

February 1, 2021

Liz Richter  
Acting Administrator  
Centers for Medicare and Medicaid Services  
U.S. Department of Health and Human Services  
7500 Security Boulevard  
Baltimore, MD 21244

Dear Acting Administrator Richter,

The Electronic Health Record (EHR) Association previously submitted comments in response to the proposed rule, *Reducing Provider and Patient Burden by Improving Prior Authorization Processes, and Promoting Patients' Electronic Access to Health Information (CMS-9123-P)*, but because of the compressed review and comment deadline for that proposed rule, we did not have sufficient time to thoroughly formulate our responses to the Requests for Information that were included at the end of that document. We have since convened our members and enclose herein the responses to those questions; we appreciate your consideration of our input despite it being submitted later than requested, as we believe several very important topics are addressed in our responses.

The EHR Association's nearly 30 member companies serve the vast majority of hospitals, post-acute, specialty-specific, and ambulatory healthcare providers using EHRs across the United States. Our focus is on collaborative efforts to accelerate health information and technology adoption, assist member companies with regulatory compliance, advance information exchange between interoperable systems, and improve the quality and efficiency of patient care through the use of technology.

In our response, we express our support for respecting patients' preferences regarding data sharing. However, we also suggest that where data segmentation becomes too granular, it quickly risks becoming more complicated to manage and may inadvertently result in unexpected data being shared or important data being withheld. We further caution that clinicians need a complete view of the patient in order to provide appropriate care.

We also note that the behavioral health sector continues to face challenges in the adoption of technology that would be capable of supporting FHIR-based API exchange. We do not believe that, without some assistance, the behavioral health sector overall has the financial resources to adopt health

---

AdvancedMD	Cerner Corporation	Epic	MEDHOST	Nextgen Healthcare
Allmeds, Inc.	CPSI	Flatiron Health	MEDITECH, Inc.	Office Practicum
Allscripts	CureMD	Foodhold Technology	Medsphere	Sevocity - Division of Conceptual Mindworks, Inc
Athenahealth	eClinicalWorks	Greenway Health	Modernizing Medicine	STI Computer Services
BestNotes	eMDs	Harris Healthcare Group	Netsmart	Varian Medical Systems
Bizmatix	Endosoff	Lumeris	Nextech	

IT with sufficient capabilities to support electronic medical records amenable to meaningful exchange. We encourage CMS and other agencies to advocate for incentive-based support of health IT adoption in the behavioral health community.

On the topic of prior authorization, we suggest CMS support efforts to streamline the prior authorization process using electronic methods. Our expectation is that when payers make APIs available, they will encourage providers to use them to speed up the prior authorization process, and providers will ask their EHR developers to enable use of the APIs. We therefore ask CMS and payers to also evaluate what improvements should be made to reduce the need for service-level prior authorizations, which will further enhance the efficiency of coordinating and managing care.

Social risk data exchange is in its early stages and lacks consensus regarding screening tools or data points to be exchanged. Documentation must be consistent to be interoperable and usable by the clinician, so there is still much work to be done in this important area.

Our detailed comments follow. Thank you for the opportunity to share our expertise and experience on these issues.

Sincerely,



Hans J. Buitendijk  
Chair, EHR Association  
Cerner Corporation



David J. Bucciferro  
Vice Chair, EHR Association  
Foothold Technology

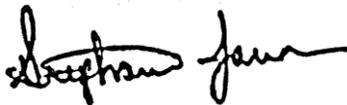
**HIMSS EHR Association Executive Committee**



Barbara Hobbs  
MEDITECH, Inc.



Cherie Holmes-Henry  
NextGen Healthcare



Stephanie Jamison  
Greenway Health



Rick Reeves, RPh  
CPSI



Alya Sulaiman, JD  
Epic



Courtney E. Tesvich, RN  
Nextech

## Electronic Health Record Association

Comments on RFIs contained in Reducing Provider and Patient Burden by Improving Prior Authorization Processes, and Promoting Patients' Electronic Access to Health Information (CMS-9123-P)

---

### Methods for Enabling Patients and Providers to Control Sharing of Health Information

***What role should patients and providers play in data segmentation decisions? Should patients assume this responsibility and are there mechanisms currently in place or available that could support the documenting of these preferences?***

The EHR Association broadly believes that it should be a patient's right to decide how their data is shared. At the same time, clinicians are severely hampered in making the best medical decisions without a complete picture of their patient's medical information. For example, a patient's decision to withhold information about their depression could lead to a redaction of that patient's MAO inhibitors prescription, which could in turn cause deadly interactions with medications used in an emergency department.

As clinicians have become more accustomed with sophisticated tools within EHRs, they expect clinical decision support that is based on a comprehensive view of that patient's data; EHR systems cannot provide such an accurate representation without discrete, complete access to full information. More work is needed to understand how to balance the needs of patient privacy against the clinician's mandate to do no harm, as well as to educate patients on the inherent risks in requesting data segmentation.

Informed consent has multiple purposes. First, for the patient, it helps ensure that they understand what it means to segment data and the possible outcomes of doing so, and confirms their decision in light of those possible consequences. Second, for clinicians, it provides an important opportunity to communicate the potential risks of data segmentation to the patient, and that it is not solely a clinician's decision that allows data to be segmented but a shared conscious decision with the patient's affirmed consent (should a negative outcome from segmentation occur).

Patient trust must be maintained through the segmentation process, which becomes increasingly difficult as segmentation becomes more granular. Consider a patient who wishes to withhold their treatment for alcoholism. While removing a single diagnosis from a patient's chronic problem list is technically feasible in many EHRs today, doing so does not hide an entire patient history of alcoholism, which might include other encounters, encounter locations, encounter complaints, care providers, those care providers' notes, allergies (e.g., to Antabuse or other treatment drugs), related medications, lab results, lab orders, patient messages, and any references to any of the former in any other notes in the chart.

Comprehensive redaction of this type is time consuming for medical professionals and error-prone. Even if such redaction was successful, a savvy clinician might discern the condition through the absence of certain data values, common comorbid conditions, or a pattern of emergency room presentations. Setting aside the clinical risks (already outlined) of conveying incomplete patient information to then be acted upon by the receiving care provider, assuring a patient that their alcoholism will be redacted, with that information then discerned by a recipient, could damage patient trust.

Ultimately, for data segmentation to have value, it must be:

- Safe
- Clearly understandable to enable informed patient consent directives
- Predictable
- Low effort to label data by provider

As data segmentation becomes more granular (withholding an entire record, withholding an entire class of information, withholding specific pieces of information), as well as associated retention policies, it strays further from these principles, and should be approached with caution. We encourage CMS and others, concurrent with improving the state of art, to additionally focus their attention on reducing stigma and introducing penalties for misuse of sensitive information. Such an approach is more likely to improve patient comfort, safety, and care.

We note that the context in which information is shared must be considered in order to determine what information can be safely redacted; e.g., an employee health clinic may not need to know about a patient's depression. However, despite the fact that this RFI is issued in the context of information being released from providers to payers, we remind CMS that initiatives like BCDA and DPC, which bring claims data to the point of care to inform clinical decision making, illustrate how data released for the purpose of payment may soon find its way back to providers for clinical care. Ultimately, given the advancement of standards and connections, shared data is increasingly expected to be complete and correct regardless of context, and it is in that spirit that we answer the questions in this RFI.

***Would providing opportunities to express these preferences negatively impact patients who are unable or choose not to state their preferences?***

To avoid negatively impacting patients who are unable or unwilling to share their preferences, regulators and the healthcare community should focus more attention on patient education regarding what information is in their file and the responsibilities that recipients have to protect that information and use it appropriately. The patient must be fully educated on the impact of their preferences as they are applied in order to make an informed decision. The patient should be cognizant of how their preferences affect the use of their clinical information downstream by other treating providers, and of the impacts that withholding sensitive data from disclosure may have on downstream treatment decisions. Likewise, the patient should be made aware of the consequences of not having their preferences applied. If a patient is simply left to apply preferences that constrain use of their data without that understanding, almost inevitably the downstream provider will lack important context or the ability to access clinical data that could manifest in patient safety or patient harm risks.

Further, efforts should be taken to destigmatize those conditions that patients are most likely to ask to withhold so they can feel more comfortable disclosing them, but abuse or unauthorized use of any and all data must always be appropriately addressed and penalized. Such an approach would allow more patients to feel comfortable with health information exchange without requiring every patient to understand the many nuances of health data segmentation, and would ultimately lead to better patient care and more holistic treatment.

Where segmentation is required, a coarser model of data segregation (withholding all data or very broad classes of data), has a higher chance of encouraging patient decision-making, as it is safer, simpler to comprehend, and more likely to be repeatable and trustworthy.

***How can patients be engaged in these decisions and acquire adequate understanding of how their data are being shared without burdening them?***

Asking patients to predict what information might be shared, both currently and in perpetuity, produces a much larger burden. In practice, it would likely fall to their practitioners to explain this process and its intricacies, which most providers are not well positioned to do, as many do not fully understand what is doable within their systems themselves. The coarser the model of segregation (meaning the entirety or large classes of data are withheld), the easier it is to be understood by both patients and providers, and the lesser the burden on everyone involved.

***Are there specific situations, use cases, or considerations that should limit how the impacted entity responds to a data segmentation request to either restrict uses and disclosures of some of the data, or to obtain access to some of the data from a patient or provider? Are there unintended consequences of such data segmentation requests or options? If so, how can they be addressed?***

Data segmentation guidelines must consider not just the provider inputting information and noting restrictions, but the receiving/requesting provider. Providers on both ends may find complex segmentation requests burdensome. Granular levels of segmentation are nearly unusable because of the burden placed on patients and providers to express or implement preferences, and for the receiver of any information to honor those preferences based on a patient's consent directives that may not be sufficiently reflected in their own system.

In addition, when choices are too complex, the tendency is often toward under-disclosing. Especially if the patient is not fully educated as to the impact of a data segmentation decision, there will be unintended consequences of data segmentation – namely overuse of segmentation – which will inevitably result in a patient safety/patient harm scenario. This may be because of either simple omission/hiding of data or because segmented data could not be included as an input into clinical decision support tools, resulting in avoidable patient harm.

We also are concerned that there could be reduced clinician trust in electronic health applications, if the users of an application believe that they may not be presented with all of a patient's existing data needed for them to make clinical decisions or perform their clinical responsibilities.

We note that it is important for clinicians to have a complete view of the patient not only to be able to provide appropriate care, but to enable more complete and accurate quality measurement reporting. Most data privacy concerns tend to be related to keeping private information out the hands of those who aren't providing direct patient care.

Finally, there may be potential consequences on data analytics or clinical research if the inclusion or exclusion of certain segmented data impacts the completeness or the integrity of the analytic or research outcome.

In addition to the need for a fully educated patient as to the consequences of a data segmentation decision, there needs to be consideration given to how recipients of the data or users of the data may appropriately override or engage in a "break glass" use of the segmented data if necessary to the clinical decision or clinical function at hand. We believe there has not been sufficient consideration of how this may be appropriately and legally done, in terms of the way in which this may be supported without creating a burdensome workflow impact on the downstream provider. We recommend that ONC and OCR consider making this a focus for future guidance development for HIPAA Privacy or for SAMHSA with 42 CFR Part 2. There has been little focus on how segmented data may still be appropriately used even if the interoperable understanding of what is sensitive by its nature is present without undue burden.

***What are examples of effective tools and methods for patients and providers to control access to portions of patients' health data? What is the readiness and feasibility of implementing successful access control methods?***

As we note above, current methods of segmentation become less and less feasible as controls attempt to become more granular, and the risk to patient safety increases as clinicians attempt to provide care from incomplete records. This is not only a technical problem but a larger cultural and socio-technical concern, and purely technical approaches will not solve it. We encourage CMS and other stakeholders to consider the larger context of how information is used and necessary protections before jumping directly to mandate technical solutions that will be difficult to deploy, difficult to educate on the implications, and difficult to meet patient and provider expectations.

The EHR Association recommends that CMS delay regulating this area until the problem space is fully understood. Only then can feasible standards be established and adoption become more widespread and consistent. Various pilot efforts have been undertaken that demonstrated that data segmentation can be done from a technical perspective, but more work must be completed to understand how to make that work consistently and at scale, including addressing the ability to segment, what policies are necessary, and when to segment using automated tools wherever possible. Additionally, patients should ideally be enabled to manage their directives based on informed decisions.

***Would requiring the ability to segment the data by, for instance, conducting data tagging, place additional burden on clinical providers? Please describe the nature of any additional burden. What are possible solutions to consider to address these concerns?***

Asking providers to manually tag specific data would be impractical and tremendously burdensome, and even more so for more granular segmentation requests. Not only is it time consuming, but providers do not always know the intricacies of how certain patient information can permeate the record (as described in our answers above). For the clinician, we believe that data element-level segmentation is impractical and burdensome due to the manual effort to identify all the data elements that need to be segmented. To move beyond the manual, this requires significant effort to determine what is sensitive by virtue of well-defined interoperable business rules that reflect semantic understanding of the meaning of the data, in order to properly apply tags to it. There are no such interoperable guidelines or specifications to inform this understanding and it is up to the implementer to determine or for the developer to determine as a “best guess” to comply with prevailing laws and regulations. This remains a problem that is unsolved by all of the standards development efforts for data segmentation; they address resolving the tag once sensitivity is determined, but that is not informed by any well-articulated interoperable guidelines or business rules but is dependent on clinician judgment.

Accordingly, asking providers to understand such complications and be responsible for the breach of patient trust if they fail to completely do so is unreasonable. To reduce provider burden, a more practical solution would be to encourage providers to share complete patient data or withhold it entirely. While we recognize the additional burden for patients, it is also possible for them to directly adjust their own record as necessary and re-disclose to intended recipients, as described in our previous responses in this RFI. While more nascent in its development and adoption, an alternative to manual tagging that has the potential to gain traction as a helpful resource in the coming years is similar functionality facilitated through artificial intelligence. This is not yet well-defined, however, and it is clear that technology alone will never be the sole solution to this challenge.

For the developer, in order to reduce all the manual identification a clinician may need to undertake to identify data to be segmented at a data element level, health information technology would need to support the creation of certain confidential data sets that would not only include specific individual data elements, but also contextual linkages between data elements necessary to represent a whole understanding of a sensitive data set. It is common that such linked data is required to accurately represent a whole of what is sensitive, such as certain laboratory results may be sensitive when linked to a specific diagnosis or for a specific medication item, but not absent that link. There are practical challenges for any developer or implementer to identify and substantiate these linkages on their own, lacking any interoperable guidelines or business rules to inform that understanding. That understanding is beyond the reach of most clinicians, and also beyond most developers or implementers.

For the patient, similar burdens and potential inadvertent effects also accrue because of content if data segmentation is not implemented accurately and appropriately. A patient may have no intention of applying a privacy preference in one context but not in another when the same clinical data is involved. For example, one patient may be using a prescription for birth control for contraception purposes (and as such consider the prescription sensitive). Another patient may simply be taking the prescription to

manage hormones and dermatological challenges that stem from a hormone imbalance. The latter patient may not consider the prescription to be sensitive, but without contextual understanding of how to define data element level tagging, mapping it as such could make it so.

***How do current consent practices inform patients of opportunities for patient engagement and provider discretion in responding to patient requests? What technology and policy gaps exist for achieving widespread successful segmentation practices?***

Currently, initial patient consent occurs as part of each organization’s patient intake process, frequently when checking in for the visit. While there is some opportunity in that process to inform the patient of how and with whom data could be shared, it’s likely that the patient isn’t considering the ramifications of data sharing consent during that initial process, and assumes that any sharing of data would be directed related to their healthcare needs. Providers as well as other stakeholders should engage with patients throughout their care to help them understand how information in their record could be used, the importance of being truthful and complete when relaying medical information, and the protections surrounding misuse of information that is allowed to be disclosed. We also encourage CMS to consider requiring “plain English” language to inform the patient.

Because there is also no consistent definition of what information may be “sensitive” and therefore should be segmented as a general policy, providers, exchange partners, and patients may all have a different interpretation. It will be important for the industry as a whole to have a consistent understanding in this area, so computable consent can come from a reliable basis of what is subject to privacy protection and patient permission, while ensuring it is not too granular, to enable practical and implementable decision-making by providers and patients.

It is important to note that adoption of segmentation practices is not yet widespread and remains an obstacle for provider organizations; even when available, healthcare organizations frequently choose not to activate it.

***What recommendations do stakeholders have to improve the data segmentation capabilities of existing FHIR standards? How would you describe the state of development projects or standards efforts planned or ongoing to address data segmentation (or segmentation of sensitive information) on FHIR or other standards? What are the key gaps or constraints that exist within ongoing and emerging efforts?***

From a technical perspective, FHIR® APIs have the ability to label and scope data at the higher level (resources that represent documents/groupings/data sets), and granular level (resources that represent individual data points). Thus, the ability to express the desired level of segmentation is not the challenge; rather, the same challenges identified in our responses above apply, as to finding a practical balance on how to segment based on well-defined and computable policies established in general or based on patient provided consent directives. Note that the standards capabilities in HL7 FHIR, HL7 C-CDA, and HL7 v2 are all in place in the latest releases, while other standards may still require further updates to enable consistent communication regardless of standard used (e.g., e-prescribing vs. reporting). Neither the existing SAMHSA Consent2Share nor the CDA-based Consent Directive ([HL7](#)

[CDA® R2 Implementation Guide: Privacy Consent Directives, Release 1](#)) are sufficiently mature and tested, nor is there an understanding of how to enable “continuous” access to the criteria indicating what to disclose and to whom.

The FHIR Security Labeling (a [DS4P implementation guide](#) is under development), along with the C-CDA focused DS4P and the recently published HL7 v2 ARV segment updates, provide the ability to tag using consistent label definitions. However, without the policy and directive framework around them, any implementation of the labels will be inconsistent and incomplete across the necessary systems.

Furthermore, other means of communication, e.g., NCPDP’s SCRIPT standards and ASC X12N’s claims standards under HIPAA, would need to have the ability and shared labeling to address consistency across any path the relevant data would flow. Limited and focused pilots have been valuable in order to identify potential opportunities and demonstrate that data can be labeled, but these pilots have also recognized that without addressing other socio-technical concerns, it will be challenging to scale a consent infrastructure that meets the expectations of patients, and of providers in particular.

Communication of and/or access to a patient’s consent directive must allow downstream recipients of the data unambiguous understanding of what they can or cannot re-disclose, based on clearly defined security labels and consent directives, including arriving at a consistent consent directive expression. We note that in general and especially without industry-wide agreement over policies, the most foolproof way to prevent downstream access to information, unfortunately, is to not disclose it in the first place, while fully relying on patient-mediated exchange based on patients selecting the data to be shared, which in itself has many unintended consequences and creates delays in sharing critical information for that care.

Most importantly, as described above, practical experience and consistent policies also remain unresolved, as do privacy issues across states. The primary focus at this point should be on establishing agreed-upon policies that are as consistent and compatible as possible across HIPAA, 42 CFR Part II, and states, in order to enable proper and practical labeling of the relevant data at the right level of granularity without (or with limited) user interaction so that the receiver can unambiguously act on it.

***What general data segmentation strategies can we leverage for the programs described in this proposed rule from standards like the Substance Abuse and Mental Health Services Administration’s (SAMHSA) Consent2Share and HL7 Data Segmentation for Privacy (DS4P)? What lessons can we learn from use of these existing standards?***

While HL7’s Data Segmentation for Privacy initiative is active, there remains insufficient activity at the policy, process, and educational level to enable providers, patients, and information systems to establish a manageable and practical consent and data disclosure management system. When the information is truly sensitive it should not be shared at all; any incremental segmentation would be burdensome. Workflow implications for this kind of segmentation are significant, and not widely in place.

As noted in prior EHR Association feedback to ONC and CMS, SAMHSA’s Consent2Share is based on an older FHIR version; there is no clear ownership and path to migrate to FHIR R4, which is required of

certified EHR technology in the 2015 Certification Edition Cures Update.

***Should preferences be something that data senders should try to honor but retain flexibility to deny in certain situations, when consistent with applicable regulations? For example, the HIPAA Privacy Rule requires a covered entity to permit an individual to request restrictions on the entity's uses and disclosures of PHI, but only requires the entity to agree to the request in limited circumstances.***

We agree that those sending electronic data should honor patient preferences within the privacy framework established by HIPAA, enabling providers to arrive at optimum clinical decisions based on an as-complete-as-possible patient record.

We stress again that a careful balance must be struck between the more practical higher level segmentation and overly granular segmentation considering the many challenges and risks involved in not sharing all relevant clinical data necessary to support optimal clinical decision making.

***What prevents patients and/or providers from recording, maintaining, or using a patient's privacy preferences when exchanging health information? How can data segmentation decisions be automated? Are there particular processes or workflows related to patient privacy preferences, consent, or data segmentation that could be improved by automation and/or standardization?***

Today, there is little adoption of standardized segmentation processes within and across provider organizations, and even less automation. While the focus of privacy policy discussions tends to be related to behavioral health, it is important to consider that a patient could ask for any information not to be shared (e.g., pregnancy), and some such requests may be technically infeasible or impossible to honor.

Currently, there are no standardized policies or definitions surrounding the sensitivity or privacy of information and what obligations such labelling imposes on the source or recipient of the information. Labelling data for segmentation without an agreed-upon understanding of what labels exist and what segmentation means is pointless because the sending and receiving entities could interpret the information differently. Instead, aligning these obligations across states and jurisdiction will be a prerequisite for segmentation to be implemented successfully on any broad scale. Additionally, patient education will be critical in order to enable patients to make informed decisions on who can access their data, while recognizing the role of providers in assisting patient decision-making.

## **Electronic Exchange of Behavioral Health**

***Can applications using FHIR-based APIs facilitate electronic data exchange between behavioral health providers and with other health care providers, as well as their patients, without greater EHR adoption? Is EHR adoption needed first? What opportunities do FHIR-based APIs provide to bridge the gap? What needs might not be addressed by the use of applications with more limited functionality than traditional EHRs?***

The behavioral health sector continues to face challenges in the adoption of technology that would be capable of supporting FHIR-based API exchange, including under the Meaningful Use and Promoting Interoperability programs. Although some eligible professionals and clinicians practicing behavioral health may have been able to benefit from these programs, many behavioral health clinical professionals could not.

The demands for clinical workflow automation to support clinical care delivery, electronic prescribing, medical record management and care management are not insignificant for behavioral health providers, even when compared to other clinical disciplines. If anything, they present a more complicated care scenario to address therapeutic, pharmacologic, counseling, referral management and sensitive information management needs. Behavioral healthcare services are often episodic and long-term, requiring ongoing care coordination and management.

The behavioral health sector overall has fewer financial resources available to fund the adoption of health IT with sufficient capabilities to support electronic forms of medical records amenable to meaningful exchange.

While we recognize that providers in the behavioral health and substance use disorder specialties may not need some of the clinical functionality that is included in EHRs on the market today, they and the patients being seen in this space do deserve robust and effective technology to mirror, as would be useful to them, that which is used in other care settings. Accordingly, we recommend that CMS, ONC and SAMHSA instead consider advocating for support of useful, clinically-relevant and interoperable IT adoption in the behavioral health community, including evaluating effective ways to do so without imposing any unnecessary burden or risk of impeding innovation.

***What levers could CMS consider using to facilitate greater electronic health data exchange from and to behavioral health providers? What costs, resources, and/or burdens are associated with these options?***

Many providers of behavioral health services do not generate enough revenue to support acquisition of an EHR, and behavioral health providers were not considered eligible for the Meaningful Use EHR adoption incentive program due to budgetary limitations, despite initial intentions to include them. It is highly possible that a program to incite the use of EHRs by behavioral health disciplines, much the way the Meaningful Use program did for other medical disciplines, would be necessary for the nation to see any real change in EHR adoption among this key group of providers, including additional training and financial support during the transition period. However, we note that a review of what worked effectively in the HITECH Incentive Program (Meaningful Use) and what ultimately ended up not being effective should be undertaken before any final decision is made. There is a very real risk of unintended consequences associated with impeded innovation, as has followed what has been, on occasion, an overly-prescriptive certification program.

***What levers and approaches could CMS consider using and advancing to facilitate greater electronic health data exchange from and to community-based health providers including use of relevant health IT standards as feasible? What costs, resources, and/or burdens are associated with these options?***

We applaud the efforts to date, but more alignment, with necessary controls for privacy, would be helpful. Additional work developing measures relevant to behavioral health would make the adoption of performance-based efforts easier for these providers, as would creation of common language and measures associated with Social Determinants of Health (SDOH). Behavioral health providers are a critical source of accurate SDOH information, so ensuring that their information exchange burden is minimal supports all providers and benefits patients. Easing (and inciting) this process for them is critical.

## **Reducing Burden and Improving Electronic Information Exchange of Prior Authorizations**

***What are the current barriers to transmitting prior authorization requests and receipts electronically? What actions could CMS and/or industry take to remove barriers?***

It's widely known that doctors find prior authorization requests burdensome and inefficient, and payers often require a very specific process that varies from one to the other. Paradoxically, electronic requests currently often incur an additional fee, inciting providers to use manual processes.

Provider frustration stems from a lack of consistency across payers, making it difficult for providers to standardize their procedure for submitting prior authorization requests. Consistent interactions across payers are one goal of the Da Vinci project's FHIR-based implementation guides, as well as enabling the expression of authorization rules in a computable format that can interact with source data expressed in an industry standard format (also FHIR-based). As that matures and the entire interaction can be managed using the FHIR-based standards, we recommend removal of the requirement to transition in to and out of X12 within the flow because HIPAA limits exchange to use of a standard less suited to the use case at hand even where a better alternative is available.

***Do the current methods for electronic transmission of prior authorization requests and receipts, including the adopted standard, and any that have been established and maintained by third-party health care insurers (including Medicare) provide the efficient and timely request and receipt of prior authorization decisions? Please provide relevant detail in your response.***

The EHR Association has no comment.

***Would the CMS CoP/CfC requirements for hospitals and other providers and suppliers be the appropriate lever by which CMS should propose new or additional provisions that would require the electronic request and receipt of prior authorization decisions? If so, under which provisions would this best be accomplished?***

Given the state of the industry and the current adoption level of the standards for prior authorization, we feel strongly that the CoP/CfC requirements are not the appropriate lever for CMS to enforce these provisions at this time. When payers make these APIs available, we expect the provider community will be eager to use them and will prioritize development from their EHR developers to do so, without regulatory penalties. If the enhancements are as beneficial to providers as has been promised, self-

driven adoption should be rapid and expansive. If the enhancements are not as beneficial as envisioned, then adequate time for revision of the standard is necessary prior to regulation.

## **Future Electronic Prior Authorization Use in the Merit-Based Incentive Payment System (MIPS)**

### ***Is this an activity that stakeholders identify as improving clinical practice or care delivery?***

While we support electronic prior authorization as an optional improvement activity, we do not recommend it be included as a MIPS measure. There is no certified technology nor standardization across payers, and because part of the transaction is outside of provider control, that puts it outside of MIPS requirements.

- ***When effectively executed, is implementation of such technology and use of these standards likely to result in improved outcomes?***
- ***If yes, should this activity be assigned a medium-weight or high-weight?***

We believe that use of electronic prior authorization can increase efficiencies and allow for more timely negotiation between provider and payer, but for the reasons listed above, we do not believe this activity should be required as a MIPS measure.

- ***Should CMS consider adding a measure to the Medicare Promoting Interoperability Program for eligible hospitals and critical access hospitals and the MIPS Promoting Interoperability performance category for clinicians and groups to encourage the use of electronic prior authorization through a payer's Prior Authorization Support API?***
- ***What are the primary considerations for developing such a measure?***
- ***How would the measure require the use of certified electronic health record technology?***

The EHR Association does not support adding a measure for prior authorization API use in the Promoting Interoperability (PI) category. Its inclusion as an Improvement Activity, where it is an optional item of benefit to those who have taken steps to adopt electronic prior authorization, is more appropriate.

We believe that CMS should not act to require electronic prior authorization measurements for PI ahead of the compliance date of this rulemaking. Even at that point, CMS should base its consideration upon the maturation and adoption level of an API-based interoperability capability for patient, provider and payer.

- ***Should the Prior Authorization Support IG be incorporated into potential future certification requirements for health IT under the ONC Health IT Certification Program?***

As payers would be responsible for creating and managing the APIs referenced in the NPRM, we recommend consideration of whether a certification approach is merited for payers to demonstrate their APIs' adherence to applicable standards and implementation guides.

However, we believe that adding certification requirements for health IT under the current or future ONC Health IT Certification Program should be unnecessary if the payers are held to a requirement to follow those standards and IGs already being embraced by certified technologies.

- ***Should CMS consider additional measures and activities under MIPS Quality, Cost, or Improvement Activities performance categories involving FHIR-based electronic prior authorization solutions?***
- ***If so, what are the primary considerations for developing such measures and activities?***
- ***What other approaches should CMS consider to help support clinician use of electronic prior authorization solutions such as the Prior Authorization Support API?***

We suggest CMS support efforts to make electronic prior authorization easier. Once payers make the APIs available, they will encourage providers to use them to speed up the prior authorization process, and providers will ask their EHR developers to enable use of the APIs. This is likely an area that market forces will naturally address.

### Accelerating the Adoption of Standards Related to Social Risk Data

- ***What mechanisms are currently used to exchange social risk and social needs data (EHRs, HIEs, software, cloud-based data platforms, etc.)? What challenges, if any, occur in translating social risk data collected in these platforms to Z-codes on claims?***
- ***How can health care payers promote exchange of social risk and social needs data? Are there promising practices used by public or private payers that can potentially be further leveraged in other settings?***

Social risk data exchange is in its early stages, and there is not yet consensus regarding assessments or data points to be exchanged. There are overlaps and gaps among the questions asked on the different screening assessment tools, which make population-level analysis of determinants more challenging. For example, the timeframe of questions varies (e.g. have you experienced a need in the past two years vs. one year vs. six months vs. are you currently experiencing), scoring methods vary, and survey tools do not cover the same or all relevant determinant data points, all of which make it difficult to understand the urgency of current needs and historical patterns. We also note that there is increasing evidence of potential racial or ethnic bias in current state data and analytics.<sup>1</sup>

There is currently little consistency in how SDOH factors are captured and documented within health IT, which also limits the value of the exchange of such data. While FHIR presents an opportunity for a more comprehensive approach as to how determinants are represented, there is still little to no consistency in how SDOH data is defined by data stewards, which presents itself in numerous ways in the industry.

For example, there is a significant lack of definitions or a data dictionary for the SDOH terms used in the ICD-10-CM Z-codes (neither the ICD-10-CM classification nor the guidelines provide definitions). The Z-codes that have been created are not often used in provider organizations; they are not included in standardized operational documentation processes, there is a lack of clarity around who can screen and document them, providers already experience a documentation burden, and there exists a perceived

---

<sup>1</sup> <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4638275/>

priority of social needs. Organizations therefore do not always feel that pulling data based on these Z-codes adequately reflects the social needs of their population and thus can perceive limited use in doing so.

We suggest that there is the need for further granularity to existing code categories Z55-Z65 to increase specificity needed to appropriately capture, analyze, and act on SDOH data in order to improve outcomes for both consumers and populations. For example, solving for an inability to pay for prescriptions is a completely different action using different resources than solving for the inability to pay for transportation, but both might currently point to use of Z59.9 (Low Income).

#### ***About the HIMSS EHR Association***

***Established in 2004, the Electronic Health Record (EHR) Association is comprised of nearly 30 companies that supply the vast majority of EHRs to physicians' practices and hospitals across the United States. The EHR Association operates on the premise that the rapid, widespread adoption of EHRs will help improve the quality of patient care as well as the productivity and sustainability of the healthcare system as a key enabler of healthcare transformation. The EHR Association and its members are committed to supporting safe healthcare delivery, fostering continued innovation, and operating with high integrity in the market for our users and their patients and families. The EHR Association is a partner of HIMSS.***

***For more information, visit [www.ehra.org](http://www.ehra.org).***

Cc:

Alexandra Mugge  
Director and Deputy Chief Health Informatics Officer  
Centers for Medicare and Medicaid Services