AHIMA
American Health Information
Management Association®

233 N. Michigan Ave., 21st Fl., Chicago, IL USA 60601-5809 | www.ahima.org | 312.233.1100

November 7, 2022

Kiran Ahuja
Director
US Office of Personnel Management
1900 E Street, NW
Washington, DC 20415

Charles P. Rettig
Commissioner
Internal Revenue Services
US Department of the Treasury
1111 Constitution Ave. NW
Washington, DC 20224

Lisa M. Gomez
Assistant Secretary
Employee Benefits Security Administration
US Department of Labor
200 Constitution Ave NW
Suite S-2524
Washington, DC 20210

Chiquita Brooks-LaSure
Administrator
Centers for Medicare & Medicaid Services
US Department of Health and Human Services
7500 Security Boulevard
Baltimore, MD 21244

To Whom It May Concern:

On behalf of the American Health Information Management Association (AHIMA), I am responding to the Department of the Treasury, Department of Labor, and Centers for Medicare & Medicaid Services' (CMS) Request for Information; Advanced Explanation of Benefits and Good Faith Estimate for Covered Individuals, as published in the September 16, 2022 Federal Register (CMS-990-NC).

AHIMA is a global nonprofit association of health information (HI) professionals. AHIMA represents professionals who work with health data for more than one billion patient visits each year. The AHIMA mission of empowering people to impact health drives our members and credentialed HI professionals to ensure that health information is accurate, complete, and available to patients and providers. Our leaders work at the intersection of healthcare, technology, and business, and are found in data integrity and information privacy job functions worldwide.

As part of the health IT community, AHIMA continues to support the development, implementation, and use of the Fast Healthcare Interoperability Resources (FHIR). This still in development set of standards could be one of the key pieces of technology that may be used to close the healthcare interoperability exchange gap and move the nation closer to nationwide interoperability. Until FHIR is complete and those tasked with implementing and using these set of standards have been consulted on testing and readiness, we caution CMS and other federal agencies from requiring FHIR as the single technical standard to solve healthcare data exchange. Instead, we encourage the federal government to pursue multiple potential solutions and to work with health IT end users to test and determine potential pathways for implementation of new standards and technologies.

The following are our responses to selected requests for information.

A. Transferring Data From Providers and Facilities to Plans, Issuers, and Carriers

What issues should the Departments and OPM consider as they weigh policies to encourage the use of a FHIR-based API for the real-time exchange of Advanced Explanation of Benefits (AEOB) and Good Faith Estimate (GFE) data?

AHIMA continues to support the use and implementation of the FHIR based API technology throughout health IT. FHIR continues to be a standard in development and, despite being on version five, is still a new entrant in the health IT arena. It is crucial for OPM to ensure the health system has multiple technical options to implement new requirements to ensure providers and developers are not reliant on one single piece of technology or standard in the event that technology either is not fully functional or available by the regulatory compliance deadline. OPM can ensure the worst-case scenario of the healthcare community having to implement an unimplementable standard does not happen by encouraging the development and implementation of multiple API standards, including but not limited to FHIR.

While OPM determines the appropriate API standards to propose for implementation to achieve the desired regulatory outcomes, it is also crucial to ensure the end users of these standards are included in the development and implementation process. AHIMA is a founding member of the Health IT End Users Alliance and is committed to ensuring robust real-world testing takes place before new technology and standards are mandated for implementation.[1] Too often front-line workers, or end-users, that interact with the technology find that the technical approaches and regulatory requirements are not sufficiently grounded in real-world experiences and do not consider the implementation pathway before being mandated. This in turn leads to significant workarounds to implement, the standards being unable to accomplish the required task, wasted money on failed implementations, and confusion from patients with respect to technological capabilities. There remain numerous opportunities for health IT end-users who use technology tools for care, as well as for patients, to guide the development of policies and standards that meet real-world needs and reduce burden.

As a member of the Health IT End-User Alliance, a group dedicated to advancing end-user perspectives in health IT policy and standards development, AHIMA believes the relevant agencies should approach providing access to AEOBs and GFEs through a culture of real-world testing. As members of the Health IT End-User Alliance, AHIMA believes real-world testing should inform/investigate whether the standard and/or policy will:

- Be implementable by health care organizations without significant effort beyond the value incurred by adoption
- Be effective at achieving its desired goal
- Encompass a complete solution to achieve the desired goal
- Not result in unintended consequences that would harm individuals (caregivers, patients, physicians, and other clinicians)
- Respect and accommodate the privacy needs of individual patients

[1] https://hitenduser.org/wp-content/uploads/2022/09/Real-world-testing-consensus-statement_FINAL.pdf

- Not add extraneous work to the care team
- Ensure sufficient return on investment to justify the health IT spend
- Disparately impact providers who care for communities that are underserved or marginalized

As part of the AEOB and GFE efforts, we urge the federal government and all relevant agencies to embrace this culture of real-world testing as one to make the health system more efficient and effective for everyone. In that spirit, AHIMA also believes that the testing of standards must include real-world implementations, production pilots, and collection of metrics regarding the effort needed to implement, the training needs for staff, the extent to which the standard achieved the stated goal and estimates of the costs and benefits of implementation. This includes, for example:

- Scoping
- Conceptual development
- Use cases
- Standards testing
- Pilot testing
- Return on investment
- Assessment of impact on different provider types and with different resources
- On-going monitoring.

Additionally, just as we have seen the inclusion of user-centered design in the development of health IT applications, so should we in the development of health standards and policies. Leveraging health IT end-user input throughout the standards and policy development process and conducting robust real-world testing can help mitigate those potential issues. It also can better align standards and policies to support the needs of front-line health workers and result in faster adoption and realization of the goals for the collection, sharing and use of health information to care for patients and support individuals on their health journeys.

Finally, and perhaps most importantly, significant privacy gaps remain in federal law related to the transfer of health data between HIPAA covered entities to non-HIPAA covered technologies. FHIR based APIs and other technology enabled APIs do not just facilitate the transfer of information from one covered entity to another. As mandated by the Office of the National Coordinator for Health Information Technology's (ONC's) 21st Century Cures Act Final Rule, electronic health record (EHR) developers are required to implement FHIR based APIs that enable access to third-party mobile applications in their products by the end of 2022. Under the information blocking provisions contained within the same final rule, providers are not allowed to stop patient directed data disclosure to those applications through an API, even if they are known bad actors who do not handle patient health data with the same standards required under HIPAA.

As OPM explores making more data transferrable by FHIR API, it is important for the agency to understand that implementing these standards may place more patient health data in areas that are unprotected by sharing restrictions like HIPAA. Currently, no agency within the federal government maintains responsibility for ensuring mobile applications appropriately protect patient health data. It is crucial for OPM to ensure any policy they implement does not place more patient data in harm's way without consequence on bad actors. Health data has never been more valuable and FHIR APIs – while secure – enable more information to be directed into unsafe and unprotected areas putting patient data privacy at risk.

What privacy concerns does the transfer of AEOB and GFE data raise, considering these transfers would list the individual's scheduled (or requested) item or service, including the expected billing and diagnostic codes for that item or service? Does the exchange of AEOB and GFE data create new or unique privacy concerns for individuals enrolled in a plan or coverage? Are there any special considerations that Departments should take into account regarding individuals who are enrolled in a plan or coverage along with other members of their household? How should the Departments and OPM address these concerns?

As stated above, whenever a patient's sensitive health data is exchanged and moves through the virtual space there are inherent privacy risks. This is especially true if the data moves from inside of a HIPAA protected space into one that is not governed by the HIPAA rules or where it is unclear if HIPAA requirements govern the data exchange or use. Prior to implementing requirements to exchange AEOBs and GFEs OPM and the related agencies must determine fully what the minimum data set to support that exchange is and then determine what sensitive patient information is included within that minimum set of data.

OPM and its partner agencies should also examine and understand the implications of enabling data transfer through the FHIR API and the potential unintended consequences of comingling of administrative and clinical data. For instance, an AEOB or GFE regarding sensitive patient healthcare issues such as treatment for substance use disorder, mental health care, and reproductive care may not be something a patient wants known or shared with other members of their medical care team. Additionally, some sensitive treatment options are not covered by insurance and a patient could be concerned that informing their insurance company of these treatment needs could impact the cost of their care. Similarly, those who previously underwent treatment for substance use disorder – but are no longer in treatment or at risk for relapse – may receive substandard or altered care if a physician were to learn they previously suffered from substance use disorder. OPM should work with other federal agencies, standards developers, and technology end-users – including patients – to determine the best path forward to protect privacy while also enabling the sharing of this data.

The concerns related to sharing sensitive medical information to unauthorized or unintended recipients is also magnified as it relates to when patients are on shared family medical care. OPM and its partner federal agencies must consult both state law and patient privacy experts to determine the best path forward for how best to protect familial information on shared insurance plans. There are many scenarios OPM must account for in the case of unauthorized disclosure, but two examples include minors and victims of intimate partner violence. In several states, a minor's health data is shielded from the parents based on age and what a parent is able to know without a minor's consent. AEBOs and GFEs have the potential to violate those requirements. A minor may not want a parent to know they sought to have treatment for conditions such as sexually transmitted infections (STIs) or mental and behavioral health conditions, but if the parent receives notice of the AEOB or GFE then they would know the minor may have sought or even received care. Similarly, an individual using medical care or their insurance as help for escaping an intimate partner violence situation would be placed in jeopardy if the person perpetrating the violence is informed their partner sought to have medical care related to the abuse. While these two scenarios are explicitly protected as it relates to access the health data specifically, it is less clear as it relates to administrative data such as GFEs and AEOBs. This gray area must be made clear prior to opening the data up for exchange across something such as a FHIR API.

On the surface AEOB and GFE data seems as if it may not put patient privacy at risk, but it contains some of the most sensitive pieces of information about a person's healthcare journey. OPM should work with all impacted agencies such as the HHS Office for Civil Rights, ONC, the US Centers for Medicare and

Medicaid Services (CMS), the Federal Trade Commission (FTC), and all other relevant agencies to fully understand the scope and impact of sharing this data under a relatively new and open FHIR API standards. OPM should also ensure all appropriate stakeholder groups are consulted and can provide input prior to mandating the use or exchange of any of this data over a FHIR API.

The ONC Health IT Certification Program consists of specified standards, implementation specifications, and certification criteria that health IT modules, including EHR systems, can meet. How could updates to this program support the ability of providers and facilities to exchange GFE information with plans, issuers, and carriers or support alignment between the exchange of GFE information and the other processes providers and facilities may engage in involving the exchange of clinical and administrative data, such as electronic prior authorization? Would the availability of certification criteria under the ONC Health IT Certification Program for use by plans, issuers, and carriers, or health IT developers serving plans, issuers, and carriers, help to enable interoperability of API technology adopted by these entities?

AHIMA encourages OPM to work with both CMS and ONC to further understand the implications of ePrior Authorization (ePA) technical requirements that need to be accounted for to facilitate both ePA and how those needs would also need to be accounted for when exchanged AEOBs and GFEs. In 2022, ONC published an RFI related to ePA that AHIMA responded to reflecting the technical and business and operational process considerations that should be accounted for when mandating ePA[2]. CMS currently has a rule pending at the Office of Management and Budget (OMB) that explicitly deals with ePA and requirements related to implementation. Further conversation and coordination with ONC and CMS by OPM to understand these ongoing efforts would help inform OPMs work related to AEOBs and GFEs.

The ONC Health IT Certification Program could be a main method for implementing any data standards related to the exchange and use of AEOB and GFE data but would be limited to impacting data exchange from a provider focus only. For the ONC Health IT Certification Program to have broad impact on this initiative, work would need to be done on the policy level as payer systems and revenue cycle work cycles are not certified health IT and are thus outside of the purview of this program. The interoperable exchange of data would be significantly hindered due to the fact that it would be unclear if certified health IT will be able to support the entire workflow, or if there would be limitations in the data flows due to the need to utilize both certified and non-certified health IT systems.

Additionally, AHIMA encourages OPM to utilize the United States Core Data for Interoperability Plus (USCDI+) program to propose new data standards to be developed and included in the baseline set of required data to be exchanged. The USCDI and the Interoperability Standards Advisory (ISA) processes inform the Health IT Certification Program and ensures that standards that are required for implementation move through a public comment and feedback process. Currently, the Health IT Certification Program already mandates the implementation of FHIR APIs for use by patients and third-party apps but does not have requirements for payers to implement or use these APIs. We encourage OPM to work with CMS, as those implementation requirements are widely expected to be included in forth coming rulemaking from the agency.

What, if any, burdens or barriers would be encountered by small, rural, or other providers, facilities, plans, issuers, and carriers in complying with industry-wide standards-based API technology requirements for the exchange of AEOB and GFE data? How many small, rural, or other providers, facilities, plans, issuers, and carriers would encounter these burdens or barriers in complying with such

[2] https://ahima.org/media/lzgbwjad/ahima-electronic-prior-authorization-rfi.pdf

technology requirements? Are there any approaches that the Departments and OPM should consider, or flexibility that should be provided (such as an exception or a phased-in approach to requiring providers and payers to adopt a standards-based API to exchange AEOB and GFE data), to account for small, rural, or other providers, facilities, plans, issuers, and carriers? If the Departments and OPM were to provide such flexibility, what factors should they consider in defining eligible providers, facilities, plans, issuers, and carriers?

All new technology requirements and mandates from the federal government pose a burden on those impacted by new requirements. The ability for a provider, facility, plan, issuer, or carrier organizations – also known as impacted parties – to implement those requirements varies widely based on a number of factors. Those factors determine the level of burden placed upon those impacted parties. Updating health IT standards, no matter the size of the organization, poses challenges including the need to have an EHR offline for deployment and recognizing risk factors such as new technologies not accurately reflecting the care environment. We urge OPM to ensure that all of these different types of impacted parties are consulted prior to implementing any new health IT API or FHIR API requirements for access to AEOBs and GFEs. The ability to interpret, understand, and implement new regulatory requirements is largely dependent on the size of the technical staff available to an impacted party. For instance, small, under resourced provider organizations will rely more on outside sources and health IT vendors to understand new regulatory requirements, costing them additional resources. Larger, better resourced organizations may most likely already have the expertise within their current employee knowledge base and would not need to bear additional cost burdens.

AHIMA recommends OPM and the relevant federal agencies undertake a series of listening sessions and/or surveys of front-line workers to fully understand the scope that these technical requirements would have on the impacted parties. It is not possible at this time to state a specific number related to how many impacted parties would be negatively impacted by implementing FHIR APIs for AEOBs and GFEs. Surveying the impacted populations would help OPM and other relevant agencies understand the widespread burden placed on the health system by implementing new technical standards nationwide.

Once the impacted population is determined, AHIMA recommends OPM pursue flexibilities for impacted parties in either hardship exemptions or delays in enforcement/implementation penalties to ensure impacted parties can realistically comply with requirements. Without providing these flexibilities, impacted parties could be negatively impacted due to circumstances outside of their control. We urge OPM to consult with CMS and to learn more about how their Promoting Interoperability Program's hardship exemption process functions and then propose those flexibilities and hardship programs to the public for comment.

B. Other Policy Considerations

What unique barriers and challenges do underserved and marginalized communities face in understanding and accessing health care that the Departments and OPM should account for in implementing the AEOB and GFE requirements for covered individuals? What steps should Departments and OPM consider to help ensure that all covered individuals, particularly those from underserved and marginalized communities, are aware of the opportunity to request AEOBs and GFEs and are able to utilize the information they received in order to facilitate meaningful decision-making regarding their health care?

A key gap in addressing care inequities also stems from a lack of patient focused education resources related to the care available to patients and how they can access that care. We encourage OPM to work with patient focused organizations to determine the best path forward to implementing new technology opportunities for patients, such as electronic access to AEOBs and GFEs. At this time there are numerous requirements being placed on patients related to access to their electronic data and ensuring additional requirements appropriately reflect patient needs is crucial.

Additionally, AHIMA continues to encourage the federal government to engage patient groups to help improve health literacy nationwide. A lack of literacy is particularly problematic as it relates to understanding AEOBs and GFEs given the complexity of both health plan coverage and healthcare services. Consumers need education on how to know what their health plan covers, how healthcare bills are structured, and how to gather information to understand their personal financial responsibility. Giving patients earlier access to this information, while good, poses a very real threat of increasing confusion about how to manage their care without additional educational needs accounted for in advance.

Finally, as we increase the use of technology to inform consumers, some patients may have health conditions or personal preferences that require other forms of communication, including paper documents or phone calls. These needs should be accounted for as the above-mentioned relevant agencies work to give greater access to some of this information earlier. Tackling those challenges also will involve understanding and solving for a patient’s need to access broadband in both rural and urban areas.

C. Economic Impacts

The Departments and OPM are also interested in how establishing standards-based APIs for these purposes may align with other HHS program requirements to implement standards-based APIs, such as requirements for certain payers covered under the CMS Interoperability and Patient Access final rule to use specific standards to implement the Patient and Provider Access APIs, as well as requirements applicable to health IT developers with health IT modules certified to certain criteria under the ONC Health IT Certification Program that provide standards-based API technology to providers and facilities as part of certified health IT products.

There are numerous other requirements placed upon payers, providers, and technology developers across different agencies both within and outside of HHS related to APIs and FHIR APIs. While the technology basis and standards language of these APIs may be similar, additional different FHIR API requirements serving a new set of purposes will require new development. Not all FHIR API requirements have the same basis for security, privacy, and exchange and ensuring that AEOB and GFE data exchange is safe, secure, and functional requires significant additional work at the developer and real-world testing and implementation activities from both payers and providers. We encourage OPM and other relevant agencies to consult closely with all impacted members of the healthcare community impacted by these potential requirements to gain a greater perspective on what an AEOB and GFE FHIR API would mean in terms of level of effort across the healthcare community. While unable to put a specific dollar value or impact number on these new potential requirements, AHIMA believes if OPM were to proceed with implementing these FHIR API requirements that significant time and cost burden would be assumed by all members of the impacted healthcare community.

What would be the cost purchasing and implementing a standards-based API for the real-time exchange of AEOB and GFE data from a third-party vendor, compared to building standards-based API functionality in-house?

Without fully understanding the standard and regulatory requirements for a AEOB and GFE standards-based API it is not possible to fully understand the cost of implementing such an API. Trends overtime have shown that it is more expensive for organizations to use a third-party to accomplish technology goals than it is to do it in-house both in the short and long-term. It is important to note that based on multiple requirements placed on technology developers and providers related to certification, cybersecurity, and privacy, that utilizing a third-party to create and implement an API may be impossible leaving many impacted organizations with only their health IT vendor as an option to create and implement new FHIR based API requirements. AHIMA recommends OPM and other relevant agencies complete a robust cost analysis to fully understand the impact of new regulatory requirements prior to proposing new requirements.

AHIMA and its membership remain committed to developing and implementing standards based FHIR APIs and exchanging new data to help patients better engage with and understand their care. At this time, we recommend federal agencies fully survey impacted parities prior to implementing new requirements to ensure alignment with other federal and state requirements and ensure that prior to the adoption of standards into federal policy, the testing of the standards include real-world implementations, production pilots, and collection of metrics regarding the effort needed to implement, the training needs for staff, the extent to which the standards achieved the stated goal, and estimates of the costs and benefits of implementation. Fully engaging with the health IT community ahead of proposing new regulations also ensures the healthcare community is prepared when new requirements are proposed. If AHIMA can provide any further information, or if there are any questions regarding this letter and its recommendations, please contact Andrew Tomlinson, Director of Regulatory Affairs, at (312) 223-1086 or andrew.tomlinson@ahima.org.

Sincerely,

Wylecia Wiggs Harris

Wylecia Wiggs Harris, PhD, CAE
Chief Executive Officer