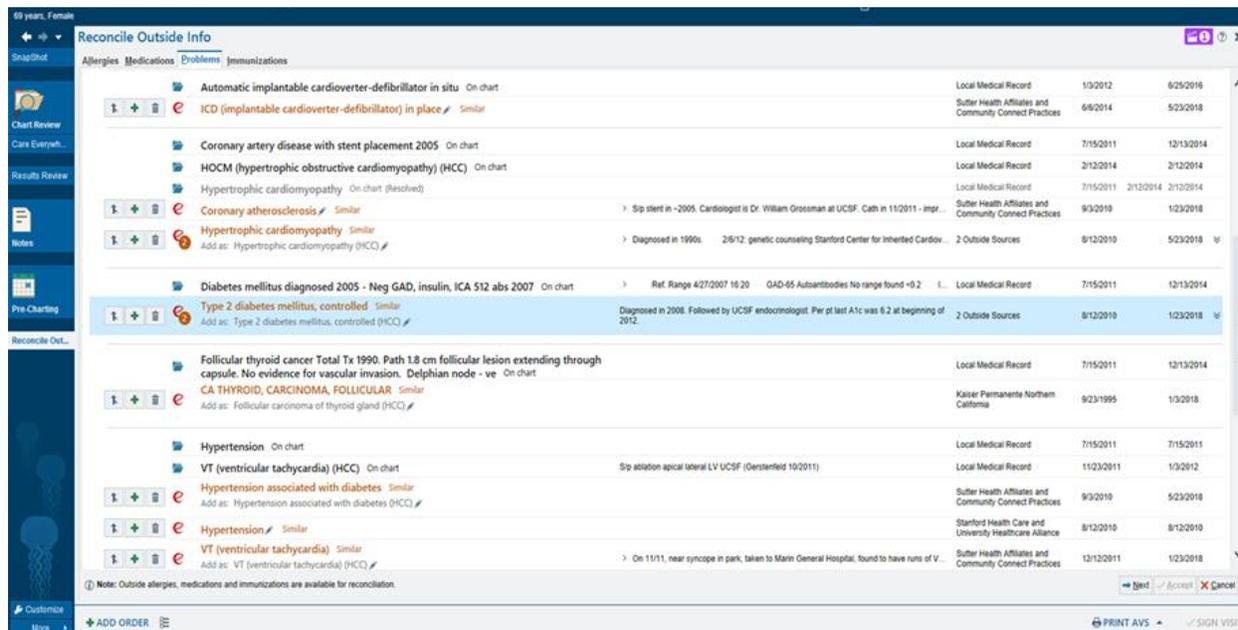


Image from an EHR prompting a physician to reconcile outside clinical information

Furthermore, EHRs typically do not identify components of the office note in the same manner. For instance, when a physician sees a note drafted in a Cerner EHR shown in an Epic EHR the information gets rearranged, misconstrued, or lost. This is because information stored in Cerner's terminologies and logic are not machine-readable by Epic's technology. For the information to interoperate between the two systems, the information must be translated into a standard terminology while, at the same time, preserving all the exchanged information's content and context. Providers spend hours documenting and searching for needed information when they lack access to interoperable and usable digital information.

To address this issue, the AMA has launched the Integrated Health Model Initiative (IHMI). The IHMI is a digital platform for stakeholder collaboration and clinical review to build a unified data model to organize data in an interoperable fashion. Utilizing the IHMI, different computer systems will be able to exchange data with unambiguous, shared meaning and be fully comprehensive across systems and clinical environments—enabling a true longitudinal patient health record independent of the data's originating source.

The IHMI will also support improvements in quality measurement. Currently, EHRs do not uniformly calculate eQMs across different vendors and practices due to the lack of specificity within the ONC's CEHRT program. Incorporation of data requires the development, maintenance, and refinement of administrative code sets such as the ICD, Current Procedural Terminology®, and clinical vocabulary standards such as SNOMED Clinical Terms®, Logical Observation Names and Codes® (LOINC), and RxNorm. Creating standards and mapping tools will facilitate working across these different codes and ensure consistency when data is exchanged. The AMA, through its IHMI, is participating in activities to support ontological structures that will provide pathways for better data collection and analytics.

We recognize that CMS alone cannot incentivize the health IT market to expose or standardize information. However, more needs to be done to increase access to all appropriate medical information—

for both patients and physicians. Access to granular data that is available, consistent, and retains the same meaning is a crucial element in improving health and lowering costs—and is ultimately the foundation of interoperability. This will require a coordinated approach involving clear objectives with a singular focus, planning and prioritization. **We urge CMS to continue to work with stakeholders and other federal agencies to focus interoperability efforts on promoting data consistency and access. This must include balancing policy goals with a sensible timeline. CMS should align future reporting programs around clinically led efforts—like the IHMI—that aim to advance terminologies, data elements, coding, and common data models to promote interoperability.**

IV. Patient Access to Information Through APIs

HIPAA provides individuals with a right to access the enrollment, payment, claims adjudication, and case or medical management records maintained by or for a health plan.³⁹ The AMA fully supports a patient's right of access and agrees with CMS that a patient should be able to easily receive this information from his or her health plan. Nevertheless, we note CMS' expectation that beneficiaries will use this information to shop for care and more effectively manage costs may not be realistic for many patients. Claims information can be complex and erroneous, and patients have varying levels of health and technology literacy. Medicare populations, in particular, often need assistance navigating the complexity of the system. As such, **beneficiaries and the individuals assisting them should have assurances that information provided across settings (e.g., online web portals, smartphone apps, payer policy booklets) contain consistent information.**

Additionally, the AMA supports the following specific measures to expand the availability of health care pricing information that allows patients and their physicians to make value-based decisions when patients have a choice of provider or facility:

- Health plans should provide plan enrollees or their designees with complete information regarding plan benefits and real-time, cost-sharing information associated with both in-network and out-of-network provider services or other plan designs that may affect patient out-of-pocket costs;
- Entities promoting price transparency tools should have processes in place to ensure the accuracy and relevance of the information they provide; and
- Patient confusion and health literacy should be addressed by developing resources that help patients understand the complexities of health care pricing and encourage them to seek information regarding the cost of health care services they receive or anticipate receiving.

We include below other ways we believe CMS can build upon its proposals to provide patients with health information to improve their care.

Drug benefit data

The AMA agrees with CMS that beneficiaries should have access to formulary data and urges CMS to extend this information to prospective beneficiaries as well—at least during open enrollment. We note that while it is helpful for patients to have formulary and pharmacy directory information, they often need clinical context provided by their physician to know what the most appropriate drug selection is for them

³⁹ 45 CFR 164.501 (*designated record set*) and 45 CFR 164.524(a)(1).

and their particular condition. Availability of accurate, real-time formulary and drug coverage information in a physician's EHRs at the point of prescribing is critical to having informed conversations with patients about drug selection, and has the potential to reduce drug costs for beneficiaries. Additionally, and equally important, provision of these data within the e-prescribing workflow will ensure physician awareness and completion of PA and step therapy requirements before a patient arrives at the pharmacy to pick up a prescription. Transparency of coverage restrictions in EHRs can thus prevent medication nonadherence and treatment abandonment.

Unfortunately, formulary data that is made available to both physicians and beneficiaries today is often not sufficiently granular to be useful, particularly with respect to the NCPDP Formulary and Benefit (F&B) standard, which is mandated under Part D. The F&B data—a batch file sent from pharmacy benefit managers (PBMs) to EHR vendors—is notoriously unreliable. This may be due to the lack of regular updates from EHR vendors to their physician clients or because of inaccuracies or delays in the information the PBMs send to the EHRs. However, the global problem with the F&B standard is that it usually provides data at a much higher level than is useful for an individual patient. For example, Sunshine Pharmacy might send an F&B file for their general national formulary, which might not be reflective of the formulary for a particular employer's drug plan or a Part D plan.

Given CMS' proposal that Payers provide information to beneficiaries using standards currently mandated under Part D, we interpret CMS' proposal to mean that the NCPDP F&B standard would be required for use, but we seek clarification if that is not the case. We are concerned that the F&B standard does not provide granular, patient-specific formulary and drug coverage information. It also does not provide the exact amount the patient will pay for a specific prescription—instead it may show co-pay ranges or symbols suggesting relative cost (e.g., \$ = cheap; \$\$\$\$ = top tier/expensive). For more granular detail, and for accurate patient-pay information, the AMA recommends that CMS require Payers to support a single real-time pharmacy benefit (RTBT) standard when made available.⁴⁰ We also note that the currently mandated version of the F&B standard (v 3.0) does not contain pharmacy directory information. The latest iteration (v. 52) does have a section on pharmacy networks and directories, but use of this version is not mandated.

CMS proposed requiring Medicaid and Children's Health Insurance Program (CHIP) plans to update formulary and pharmacy directory changes through the API within one business day, but did not identify a timeline for Part D updates. We recommend that CMS ensure that updates for Part D are consistent across platforms to avoid unnecessary confusion of beneficiaries and those who may be assisting beneficiaries with care decisions. Part D plans should also be required to make formulary and pharmacy directory information for an upcoming year (e.g., 2020) available through the API by October 15 of the preceding year (e.g., 2019), in accordance with current Part D policy.

⁴⁰ The National Council for Prescription Drug Programs (NCPDP) has been developing an electronic standard for the communication of real-time prescription drug coverage and pricing information, including therapeutic alternatives, between payers and prescribers over the past few years. The AMA participates in the NCPDP group involved in this effort and expects that a standard RTBT will be published within the next year. The AMA does not support a policy that would permit plans to each implement different RTBTs, as this could result in an overwhelming, expensive, and burden proposition for both EHR vendors and physicians. For additional information, we refer you to our letter to CMS on Modernizing Part D and Medicare Advantage to Lower Drug Prices and Reduce Out-of-Pocket Expenses, available at <https://searchf.ama-assn.org/undefined/documentDownload?uri=%2Funstructured%2Fbinary%2Fletter%2FLETTERS%2F2019-1-25-Letter-to-Verma-re-Part-D-MA-Drug-Pricing-Comments.pdf>.

In addition to the policies CMS has proposed in this rule, the agency should foster additional transparency between Payers and beneficiaries by implementing the following policies:

- Payers must provide 60 days-notice of changes in retail pharmacy networks to both beneficiaries and all physicians treating these patients;
- Payers making changes to their pharmacy network must allow beneficiaries to designate a new pharmacy of choice within the network; and
- When Payers mandate prescription transfers due to a change in their retail pharmacy network, the Payer and pharmacies within their network must have mechanisms in place to seamlessly transfer the prescription, as initially prescribed with regard to refills, substitutions, and other pertinent prescription details, to the beneficiary's pharmacy of choice without the need for the beneficiary or physician to initiate such transfer, as well as safety mechanisms to ensure that the formulation which has been established and tolerated is available to the beneficiary without a lapse in dispensing.

Prior authorization information

In addition to providing beneficiaries with adjudicated claims data, standardized encounter data, provider directory data, clinical data, and (as applicable) drug benefit data through an API, **Payers should provide beneficiaries (and prospective beneficiaries) and providers with information about medications and services requiring prior authorization.** An AMA-convened workgroup of 17 state and specialty medical societies, national provider associations, and patient representatives developed best practices for prior authorization and other utilization management requirements by identifying the 21 most common provider and patient concerns (the Principles). Over 100 additional stakeholders have signed-on in support of the Principles, one of which states: "Utilization review entities should publicly disclose, in a searchable electronic format, patient-specific utilization management requirements, including prior authorization, step therapy, and formulary restrictions with patient cost-sharing information, applied to individual drugs and medical services. Such information should be accurate and current and include an effective date in order to be relied upon by providers and patients, including prospective patients engaged in the enrollment process. Additionally, utilization review entities should clearly communicate to prescribing/ordering providers what supporting documentation is needed to complete every prior authorization and step therapy override request."⁴¹

To reduce administrative burdens and promote access to safe, timely care, the AMA, along with the American Hospital Association, America's Health Insurance Plans, American Pharmacists Association, Blue Cross Blue Shield Association, and Medical Group Management Association, released the "Consensus Statement on Improving the Prior Authorization Process" in January 2018 (the CS).⁴² The CS reflects agreement between health care providers and health plans on key reforms needed to reduce PA hassles and enhance patient-centered care and states the importance of transparency and communication between health plans, health care providers, and patients to "ensure timely resolution of prior

⁴¹ Prior Authorization and Utilization Management Reform Principles, available at <https://www.ama-assn.org/sites/ama-assn.org/files/corp/media-browser/principles-with-signatory-page-for-slsc.pdf>.

⁴² Consensus Statement on Improving the Prior Authorization Process, available at <https://www.ama-assn.org/sites/ama-assn.org/files/corp/media-browser/public/arc-public/prior-authorization-consensus-statement.pdf>.

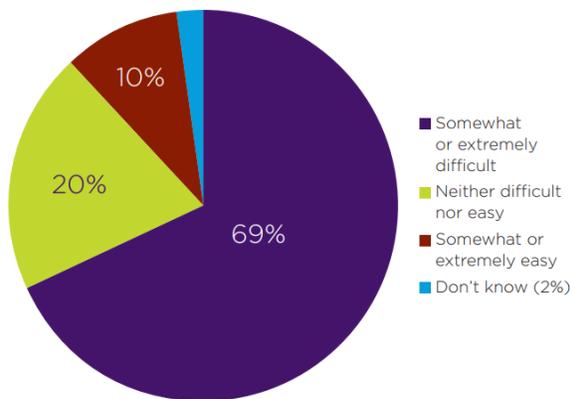
authorization requests to minimize care delays and clearly articulate prior authorization requirements, criteria, rationale, and program changes.”⁴³ The CS represented a landmark agreement on what is traditionally a contentious issue between the physician and health plan communities. The signatories agreed to “Encourage transparency and easy accessibility of prior authorization requirements, criteria, rationale, and program changes to contracted health care providers and patients/enrollees.”⁴⁴

Unfortunately, overall progress on PA reforms is negligible, with few meaningful changes to plans’ PA programs evident more than a year since the release of the document. Almost seven in 10 (69 percent) of 1,000 practicing physicians surveyed in 2018 report that it is difficult to determine whether a prescription or medical service requires PA, demonstrating that many of the PA reforms agreed to in the CS have yet to be widely implemented by health plans.⁴⁵

Transparency and communication regarding PA

CS agreement Encourage transparency and easy accessibility of PA requirements, criteria, rationale and program changes to contracted health care providers and patients/enrollees.

Survey Almost seven in 10 (69%) physicians report that it is difficult to determine whether a prescription or medical service requires PA.



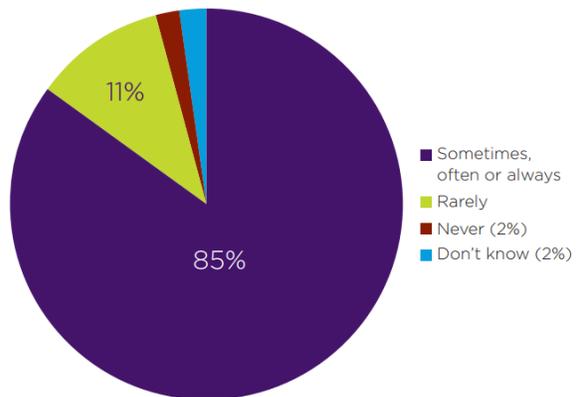
Total does not sum to 100% due to rounding.

Q: How difficult is it for you and/or your staff to determine whether a prescription medication or medical service requires PA?

Continuity of patient care

CS agreement Encourage sufficient protections for continuity of care during a transition period for patients undergoing an active course of treatment when there is a formulary or treatment coverage change or change of health plan that may disrupt their current course of treatment.

Survey An overwhelming majority (85%) of physicians report that PA interferes with continuity of care.



Q: How often does the PA process interfere with the continuity of ongoing care (e.g., missed doses, interruptions in chronic treatment)?

⁴³ Consensus Statement on Improving the Prior Authorization Process, available at <https://www.ama-assn.org/sites/ama-assn.org/files/corp/media-browser/public/arc-public/prior-authorization-consensus-statement.pdf>.

⁴⁴ Consensus Statement on Improving the Prior Authorization Process, available at <https://www.ama-assn.org/sites/ama-assn.org/files/corp/media-browser/public/arc-public/prior-authorization-consensus-statement.pdf>.

⁴⁵ Industry Checkup: Measuring progress in improving prior authorization, available at <https://www.ama-assn.org/system/files/2019-03/prior-auth-survey.pdf>.

To the extent that CMS has committed to utilizing the Da Vinci project both to communicate PA requirements and (in another use case) exchange data to complete PA decisions, all Payers should be required align with the project. As always, having various payers use different processes for PA exponentially increases PA burdens, so if CMS is fully committed to Da Vinci for their PA process, other payers should use this technology. **CMS should require all Payers to select a single API for Da Vinci/coverage discovery and should urge other payers to follow suit so that each payer does not have its own PA API.** Multiple PA APIs would be costly and burdensome for physicians to support.

Request for information sharing between payers and providers through APIs

The AMA is generally supportive of the concept of information sharing between payers and providers through APIs. The AMA appreciates CMS' acknowledgement that such an exchange should be at the direction of the patient. As described throughout this letter, patient notice and meaningful consent are key factors in maintaining and building trust between a patient and physician. Subject to other state and federal privacy laws, such notice and consent need not occur every time a provider accesses a patient's records. Instead, the patient and physician should have an established relationship and be aware that his or her physician is coordinating with his or her payer and other providers for purposes directly related to his or her treatment or payment for such treatment.

As CMS explores sharing information between payers and providers, CMS should consider the HIPAA electronic attachments standards as a potential starting point because of its querying, response, and acknowledgement elements. The standards are also applicable to claims management, prior authorizations, and other administrative data processes. As noted above, the AMA objects to providing payers unfettered access to a physician's EHR.

V. Provider Directories

CMS is proposing to require MA organizations, state Medicaid and CHIP fee-for-service programs, Medicaid managed care plans, and CHIP managed care entities to make standardized information about their provider networks available through an API so that a beneficiary (or future beneficiary) can use an app to access the directory. CMS notes in the rule that provider directories make key information about health care professionals and organizations available, including hours of operation, languages spoken, specialty services, and availability for new patients, and that the directories serve as a resource for the provider community to facilitate referrals, transitions of care, and care coordination. **As such, we wholeheartedly support CMS' proposal that Payers expose provider directory information through an API to current enrollees, prospective enrollees, and the general public. We advise CMS to make it a requirement for QHPs in FFEs, as well. We also urge CMS to require Payers to update their provider directories in real-time and to expeditiously correct errors.**

Provider directories need to be easy to access, user-friendly, and accurate. Accurate provider directories are essential to patients when choosing plans and in helping regulators monitor network adequacy. The AMA remains deeply concerned about provider directory inaccuracies, which can create significant barriers in access to care. As the Washington Post notes, many patients—particularly those needing care for chronic conditions—choose their insurance company based on whether they can obtain a plan that

includes their preferred physicians.⁴⁶ One misstep in this process can result in patients receiving surprise bills as a result of seeing out-of-network physicians. Payers should not be permitted to maintain erroneous directories at a beneficiary's (literal) expense.

Unfortunately, many Payers, notably MA plans, fail to provide accurate provider directories. Evidence from three separate MA audits conducted by CMS from 2016 to 2018 exhibit ongoing inaccuracies in online provider directory information, with the lack of improvement in this critical information source globally affecting patient access and quality care delivery.⁴⁷ The types of inaccuracies included the following: (1) the provider was not at the location listed; (2) the phone number was incorrect; or (3) the provider was not accepting new patients when the directory indicated they were. Of greater concern, these errors were found to create significant barriers to access to health care services by MA patients and beneficiaries. In its 2020 Call Letter to MA plans, CMS emphasized the importance of accurate provider directories, saying that inaccuracies can bring plans' network adequacy into question, but did not finalize new policy to improve the directories as part of the MA and Part D call letter for next year. **The AMA remains deeply concerned about the persistent rate of error among provider directories, and strongly encourages CMS to implement and enact enforcement actions for Payers that demonstrate noncompliance.** Even if provider directories are made available to beneficiaries through an API, the information will be meaningless if it is not accurate.

Payers could reduce the administrative burden on themselves and on physicians if they would use a common system for updating provider directory information, such as the AMA/Lexis-Nexis VerifyHCP system.⁴⁸ The AMA created VerifyHCP, a one-stop solution for physicians and providers to update their directory information. By utilizing data from both the AMA Masterfile and LexisNexis, VerifyHCP was created as an online, user-friendly platform that enables practices to validate or update directory information through one channel for all participating health plans. This solution makes even more sense given that there is no mandated standard on provider directory information.⁴⁹

⁴⁶ Paige Winfield Cunningham, The Washington Post, *The Health 202: Obamacare plans face lawsuits over erroneous doctor directories* (March 19, 2019), available at https://www.washingtonpost.com/news/powerpost/paloma/the-health-202/2019/03/19/the-health-202-obamacare-plans-face-lawsuits-over-erroneous-doctor-directories/5c9011581b326b0f7f38f1cb/?utm_term=.77f679bc3349

⁴⁷ https://www.cms.gov/Medicare/Health-Plans/ManagedCareMarketing/Downloads/Provider_Directory_Review_Industry_Report_Final_01-13-17.pdf; https://www.cms.gov/Medicare/Health-Plans/ManagedCareMarketing/Downloads/Provider_Directory_Review_Industry_Report_Year2_Final_1-19-18.pdf; https://www.cms.gov/Medicare/Health-Plans/ManagedCareMarketing/Downloads/Provider_Directory_Review_Industry_Report_Round3_11-28-18.pdf

⁴⁸ VerifyHCP FAQs, available at <https://www.ama-assn.org/sites/ama-assn.org/files/corp/media-browser/verify-health-care-portal-faqphysician.pdf>.

⁴⁹ The X12 274 Transaction Set communicates provider directory information between providers and health plans, but it is neither mandated nor widely used.

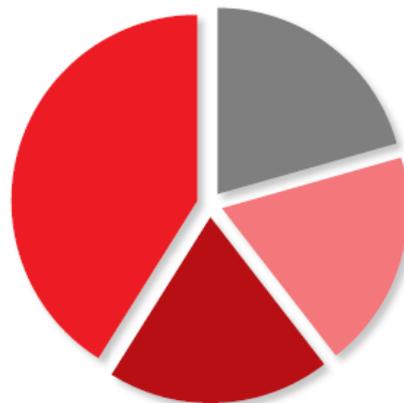
79% of all deficiencies impact the basics of making an appointment

41% Clinician should not be listed in the directory at this location

19% Clinician should not be listed at any of the directory-indicated locations

19% Phone number needs to be updated

21% All others



CMS should enhance its efforts to ensure directory accuracy by:

- Requiring Payers (as applicable) to submit provider directories to CMS every year prior to the Medicare open enrollment period and whenever there is a significant change in the physicians included in the network;
- Auditing directory accuracy more frequently for plans that have had deficiencies;
- Publicly reporting accuracy scores (as applicable) on Medicare Plan Finder;
- Taking enforcement action against plans that fail to maintain complete and accurate directories, or to have a sufficient number of physician practices open and accepting new patients; and
- Offering plans the option of using AMA/Lexis-Nexis VerifyHCP system to update provider directory information.

Plans should also make provider directory information available to physicians who seek to ensure their referrals are in a patient's network. Currently, finding out whether a patient's physicians are in each plan's network requires going separately to each health plan's website, finding the directory, and searching it. If a patient receives care from multiple physicians, this requires considerable time and effort. The plans are already required to submit their initial list to CMS in an electronic form that includes the physician's National Provider Identifier (NPI), so it should be feasible to not only make the lists downloadable, but also to link the information in the lists to Physician Compare. There is also currently no simple way for a physician to determine whether they are being accurately reported as in-network by the plans with which they currently contract and as out-of-network by other plans. A physician could use a Physician Compare linkage to find which plans say they have contracts with the physician. CMS should take the following steps:

- Require that MA plans submit their contracted provider list to CMS annually and whenever changes occur;
- Post the lists on the Medicare Plan Finder website; and
- Linking the provider lists to Physician Compare so that a patient can first find a physician and then find which health plans contract with that physician.

Finally, we note that CMS proposes to require States to update their provider directory information no later than 30 calendar days after the State receives the provider directory information or updates to provider directory information. First, MA plans are given 30 business (not calendar) days to update their information. CMS should modify the MA plan timeline to 30 calendar days. Furthermore, MA plans and QHPs in FFEs should have to provide updated provider directory information to States within one business day after the data is received by the MA plan or QHP. Failure to do so could result in a 60-day gap between when a plan receives updated provider directory information and when the State is required to provide such data to a current or potential beneficiary, which could result in old data that is not useful to a beneficiary.

VI. Payer to Payer USCDI Exchange

CMS is proposing to require Payers to coordinate care between plans by exchanging the information contained in the USCDI (at a minimum) upon enrollee request. CMS further requires that a recipient Payer incorporate the information received from a sending-Payer into the recipient-Payer's systems. We support CMS' proposal to the extent that it can promote patient continuity of care, as chronic, ongoing, effective treatment can be disrupted when patients change health plans and face new prior authorization or step therapy requirements. Sharing of the USCDI between plans could prevent or reduce these types of situations. 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 HIPAA's right of access (directed to a third party). However, we have significant concerns about other potential consequences of this requirement and whether excessive data access will lead to increased prior authorization and patient profiling—limiting coverage and access to care.

CMS must safeguard against pre-existing condition discrimination

Information sharing between Payers must come only at the beneficiary's direction and must never be used to deny or limit coverage even if a beneficiary requests the information exchange. Once a beneficiary has made the request, however, Payers must be prohibited from using this information to discriminate against a beneficiary—both newly covered and those in the application process.

As The Commonwealth Fund reports, the ACA has “dramatically improved the ability of people with preexisting conditions to buy coverage.”⁵⁰ The Commonwealth Fund conducted a survey finding that, in 2010, before the law passed, “70 percent of people with health problems said it was very difficult or impossible to buy affordable coverage, and just 36 percent said they ended up purchasing a health

⁵⁰ Sara R. Collins, *The ACA Protects People with Preexisting Conditions; Proposed Replacements Would Not* (Nov. 1, 2018), available at <https://www.commonwealthfund.org/blog/2018/aca-protects-people-preexisting-conditions-proposed-replacements-would-not>.

plan.”^{51,52} It notes that by 2016, “the percentage of people who had trouble buying an affordable plan had dropped down to 42 percent—still high but much improved—and 60 percent ultimately bought a plan.”⁵³

If protection for pre-existing conditions goes away, this provision could allow a Payer to uncover data showing the patient had been previously treated for a condition and deny that care. Or the Payer could determine that the patient had already received imaging or another service from another plan and therefore deny coverage of that imaging service. Or, seeing that the prospective patient has multiple chronic conditions, the Payer could perhaps deny health insurance coverage altogether. In fact, 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:

“The doctors and providers are not in control of medicine anymore,” says Harry Lawrence, owner of Advanced Oxy-Med Services, a New York company that provides [continuous positive airway pressure, or CPAP] supplies. “It’s strictly the insurance companies. They call the shots.”

But the companies’ practices have spawned lawsuits and concerns by some doctors who say that policies that restrict access to the machines could have serious, or even deadly, consequences for patients with severe conditions. And privacy experts worry that data collected by insurers could be used to discriminate against patients or raise their costs⁵⁴

To help ensure that patients are able to receive the care they need in a timely manner, 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.

CMS must prohibit Payers from conditioning network participation on unlimited or automated access to the USCDI

Again, we understand that HIPAA permits a patient to request that his or her records be sent to a third-party under a patient’s right of access, and we support a patient’s right to do so. We note, however, that

⁵¹ Sara R. Collins, Munira Z. Gunja, Michelle M. Doty, and Sophie Beutel, *How the Affordable Care Act Has Improved Americans’ Ability to Buy Health Insurance on Their Own*, available at <https://www.commonwealthfund.org/publications/issue-briefs/2017/feb/how-affordable-care-act-has-improved-americans-ability-buy>.

⁵² Sara R. Collins, *The ACA Protects People with Preexisting Conditions; Proposed Replacements Would Not* (Nov. 1, 2018), available at <https://www.commonwealthfund.org/blog/2018/aca-protects-people-preexisting-conditions-proposed-replacements-would-not>.

⁵³ Sara R. Collins, *The ACA Protects People with Preexisting Conditions; Proposed Replacements Would Not* (Nov. 1, 2018), available at <https://www.commonwealthfund.org/blog/2018/aca-protects-people-preexisting-conditions-proposed-replacements-would-not>.

⁵⁴ 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>.

the ultimate source of the USCDI's clinical data is a clinician. A Payer will not necessarily have a beneficiary's complete USCDI, which would be needed for Payer A to comply with a beneficiary's request that it send his or her USCDI to Payer B. We are therefore concerned about how CMS envisions a Payer complying with this regulation if the Payer does not have the full USCDI.

We anticipate that some commenters will suggest that Payers be allowed to pull information out of a provider's EHR via API to relieve burden on the patient and physician—in fact, some payers are already doing it, either as an elective offering⁵⁵ or through contractual requirements (see screenshot pasted in below).

ACCESS TO EMR

When Health Net requests access to EMR, the provider will grant Health Net access to the provider's EMR in order to effectively case manage members and capture medical record data for risk adjustment and quality reporting. There will be no other fees charged to Health Net for this access.

Relevant sections of Health Net's provider operations manuals have been revised to reflect the information contained in this update as applicable. Provider operations manuals are available electronically in the Provider Library, located on Health Net's provider website as listed in the right-hand column.

*Excerpt from Health Net (now California Health and Wellness) Provider Update (March 21, 2019)*⁵⁶

Compliance with this requirement would seem a logical use case for payers. 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., paying less 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. **We strongly oppose any type of automatic, unfettered Payer access to a physician's EHR, including through contractual means.** API access requires privacy and security guardrails that have not been discussed in this rule. Physicians must not be forced to allow a Payer electronic access to the practice's EHR as a way to facilitate Payer access to the USCDI.

The AMA has continuously maintained that an expressed “need” for information—including for care coordination purposes—does not confer a right to such information, particularly when it conflicts with a patient's wishes. Some parties may reject this principle as too deferential to patients' rights at the expense of administrative feasibility. However, the AMA believes that this approach properly balances the interests at stake. As such, we urge CMS to 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 law; (b) physicians may use their best judgement in responding to a request from a Payer for clinical

⁵⁵ UnitedHealthcare Enterprise Medical Records Program: An Easier Way to Share Medical Records, <https://www.uhcprovider.com/en/resource-library/uhc-enterprise-medical-records.html>

⁵⁶ See California Health & Wellness Provider Manual (March 2019), available at https://www.cahealthwellness.com/content/dam/centene/cahealthwellness/pdfs/CHW_Provider_Manual_3.18.19.pdf

information; and (c) Payers may not condition provider participation in a plan on a contractual agreement to fulfil requests for the USCDI.

Claims information can be erroneous and duplicative

In an effort to assist patients with the development of a longitudinal health record, CMS proposes to require Payers to integrate information received from other Payers into their own systems. We are concerned about the integrity of the claim information, particularly as a longitudinal health record builds across multiple payers. Who becomes responsible for ensuring that claims data is synthesized correctly without duplicate or conflicting information? The AMA has already seen examples from our members of how unstandardized data entry can create confusion about the most appropriate entry to keep when there are multiple similar options; we fear that similar results could occur as a result of this proposal given the various ways that certain conditions are coded. A Payer's attempt to reconcile the information is likely not the best solution given that the Payer will not necessarily have the appropriate clinical data to make such a determination. Furthermore, each Payer will likely expose claims elements with a mix of standards-based data representation, proprietary data models, unique health system or plan attributes, and patient-readable formats. Accordingly, the burden of ensuring accuracy will fall to the patient or—most likely—the physician. We encourage CMS to re-examine its proposal to have Payers integrate information from other Payers into their own or propose a mechanism to ensure quality, consistent, and accurate data that does not overly burden physicians and patients.

VII. Care Coordination Through Trusted Exchange Networks

CMS is proposing to require Payers to participate in a trusted exchange network (TEN) to allow for broader interoperability beyond one health system or point to point connections among payers, patients, and providers. CMS also notes—in context of ONC's draft Trusted Exchange Framework (TEF) from January 2018—that it is considering proposing in the future an approach to payer to provider interoperability that leverages existing trust networks to support care coordination and improve patient access to their data.

Overall, the AMA supports the general goals of TENs, including the ability to (1) provide physicians access to health information about their patients, regardless of where the patient received care; (2) provide patients and their caregivers access to their health information electronically without special effort; and (3) ensure that organizations accountable for managing benefits and the health of populations can receive necessary and appropriate information on a group of individuals.

CMS should ensure that physician participation in TENs is voluntary

We encourage CMS to address issues of physician choice and voluntary participation when evaluating the use of TENs to facilitate payer-provider interoperability. We note that some of the potential use cases outlined in ONC's draft TEF raised questions as to physicians' ability to willingly participate (or not participate) in trusted networks. Due to the sensitive nature of electronic health information and the potential disruption to physician practices involved in implementing the required technology, **the AMA underscores the importance of ensuring that physicians understand and can willingly elect to participate in information sharing via TENs.**

Specifically, in many states and cities, physicians' financial viability is entirely dependent on participation in particular health insurer networks. For example, 43 percent of U.S. metropolitan areas have a single health insurer with at least half of the commercial insurance market share.⁵⁷ In locations such as these, physicians would face potentially insurmountable financial disadvantages if they were to choose not to participate in the dominant insurer's network. In turn, this would force physicians to agree to the dominant insurer's terms of participation for a TEN that they might otherwise oppose, including participation in a TEN about which they have technological or security concerns.

Additionally, payers might require a physician to participate in a particular health information exchange network as a condition of participation in a plan. Physicians could also be forced to join multiple TENS based on different health plans' requirements for network providers, resulting in the physician needing to comply with multiple network requirements, policies, and fees. This would likely impose significant burdens upon practices—particularly smaller practices with already strained resources. **As a result, we recommend that CMS include language in its final rule that protects physicians' ability to voluntarily join a TEN and prevents insurers from requiring TEN participation as a term of network contracts.**

CMS must protect the minimum necessary standard

With respect to future policies related to payer-provider interoperability, CMS should ensure that Payers have access only to information they need, consistent with HIPAA's minimum necessary standard. The AMA agrees that reducing the difficulties inherent in accessing medical information at the individual or population health level is an important goal; however, we have concerns with the potential pitfalls of stakeholders having unprecedented access to wide swaths of information across the health care system. Current data request processes, while limiting, are narrowly scoped for specific use cases and involve some level of "gating" that helps prevent improper use and disclosure, and helps enforce compliance on both ends of the transaction (collection (query) and disclosure). **CMS must ultimately include policy mechanisms to limit data exchange in response to both broadcast and directed queries to the minimum amount of information necessary.**

ONC's Trusted Exchange Framework

The AMA provided comments to ONC during its first public comment period on the TEF. Our comments highlighted the importance of recognizing ongoing efforts by private sector stakeholders, and we appreciate ONC's efforts in the draft TEF to survey the HIE landscape and identify areas where greater harmony could lower exchange cost, complexity, confusion, or other friction points.

We also recommended that ONC consider realistic and achievable goals for the TEF, that the agency derive these goals from provisions within the 21st Century Cures Act (Cures), and use the goals as a metric for measuring success. Furthermore, we recommended avoiding duplication of existing agreements and additional complexity and burden on physicians. Our major goals for a successful TEF include the following:

⁵⁷ American Medical Association, *Metro areas increasingly dominated by single insurance companies* (Oct. 23, 2017), available at <https://www.ama-assn.org/press-center/press-releases/metro-areas-increasingly-dominated-single-insurance-companies>

- The TEF should address, at a national level, the business, technical, and governance components of interoperability to achieve patient-centered care;
- The TEF should incorporate Cures provisions around vendor information blocking and access to longitudinal patient health records while also limiting administrative burden; and
- The TEF should empower physicians and patients with clear and up-to-date information about the value proposition, structure, and limitations of health information exchange networks.

We look forward to providing comment to ONC on the second draft of the TEF in a future letter.

VIII. Public Reporting and Prevention of Information Blocking on Physician Compare

The AMA has commented numerous times on the need for interoperability and views the seamless exchange of useful information as a key component in improving quality, enabling care coordination, and achieving patient goals. We understand that MACRA requires that physicians participating in the Quality Payment Program (QPP) demonstrate their certified electronic health record technology (CEHRT) is connected, supports the exchange of information, and the physician has not knowingly or willfully acted to block or limit interoperability. We have commented to CMS that a simple attestation is an appropriate mechanism to accomplish this goal while meeting the MACRA's requirement. However, physicians participating in the QPP must make three separate attestations, each of which encompass complex health IT issues with which most physicians are not familiar or do not fully understand. Specifically, physicians must attest to the implementation of health IT standards and validate that EHRs are "implemented in a manner that allows for the timely, secure, and bi-directional exchange of structured electronic health information." Not only is the technical implementation of health IT outside the control of most physicians, but more importantly, health IT vendors themselves have yet to establish secure and bidirectional exchanges between their own systems. Asking physicians to attest that they understand and comply with these requirements is well outside the scope of their medical training and forces them to inappropriately and needlessly assume risk. We also note that physicians participating in the QPP must utilize CEHRT, which by definition must support APIs that provide access to patient data.

CMS now proposes to publicly report the names of physicians who attest "no" to these statements under the QPP on Physician Compare, even though—by CMS' own admission—it has "already implemented what is required by...MACRA through the attestation requirements [it] has established in prior rulemaking."⁵⁸ CMS goes on to note that the prevention of information blocking attestation statements are required for a clinician to earn any points in the Promoting Interoperability (PI) performance category of the Merit-Based Incentive Program (MIPS). As such, if a physician attests "no" to those statements, he or she will receive zero points in one of the four categories of MIPS, which would significantly negatively impact his or her overall MIPS performance score. CMS also already posts on Physician Compare both a physician's PI performance category and overall MIPS performance scores. Finally, CMS acknowledges that physicians will be subject to the separate information blocking provisions proposed by ONC for HHS adoption at 45 CFR part 171. **These duplicative requirements contradict the Administration's effort to reduce regulatory burden.**

The AMA is unclear as to why CMS believes it necessary to propose yet another punitive measure related to information blocking, particularly given that it has declined to adopt other creative, positive incentives to encourage information exchange—particularly those that would encourage patient engagement while

⁵⁸ 84 Fed. Reg. 7610, at 7646 (Mar. 4, 2019).

promoting privacy and security. For example, the AMA has proposed the following activities for including in the MIPS Improvement Activities (IA) performance category library:

- Work with EHR vendors to learn about patient-facing apps so that the physician can discuss them with their patients and assist them with accessing their medical information; and
- Provide face-to-face and written education to consumers about privacy and security considerations when electronically accessing health data.

Neither activity was approved by CMS for inclusion, despite each proposal meeting multiple criteria established by CMS.

Additionally, in its 2017 QPP Reporting Experience Report, CMS found that one of the five top IAs reported by physicians was “engagement of patients through implementation of improvements in patient portal.”⁵⁹ The agency “noticed the desire to enhance access for patients through the widely selected” activity, stating that the goal of the activity was to allow for a bi-directional communication between patients and clinicians, which ultimately enhances access to care, promotes communication, and puts patients in control of their health information.⁶⁰ CMS also relayed in its insights on the PI category that it is “encouraged that MIPS eligible clinicians are seeking innovative ways to ensure that patients have timely and unrestricted access to their health information.”⁶¹ These findings demonstrate that physicians are prioritizing interoperability activities in the MIPS program. **CMS should move away from additional punitive levers and increase its efforts to provide positive incentives that will continue to increase rates of interoperability and patient access.**

IX. Provider Digital Contact Information

CMS is proposing to publicly report the names and NPIs of providers who do not have digital contact information included in the National Plan and Provider Enumeration System (NPPES) system and requests comment on the most appropriate way to pursue the initiative. It notes that entities seeking to exchange data in electronic health information exchanges need accurate information about the electronic addresses (e.g., Direct address, FHIR server URL, query endpoint, or other digital contact information) of potential exchange partners. We agree that including digital contact information in a national provider directory is an important and worthwhile effort. However, **we encourage CMS to support its development through positive incentives as opposed to public shaming, through Medicare enrollment/revalidation, or through Medicare reporting programs such as MIPS, as there may be valid or unforeseen reasons for which physicians do not include digital contact information in the NPPES.**

For example, we have heard concerns from physicians on the frontlines of high costs associated with moving data using Direct, which requires use of a health information service provider (HISP). A physician’s HISP may be his or her EHR vendor. CEHRT developers do not typically disclose which HISP they support for physicians to exchange Direct messages. This has impacted the adoption of Direct

⁵⁹ 2017 QPP Reporting Experience report, p. 22, referencing IA_BE_6. Available at <https://qpp-cm-prod-content.s3.amazonaws.com/uploads/491/2017%20QPP%20Experience%20Report.pdf>

⁶⁰ Id.

⁶¹ 2017 QPP Reporting Experience report, p. 24, available at <https://qpp-cm-prod-content.s3.amazonaws.com/uploads/491/2017%20QPP%20Experience%20Report.pdf>

and added to the confusion and cost associated with secure message exchange. Furthermore, CEHRT developers are not expected to share the addresses of their customers using Direct, citing intellectual property concerns, which limits the ability of physicians to include theirs in the NPPES—many physicians are not even aware that they have a Direct address. CMS should work with ONC to require CEHRT developers to report the Direct addresses of their customers to the NPPES and—rather than punish physicians who may not be aware of their Direct address, not be given their Direct address, or charged high fees to obtain and use the Direct address—publicize the names of the developers who fail to do so. This policy would increase the utility of Direct and further support the foundation of secure data, while also not being overly burdensome to the physician, since the information already maintained by the CEHRT developer.

Separately, we note for CMS that since the NPPES is a publicly-facing directory, physicians listing digital contact information may receive an influx of digital communication from a variety of parties (not only patients and covered entities, but also marketers, pharmaceutical companies, and sales agents). Physicians are already stretched thin from seeking prior authorizations, secure messaging through patient portals, and compliance with other regulatory requirements such as federal payment reporting programs—all on top of clinic hours—and may struggle to review in a timely manner all the digital communication they receive. We encourage CMS to evaluate whether making digital contact information available to the public could unduly burden the physician or even pose risks to patient safety if important clinical information is buried among the spam a physician will surely receive. **To address these concerns, CMS should make access to the NPPES accessible only to the provider and payer community (as opposed to public) or, alternatively, utilize an industry solution that is selected via a robust RFP process with input from cross-industry stakeholders.**

X. Revisions to the Conditions of Participation for Hospitals and Critical Access Hospitals

We appreciate CMS' proposal to improve care coordination through notifications of admission, discharge, and treatment. We support the intent of the proposal, but do have questions about details of the execution. We request that CMS clarify certain aspects of the proposal and address areas where we have identified potential for increased provider burden, including the following:

- How does CMS define an “established care relationship”? How close the relationship must be (i.e., is it a physician who sees a patient once a year? Once a month?)?
- What are CMS' expectations of physicians who receive ADT notifications? Must physicians review and incorporate into their EHRs every notification? Some physicians may receive multiple notifications a day on multiple patients.
- Will physicians receive payment to review all of the notifications to ensure they do not miss important health information?
- Will physicians be responsible for paying for additional server space to store the additional electronic health information they will receive?
- Will this proposal potentially disproportionately burden physicians who care for high-risk patients?
- How will CMS ensure that hospitals that respect a patient's request to not share their ADT information—even if there is no applicable privacy law—are not excluded from the Medicare program?
- If a hospital in an area with a limited number of hospitals or specialists is excluded, where will patients in that area go?

- Does threatening hospitals with exclusion from Medicare increase the risk of improper disclosure, particularly given the unclear meaning of “established care relationship”?

We agree 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 ADT is a desirable goal. However, CMS should not attempt to reach this goal by requiring new clinical standards in the form of conditions of participation (CoPs) or requirements. Furthermore, many of the entities at issue are at vastly different stages of health IT implementation and integration; we are unsure that hospitals possess the infrastructure, technology and interoperability capability required for CMS to make ADT notifications a requirement. Rather than trying to spur interoperability and care coordination through additional requirements in the CoPs or elsewhere, CMS should work to provide positive financial incentives for entities to adopt technology and engage in event notifications.

We are concerned that compliance fears and costs associated with new standards could hinder investments and actions to enhance interoperable data exchange. Furthermore, health care stakeholders have not had sufficient time to evaluate the impact of forthcoming regulations and enforcement around information blocking, and the operations of TEFCA and U.S. Core Data for Interoperability (USCDI)—each of which will affect interoperability going forward.

We strongly suggest CMS explore potential pilot programs in which it could test and evaluate this proposal. The pilot should be limited in time and scale, and collect feedback from hospital, physician, and patient stakeholders on the burden to benefit ratio.

XI. Advancing Interoperability in Innovative Models

Allowing APMs to customize use of health information technology

CMS describes its intention to utilize the Center for Medicare and Medicaid Innovation’s (CMMI’s) authority under section 1115A of the Social Security Act to test ways to promote interoperability across the health care spectrum. The AMA supports the goal of using innovative new models to test the best ways to promote interoperability and believes alternative payment models (APMs) should have choices regarding how health IT can best improve care delivery for each model.

Specifically, the AMA has repeatedly recommended that CMS take a different approach to assessing APMs’ use of health IT to coordinate and improve patient care. CEHRT has come to be widely viewed as a tool for documenting, reporting and billing instead of as a tool for improving clinical care, coordination, and patient engagement. Furthermore, CEHRT is identified as contributing to physician burden and burnout.⁶²

⁶² Tait D. Shanafelt, MD et al., *Relationship Between Clerical Burden and Characteristics of the Electronic Environment With Physician Burnout and Professional Satisfaction*, Mayo Clinic Proceedings, Volume 91, Issue 7, July 2016, Pages 836-84, available at <https://www.sciencedirect.com/science/article/pii/S0025619616302154>; <http://annals.org/aim/fullarticle/2546704>; Brian G. Arndt, MD et al., *Tethered to the EHR: Primary Care Physician Workload Assessment Using EHR Event Log Data and Time-Motion Observations*, Annals of Family Medicine, Vol. 15, no. 5, September/October 2017, Pages 419-426, available at <http://www.annfammed.org/content/15/5/419.short>.

Instead, the AMA believes physicians need health IT that responds to and supports physician, patient, and care team interactions, not merely CEHRT. Instead of requiring that 75 percent of APM participants use CEHRT, CMS should allow APM entities to attest that a percentage of APM participants are either using CEHRT or using health IT that “builds on” or is an extension of CEHRT, such as plug-and-play modules, to achieve the specific goals of the APM. Health IT that builds on or is an extension of CEHRT is a concept taken directly from CMS’ priorities in the PI QPP performance category.

For example, in addition to using certified EHRs, APMs would be able to attest to using customized messaging or care coordination technology developed for the unique needs of the patients in that APM. This approach rewards APMs for using innovative technology that meets physician and patient needs. This approach will also encourage significant improvements in technology to be developed that would lessen the burden on physicians. CMS needs to encourage health IT developers to listen to APM participants and learn what they need to enter, retrieve, exchange, and analyze data, instead of developing technology that is only as advanced as the federal government requires.

The AMA is also concerned that physicians, including physicians participating in APMs, have little to no control over their EHR’s ability to help achieve the APM’s goals. Health IT companies frequently charge fees for each and every requirement imposed by federal reporting programs. Vendors need to be held accountable for producing tools to advance care outcomes without burdening physician practices or APMs with exorbitant fees and lack of usability.

Data availability

Provide patients access to electronic health data

CMS notes its first principle for promoting interoperability in innovative model tests is to provide patients access to their own electronic health information. The AMA strongly supports this principle and urges CMS to include models that may use technology that interacts with patients to help ensure patients have easy access to their health data.

For example, SonarMD, an APM developed by an Illinois gastroenterologist, Dr. Lawrence Kosinski, creates a specialty medical home model for patients with Crohn’s disease and ulcerative colitis with support from Illinois Blue Cross Blue Shield. The model grew out of data that the payer provided to him showing that, of the more than 50 percent of Crohn’s disease patients hospitalized with complications of their disease, less than one third had seen any physician within the 30 days preceding their hospital admission. Interviews with the patients revealed that the symptoms of their disease had come to seem normal to them over time, so they had no way of knowing that a change needed to be made in their treatment plan to avoid a developing emergency. Under the Sonar model, participating gastroenterologists receive funding support for proactive outreach to patients by nurse care managers. Each patient receives a “ping” via text message, email or phone each month with a few structured questions. The nurses can use the patients’ responses to these questions, called Sonar scores, to alert the gastroenterologists if they need to see the patient or adjust their medication regimen. The Sonar model has cut the rate of hospitalizations in half, and was the first APM recommended by the Physician-Focused Payment Model Technical Advisory Committee (PTAC) to the Secretary of Health and Human Services.

Provide physicians with data needed to deliver high-value care

While the AMA supports patient access to health information, we urge CMS to also consider physicians' need for data to drive innovative care delivery. It has been difficult for physicians to provide higher-value care and succeed under APMs because they do not have access to the data needed to do so. For example, physicians developing proposed APMs cannot project how much Medicare and other payers would save because they cannot access payer claims data.

We recommend providing easy, affordable ways for physicians to access and analyze Medicare claims data—even before they apply to participate in an APM—and establishing effective Health Information Exchanges so that physicians can identify opportunities to reduce spending, measure the impacts of care delivery changes, and quickly identify when services for patients need to be changed.

Models leveraging non-traditional data

The AMA also supports CMS' plan to leverage non-traditional data in model design, such as data on food insecurity. We support testing the incorporation of social determinates of health to see if it can lead to more accurate risk adjustment. The AMA has previously noted that social risk factors such as dual eligibility or geographic area of residence have a significant impact on beneficiaries' potential outcomes, ability to follow treatment plans, and community and family support and should be accounted for in new payment models.

XII. Request for Information on Policies to Improve Patient Matching

The absence of a consistent approach to accurately identifying patients has resulted in significant costs to the health care system. Patient identification errors often begin during the registration process and can initiate a cascade of errors, including wrong site surgery, delayed or lost diagnoses, and wrong patient orders. As data exchange increases beyond traditional medicine, patient identification and data matching errors will become exponentially more problematic and dangerous. Precision medicine and disease research will continue to be hindered if records are incomplete or duplicative. Accurately identifying patients and matching them to their data is essential to coordination of care and is a requirement for health system transformation and the continuation of our substantial progress towards nationwide interoperability. The AMA shares the goals of CMS and ONC in increasing patient matching to improve patient safety, better coordinate care, and advance interoperability.

Patient matching algorithms and software

Before discussing the requirement of patient matching algorithms or software, the AMA believes that indicators surrounding proper validation should be first established as guidance and provide flexibility in allowing patient-matching technologies to mature. Indicators that are necessary for assessment and reporting include database duplicate rate, duplicate creation rate, and true match rate. The current lack of consensus, adoption, and transparency of such indicators makes communication, reporting, and cross-provider or cross-organizational comparisons impossible, impedes a full and accurate assessment of the extent of the problem, prohibits informed decision making, limits research on complementary matching methods, and inhibits progress and innovation in this area. Moreover, CMS needs to account for the fact that specific algorithms and software solutions are system, vendor, data, and organization dependent. Thus, any guidance or requirements should be algorithm agnostic.

CMS identifier

The AMA has concerns about requiring a CMS-wide identifier as being a step towards a government-issued unique patient identifier. CMS and ONC should be offering technical assistance to private-sector led initiatives that support a coordinated national strategy to promote patient safety by accurately identifying patients and matching them to their health information. A CMS identifier would go beyond such technical assistance and raises privacy concerns and risk that the identifier becomes a de facto ID for other potentially questionable purposes. Moreover, implementation and operation of a required identifier could be expensive and administratively burdensome. Furthermore, the presence of an identifier does not equate to a high assurance identity proofing process or a high assurance authentication process.

Use of USCDI

The AMA believes that CMS should coordinate with ONC to advance more standardized data elements for patient matching by leveraging the USCDI. Additionally, CMS and ONC should work together to establish guidance surrounding common issues that could be resolved by standardization, such as the following:

- Recording names with spaces, hyphens, or apostrophes;
- Listing addresses in single or separate fields (e.g., separately street names from the city and state);
- Including special characters in phone numbers; and
- Handling missing data for fields (e.g., SSN, email address).

Verifying data sources for identity proofing

The AMA believes that use of any potential data source for identity proofing and patient matching should only be used for those specific purposes. CMS should not support the use of identity proofing data sources for discriminatory reasons, eligibility determinations, or to limit medically necessary care.

Patient-generated data

Patient-generated data should complement patient-matching efforts to help properly engage patients. Patients should be engaged as an active participant in their identity management as early as possible to educate patients about the importance of proper patient identification and further reduce instances of patient matching errors. Accurate patient matching is a pre-requisite for the ability to enable patients to become more engaged in their data exchange. Additional consideration should also be given to understand whether these patient-generated data and associated tools present any workflow challenges in provider settings, such as with any IT tools that providers would need to access the data stored via smartphone applications or with the steps needed to incorporate that data into their EHR systems.