The CARIN Alliance

Creating Access to Real-time Information Now through Consumer-Directed Exchange

Administrator Seema Verma
Centers for Medicare & Medicaid Services
Department of Health and Human Services
Attention: CMS-9115-P
P.O. Box 8013
Baltimore, MD 21244-8013

RE: Medicare and Medicaid Programs: Patient Protection and Affordable Care Act; Interoperability and Patient Access for Medicare Advantage Organization 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

Dear Administrator Verma,

On behalf of the CARIN Alliance, we thank you for the opportunity to comment on the proposed rule for promoting patient access and interoperability. We appreciate your consideration of our comments.

The CARIN Alliance is a multi-sector group of stakeholders representing numerous hospitals, thousands of physicians, millions of consumers, individuals, and caregivers. We are committed to enabling consumers and their authorized caregivers to easily get, use, and share their digital health information when, where, and how they want to achieve their goals. Specifically, we are promoting the ability for consumers and their authorized caregivers to gain digital access to their health information via open APIs.

We want to thank CMS for the number of advancements that you have made and the focus that you have brought to empowering consumers with access to their digital health information. Through MyHealthEData, Blue Button 2.0, the Promoting Interoperability Program, and other initiatives, CMS has significantly advanced industry efforts to empower consumers and their authorized caregivers. As discussed below, we believe this rule, and the ONC rule on information blocking, will significantly benefit consumer's access to their own health information, advance value-based purchasing in health care, and increase an individual's understanding of quality in the health care system.

Overall, we are very supportive of this proposed rule. We believe the comments we are making, if implemented, will help to streamline the business, policy, and technical hurdles that remain for consumers and their caregivers to access their own digital health information.

Again, we appreciate your work here and your consideration of our comments. If you have any questions or additional follow-up, please contact me at ryan.howells@leavittpartners.com.

R Ryan Howells

Ryan Howells
Leavitt Partners
On behalf of the CARIN Alliance

CMS language:
We believe patients should have the ability to move from health plan to health plan, provider to provider, and have both their clinical and administrative information travel with them throughout their journey. When a patient receives care from a new provider, a complete record of their health information should be readily available to that care provider, regardless of where or by who care was previously provided. When a patient is discharged from a hospital to a post-acute care (PAC) setting there should be no question as to how, when, or where their data will be exchanged. Likewise, when an enrollee changes health plans or ages into Medicare, the enrollee should be able to have their claims history and encounter data follow so that information is not lost.

All payers, including health plans, should have the ability to exchange data seamlessly with other payers for timely benefits coordination or transitions, and with providers to facilitate more coordinated and efficient care. Health plans are in a unique position to provide enrollees a complete picture of their claims and encounter data, allowing patients to piece together their own information that might otherwise be lost in disparate systems. This information can contribute to better informed decision making, helping to inform the patient's choice of coverage options and care providers to more effectively manage their own health, care, and costs.

CARIN Response:
The CARIN Alliance wholeheartedly agrees with CMS that patients should always have as complete an electronic record of their health information as possible and that claims and encounter information available from health plans is an essential part of this view. We also believe as individuals move from one health plan to another, they should also be able to receive, manage, and use their digital information from one health plan to improve their own health and to have a complete longitudinal clinical and claims history of their own experience with the health care ecosystem. There are hundreds, if not thousands, of situations where consumers and their caregivers can use this information to improve their own health care, lower their out of pocket costs, look for the best provider or health plan that meets their needs, and many, many more.

CMS language:
We understand the significant health information privacy and security concerns raised around the development of a UPI standard and the current prohibition against using HHS funds to adopt a UPI standard. Recognizing Congress' statement regarding patient matching and stakeholder comments stating that a patient matching solution would accomplish the goals of a UPI, we seek comment for future consideration on ways for ONC and CMS to continue to facilitate private sector efforts on a workable and scalable patient matching strategy so that the lack of a specific UPI does not impede the free flow of information. We also seek comment on how we may leverage our program authority to provide support to those working to improve patient matching. In addition, we intend to use comments for the development of policy and future rulemaking.

CARIN Response:
The CARIN Alliance agrees with and support CMS and their focus on developing a national strategy around identifying and matching patients and individuals across systems. Furthermore, we appreciate ONC's work on standards in this space and encourage CMS, as you have done in other areas of the proposed rule, to support that work. Patient matching is essential for many use cases, including the use of open APIs. We believe the promise of APIs will only work at a national scale across provider, plans, and applications if we can effectively match individuals across systems. As such, the CARIN Alliance created a workgroup that

has focused exclusively on this issue for the last couple of years. You can learn more about our work by going to our website (https://www.carinalliance.com/our-work/consumer-id-authentication/).

During that time, here is a summary of what we have learned regarding patient matching for APIs, some of which is more broadly applicable to healthcare and will be increasingly important as API-based data access grows rapidly in importance.:

- The issue of patient matching (defined as matching an individual with their health records) begins with the accurate collection of appropriate personal demographic identifying information when the member or patient first enters into the system.
- Because there of the lack of standards (due to system customization, diverse capture of demographic information, etc.) and human error, there is lower quality demographic information than is ideal for patient identification, patient authentication, and patient matching.
- Health care is relatively unaware of the latest advancements in digital identity (i.e., NIST 800-63-3, etc.) and therefore have not sufficiently upgraded their systems accordingly.
- Historically, health care has taken an 'institution-first' approach. The organization enters the individual's information in the system, *then* finds out exactly who they are. In CARIN, we are taking a 'individual-first' approach. We are advocating a focus on accurately identifying the individual *before* you enter their information in the system.

As we indicated in our August 2017 letter to the ONC in response to the initial version of the Trusted Exchange Framework (TEF), we believe health care organizations should be required to adopt at a minimum the NIST 800-63-3 guidelines related to Identity Assurance Level 2 (IAL2) and Authenticator Assurance Level 2 (AAL2) similar to what the ONC has recommended in the initial and subsequent version of the TEF.

Currently, individuals do not have a seamless method to request access to PHI across different EMRs without logging in to each portal separately. We are supportive of the SMART on FHIR workflow that allows the user to enter a pre-registered portal user name and password to access their health information using a third-party application. When an individual has their data spread across multiple portals (including some that may not be known to the individual) there is no easy way to aggregate all of their data without remembering every provider the individual has ever seen, registering with all of those portals, and then remembering every single username and password so they can be used in the application. That is not a good user experience.

As discussed above, the CARIN Alliance suggests unifying identity proofing and authentication through utilization of shared login services that conform to NIST 800-63-3 standards. For example, the Department of Veterans Affairs has implemented a unified authentication approach aligned to NIST 800-63-3 standards at www.Vets.gov. Implementing this type of an approach across the entire commercial provider community will enable veterans to access Community Choice Care Act providers with the same ID proofing credential they used for Vets.gov. This can be done remotely following the NIST standards or in person. Similarly, if a veteran were to initially create a certified IAL2 credential with a Community Choice Care Act provider, that credential could also be accepted by www.Vets.gov.

A NIST certified shared login service need not replace a provider or EMR's direct authentication flows or the use of SMART on FHIR but should act as a universally recognized login option in addition to the proprietary login flows through the portals provided by data holders today. NIST IAL2 and AAL2 credentials would be recognized as a common, trusted login for cross-entity authentication to PHI. Individuals may request access from multiple EMRs and providers with the same authority through a single-credentialing and authentication event without having to login to each provider or EMR individually.

NIST 800-63-3 provides the foundation for interoperability between organizations at a given level of risk the same way Visa's standards provide trust between card issuing banks and merchants. Authentication interoperability for shared login services should use open standards such as OAuth 2.0, OpenID Connect, and SAML 2.0 to transmit identity attributes.

All certified identity providers would be published on a publicly-available government website (https://www.idmanagement.gov/trust-services/#consumer-identity-credentials) to provide transparency with everyone in the health care ecosystem. Based on initial conversations with major health delivery systems and health IT companies, the CARIN Alliance believes if ONC creates or helps facilitate the creation of an environment where key stakeholders (e.g.., hospitals, EHR vendors, Health IT companies, etc.) can become a certified credentialing authority at an IAL2 level and ensures data holders can accept that IAL2 certified credential from anyone who is a certified ID provider, the market will develop a proliferation of entities who develop unique business models to compete for the opportunity to credential an individual.

Here are the various ways in which a consumer / patient could authenticate themselves in order to access their data today.

Use Case	**Technical workflow solutions available today to support API access**
Patients who already have a 'tethered portal' account	SMART on FHIR
Patients who do not have a 'tethered portal' account	Data holders need to ask their patients/members to register through their portal and create a UN/PW so the application can use SMART on FHIR to access the consumer's data
Personal representatives who already have a 'tethered portal account' for the patient they represent	SMART on FHIR
Personal representatives who do not have a 'tethered portal account' for the patient they represent	Data holders need to ask the personal representatives to register through their portal and create a UN/PW so the application can use SMART on FHIR to access the consumer's data
Providers or health plans who do not currently have a portal and only offer API access	No option available today; the CARIN Alliance membership has seen many examples of data holders who do not have a portal

Therefore, the ability to use open standards to **clearly identify the consumer and authorized caregiver** making the request to ensure each party involved is able to verify the person is who they say they are upfront, *with or without a portal,* will be critical to matching individuals to their information across systems.

According to the Individuals Right Under HIPAA to Access their Health Information, the OCR says:

The Privacy Rule requires a covered entity to take reasonable steps to verify the identity of an individual making a request for access. See 45 CFR 164.514(h). The Rule does not mandate any particular form of *verification (such as obtaining a copy of a driver's license), but rather generally leaves the type and manner of the verification to the discretion and professional judgment of the covered entity, provided the verification processes and measures do not create barriers to or unreasonably delay the individual from obtaining access to her PHI, as described below. Verification may be done orally or in writing and, in many cases, the type of verification may depend on how the individual is requesting and/or receiving access – whether in person, by phone (if permitted by the covered entity), by faxing or e-mailing the request on the covered entity's supplied form, by secure web portal, or by other means.*

Therefore, the CARIN Alliance supports open standards for providers, EMR systems, health plans, and applications to follow when ID proofing someone across systems who may be coming through a third-party application. While we believe in the short-term, users may continue to be ID proofed via portals, we believe in the long-term there will and should be ways to perform ID proofing that are consistent with NIST and other relevant standards. We anticipate development in other industries, and in healthcare, of federated, decentralized identity-proofing and authentication services, which can streamline the process for requesting electronic health information across the ecosystem.

RECOMMENDATION: The CARIN Alliance recommends CMS support the NIST Special Publication 800-63A, "Digital Identity Guidelines: Enrollment and Identity Proofing Requirements" and implement Identity Assurance Level 2 (IAL2) for a consumer who is using a third-party application to request electronic access to their health information and allows for both remote and in-person ID proofing.

RECOMMENDATION: The CARIN Alliance recommends CMS support the NIST Special Publication 800-63B, "Digital Identity Guidelines: Authentication and Lifecycle Management" and implement Authenticator Assurance Level 2 (AAL2) for a consumer who is using a third-party application to request electronic access to their health information.

In addtion to the recommendations above, CMS should work with ONC to require the use of standards for certain demographic data elements—an approach long recommended by many other organizations, including Audacious Inquiry in a report contracted by ONC.

In Pew-funded research published recently in the *Journal of the American Medical Informatics Association*, experts at Indiana University studied whether the standardization of different data elements improves patient matching rates. Researchers attempted to match records in four databases, standardized the data in those databases, and then retried matching the records to determine whether that standardization yielded better results. The researchers culled tens of thousands of records from the Indiana Health Information Exchange; a county public health registry; Social Security's Death Master file; and a newborn screening laboratory. Each of these databases had already been reviewed to ensure that the record matches were accurate, which allowed researchers to understand the number of correct and inaccurate matches both before and after the standardization of select demographic data.

The research revealed that the standardization of address to the standard employed by USPS, which details the preferred abbreviations for street suffixes and states, for example, would improve match rates by approximately 3 percent. One technology developer indicated that this would help their system match an additional tens of thousands of records per day. Separately, standardizing last name to the standard used by the Council for Affordable Quality Healthcare—while showing limited utility on its own—would further improve match rates up to 8 percent if standardized along with address.

As part of ONC's proposed rule, the agency incorporates phone number and address in the U.S. Code Data for Interoperability (USCDI), a collection of critical health information that should be exchanged and made available by EHRs via APIs. ONC could further improve match rates by requiring use of the USPS standard for address within the USCDI. To further promote use of this standard, ONC and CMS should also coordinate with USPS to ensure that health care organizations can use the postal service's online, API-based tool—or another easily accessible mechanism—to convert addresses to the USPS standard. There may also be scenarios—such as for military personnel stationed abroad—where the use of the USPS standard is not feasible. ONC could restrict use of the USPS standard to domestic, non-military addresses if challenges arise in the broader use of the standard.

Adopt additional data elements for patient matching

Second, CMS should encourage ONC to require use of other regularly collected demographic data elements for patient matching. ONC currently requires EHRs to make some demographic data—such as name, birth date, and sex—available, and proposes to add address and phone number to the USCDI. However, health records contain other demographic data routinely collected that aren't typically used or made available to match records.

For example, research published in 2017 showed that email addresses are already being captured in more than half of patient records. The documentation of email is likely higher today given the adoption of patient-facing tools, like portals, that often require emails to register.

CMS should encourage ONC to improve match rates by identifying and including in the USCDI readily available data elements—such as email address, mother's maiden name, or insurance policy identification number—that health information technologies should use for matching.

Specific comments on CMS' patient matching RFI

CMS seeks input on a variety of steps the agency can take to address patient matching.

First, CMS requests information on whether the agency should advance more standardized data elements across all appropriate programs for matching purposes, perhaps leveraging the USCDI proposed by ONC. As mentioned above, CMS should work with ONC and then adopt enhanced standards for demographic data. Specifically, CMS should encourage ONC to use the USPS standard for address and facilitate the addition of other regularly collected demographic data, such as email address, to the USCDI.

Second, CMS solicits input on whether to require use of a patient matching algorithm or solution with a "proven" success validated by the Department of Health and Human Services or a third-party. While not requiring the use of a specific technology, benchmarking different approaches would help shed a spotlight on matching deficiencies and the wide variation in quality across different algorithms. Technology developers could then use that information to improve their algorithms, and health care providers could adopt the most promising approaches. CMS should work with ONC to determine how to benchmark different matching approaches; this likely requires the identification of a large, real-world data set to test different algorithms. The use of real-world data, rather than synthetic data, is essential given that some innovative approaches—such as referential matching—use third-party databases to support their algorithms. CMS or ONC may be able to use grantmaking authorities or other policies to obtain such a data set for benchmarking. This benchmarking could assess duplicate creation rates, the number of records correctly matched, and the frequency with which records are incorrectly merged.

Third, CMS requests input on whether to expand recent efforts to issue new Medicare identification numbers to support patient matching. Implementing an agency-wide identifier may help CMS better serve beneficiaries and improve matching. However, this approach is still insufficient to address matching on a nationwide scale. A unique identifier would still face limitations in matching patients to information prior to enrollment in federal health insurance programs, and they may still be susceptible to errors (e.g. typos that exist today with the use of Social Security numbers). For example, the Pew Foundation conducted focus groups with patients on patient matching that highlighted frustration with having to remember a number or card that could be lost or stolen, just like Social Security numbers. Given those limitations, even if CMS pursues broader use of a CMS-wide identifier, the agency should still push forward with optimizing the use of other demographic data, including adoption of the USPS standard for address and the use of additional data elements.

Fourth, CMS seeks information on the number and type of third-party data sources to use for identity proofing and verification, as well as limitations. Referential matching—wherein these third-party data sources are used to support matches—has shown promise for improving patient matching. However, use of third-party data also has limitations. These data sources may contain inaccuracies, and lack information for some populations. For example, these data sources do not contain information on children, and therefore have limitations in providing an added benefit for matching pediatric records.

Finally, CMS requests information regarding how patient-generated data can complement patient matching efforts. Pew collaborated with the RAND Corporation to examine patient involvement in record matching. The research revealed two key ways for patients to support record matching. For one, patients could validate their demographic information by verifying their mobile phone number and other data. The CARIN Alliance believes the consumer can play a key role in verifying their demographic information through the use of mobile technologies. In addition, EHRs and health plans could support smartphone applications that use standard APIs to allow patients to update their demographic data. CMS could coordinate with ONC, the technology industry, and the CARIN Alliance to pilot these patient-led approaches. In addition, Pew and the CARIN Alliance discovered a promising approach to patient matching that has not yet been widely used in health care: biometrics, such as fingerprint or facial recognition scans. In Pew-led focus groups on patient matching, patients overwhelmingly preferred the use of biometric over other options. Patients in the focus groups indicated that they already use biometrics in other aspects of their lives—such as to unlock smartphones or board airplanes—and should be able to use the same approach for record matching.

The CARIN Alliance is supportive of the work the FIDO Alliance is doing in developing a universal two-factor authentication (U2F) open standard that uses the combination of your fingerprint biometric and a cryptographic key embedded in the hardware of your mobile phone to securely authenticate you online with any application. Within the next few years, the FIDO standard (FIDO2) will be ubiquitous across all major browsers and operating systems making it readily available to any health care organization in the country.

CMS language:

Section 1899B(b)(1)(A) of the Act requires that such data must be submitted through the applicable reporting provision that applies to each PAC provider type using the PAC assessment instrument that applies to the PAC provider. Section 1899B(a)(1)(B) of the Act additionally requires that these data be standardized and interoperable so as to allow for their exchange among health care providers, including PAC providers, to ensure coordinated care and improved Medicare beneficiary outcomes as these patients transition throughout the care continuum. To enable the interoperable exchange of such information, we have adopted certain patient assessment data elements as standardized patient or resident assessment data and mapped them to appropriate health IT standards which can support the exchange of this information. For more information, we refer the reader to the CMS website at https://del.cms.gov/DELWeb/pubHome.

CARIN response:
The CARIN Alliance is supportive of CMS and their effort to make available the information that is found in the Data Element Library (DEL). The CARIN Alliance created a post-acute care workgroup in early 2019 focused on developing a FHIR patient profile that would enable consumers to access the information found in the DEL. In partnership with CMS and MITRE, we kicked off a workgroup with industry to develop a FHIR implementation guide that would exchange the standardized patient assessment information found in the DEL with patients. We continue to work with industry, CMS, and MITRE to complete an implementation guide later this year for the benefit of all consumers and their authorized caregivers.

CMS language:

An "open API," for purposes of this proposed rule, is simply one for which the technical and other information required for a third-party application to connect to it is openly published. Open API does not imply any and all applications or application developers would have unfettered access to people's personal or sensitive information. Rather, an open API's published technical and other information specifically includes what an application developer would need to know to connect to and obtain data available through the API.

CARIN response:

We support this definition of 'open API' and the work done by ONC to similarly define an 'open API'. We encourage CMS to align its definition on this critical piece to that of ONC. (We note that "open" alone is not sufficient—we underscore ONC's definition of "standards-based APIs" must be included in a broad statement on "open APIs" requirements[1]). We would also recommend including in the definition of an 'open API' the language found elsewhere in the rule which includes the concepts of the technology and the data being standardized and the APIs being transparent and pro-competitive. The phrase 'openly published' isn't well known in the industry. We would recommend CMS change that phrase to instead say, 'published on one or more websites available to the public and able to be access and used.'

CMS language:

However, we note that a number of stakeholders may believe that they are responsible for determining whether an application to which an individual directs their PHI be disclosed applies appropriate safeguards for the information it receives. Based on the OCR guidance discussed below, covered entities are not responsible under the HIPAA Rules for the security of PHI once it has been received by a third-party application chosen by an individual.

CARIN response:

The CARIN Alliance strongly agrees with CMS that a covered entity is not responsible under the HIPAA rules for the security of PHI once it has been received by a third-party application. We have been clear in

[1] ONC defines open APIs as "standardized, transparent, and pro-competitive". See 84 Fed. Reg. 42, page 7477.

our code of conduct (https://www.carinalliance.com/wp-content/uploads/2019/05/2019_CARIN_Code_of_Conduct_05082019.pdf) and in past comment letters to CMS that an individual can request access to their health information in a form that is 'readily producible'. We appreciate the new OCR FAQs that were released in April of 2019 that reaffirms this concept.

CMS language:

When a non–HIPAA-covered entity discloses an individual's confidential information in a manner or for a purpose not consistent with the privacy notice and terms of use to which the individual agreed, the FTC has authority under the FTC Act to investigate and take action against unfair or deceptive trade practices. The FTC has applied this authority to a wide variety of entities. The FTC also enforces the FTC Health Breach Notification Rule, which applies to certain types of entities that fall outside of the scope of HIPAA, and therefore, are not subject to the HIPAA Breach Notification Rule.

CARIN response:

The CARIN Alliance supports this approach by CMS and believes it's important for the industry to support a set of best practices that will ensure the FTC can use those best practices to 'take action against unfair or deceptive trade practices'. Similar to other industries, when the industry has agreed on a consensus set of principles for exchanging information under FTC jurisdiction, the FTC has shown they are willing to enforce those set of principles to help eliminate bad actors.

The CARIN Alliance has developed a set of industry best practices called the 'CARIN Code of Conduct' to hold third-party applications who are not covered by HIPAA accountable for using, managing, and storing protected health information (PHI) on behalf of consumers. The current CARIN Code of Conduct can be found on our website www.carinalliance.com (https://www.carinalliance.com/wp-content/uploads/2019/05/2019_CARIN_Code_of_Conduct_05082019.pdf). The CARIN Alliance worked with more than 60 stakeholders for many months to release the initial version of the Code of Conduct in November of 2018. Numerous organizations offered quotes in support of the code of conduct as indicated in our initial press release (https://www.prnewswire.com/news-releases/voluntary-code-of-conduct-developed-by-more-than-60-industry-stakeholders-can-help-facilitate-health-data-exchange-with-entities-not-covered-by-hipaa-300755734.html).

We believe this is the only voluntary code of conduct that exists that outlines how entities not covered by HIPAA should handle PHI. **As such, we would strongly recommend that CMS, the VA, and all other covered entities and data holders adopt the CARIN Code of Conduct as being foundational to exchanging PHI with entities not covered by HIPAA.** In doing so, the FTC and the private sector can have a common set of industry best practices to rely on so they know who has voluntarily attested to the code of conduct and who has not. Without a common set of best practices, it will become difficult for the FTC to define 'unfair or deceptive trade practices' on behalf of the health care industry.

CMS proposed language:
§422.119 Access to and exchange of health data and plan information
(a) *Application Programming Interface to support MA enrollees.* A Medicare Advantage (MA) organization must implement and maintain an open Application Programming Interface (API) that permits third-party

applications to retrieve, with the approval and at the direction of an individual MA enrollee, data specified in paragraph (b) of this section through the use of common technologies and without special effort from the enrollee.

CARIN response:

We support this language as proposed by CMS. We would recommend CMS use the phrase 'common standards and technologies' to describe how the information will be transmitted between systems. In the preamble to this rule, CMS defines the term 'open API' as being "openly published" (or simply "open") - that is, APIs for which the technical and other information required for a third-party application to connect to them is publicly available. CMS also mirrors language from ONC, as discussed above, which requires APIs be standardized, technically transparent, and pro-competitive. Finally, CMS incorporates by reference the ONC API standards and specifications. We applaud this incorporation and, as discussed in our comments to ONC, support CMS and ONC alignment and coordination.

CARIN supports this language and would recommend that CMS include this additional clarity related to the definition of an 'open API' as part of the final regulatory language to ensure consistency in how the term is used and interpreted by those within the industry. We would also encourage CMS to include the fact the API would be 'non-proprietary' (i.e. when used for the purposes and in the manner outlined here, APIs are "open and standard").

CMS proposed language:

§422.119 Access to and exchange of health data and plan information

(b) Accessible content. (1) An MA organization must make the following information accessible to its enrollees through the API described in paragraph (a) of this section:

(i) Standardized data concerning adjudicated claims, including claims data for payment decisions that may be appealed, were appealed, or are in the process of appeal, and provider remittances and enrollee cost-sharing pertaining to such claims, no later than one (1) business day after a claim is processed;

(ii) Standardized encounter data, no later than one (1) business day after data concerning the encounter is received by the MA organization;

(iii) Provider directory data on the MA organization's network of contracted providers, including names, addresses, phone numbers, and specialties, updated no later than 30 business days after changes are made to the provider directory; and

(iv) Clinical data, including laboratory results, if the MA organization manages any such data, no later than one (1) business day after the data is received by the MA organization.

CARIN response:

Since 2018, the CARIN Alliance has worked with multiple regional and national health plans representing over 40% of the total covered commercial lives in the US to build a FHIR API implementation guide that maps existing health plan claims data to resources found in FHIR® Release 4. We have also been working with the CMS Blue Button team to ensure the same data element found in CMS Blue Button is also included in our API implementation guide. As a result of this work, earlier this year the CARIN Alliance was identified by Health Level 7 (HL7) as one of only 3 organizations designated as a FHIR Accelerator program. Our 'in process' work is always accessible by the public on our website, our meetings are open, and we have received approval from the HL7 Financial Management workgroup and the FHIR Management Group to ballot the CARIN Blue Button implementation guide in an STU format by January 2020.

We strongly recommend that CMS require in their final rule commercial health plans implement the CARIN Blue Button FHIR API implementation guide. This will enable all commercial health plans to implement the same standards-based API. The link for the CARIN Blue Button implementation guide can be found here: https://build.fhir.org/ig/HL7/carin-bb/index.html and is available for all health plans across the country to use for free. We will have an initial draft published in June 2019, a reference implementation in the Fall, and a connectathon at the Annual HL7 meeting in Atlanta in September.

We are working with the CMS Blue Button team who has informed us they will also be moving to the CARIN Blue Button implementation guide later this year. This will allow both the public and private sector to implement the same standards-based API using the same CARIN Blue Button implementation guide thus achieving CMS' vision for seamless interoperability between systems.

CMS proposed language:

(2) In addition to the information specified in paragraph (b)(1) of this section, an MA organization that offers an MA-PD plan must make the following information accessible to its enrollees through the API described in paragraph (a) of this section:
(i) Standardized data concerning adjudicated claims for covered Part D drugs, including remittances and enrollee cost-sharing, no later than 1 business day after a claim is adjudicated;
(ii) Pharmacy directory data, including the number, mix, and addresses of network pharmacies; and
(iii) Formulary data that includes covered Part D drugs, and any tiered formulary structure or utilization management procedure which pertains to those drugs.

CARIN response:

The CARIN Alliance fully supports making this data available to consumers. We encourage CMS to reference the work of the CARIN Alliance on each of these items:
For (2i) – The CARIN Alliance consumer payer data set (CPCDS) Blue Button 2.0 project is developing an implementation guide that will be made available this year for developers and health plans to be compliant with the proposed rule.
For (2ii) – The CARIN Alliance work to create a consumer-facing real-time pharmacy benefit check implementation guide will include pharmacy directory information.
For (2iii) – The CARIN Alliance work to create a consumer-facing real-time pharmacy benefit check implementation guide will include formulary data. We would suggest amending the language in the proposed rule to include: "*Formulary data that includes covered Part D drugs, and any tiered formulary structure or coverage restrictions which pertain to those drugs.*"

CMS proposed language:

(c) Technical requirements. An MA organization:
(1) Must implement, maintain, and use API technology conformant with the API technical standards adopted by the Secretary at 45 CFR 170.215;
(2) Must conduct routine testing and monitoring to ensure the API functions properly, including assessments to verify that the API is fully and successfully implementing privacy and security features such as, but not limited to, those minimally required to comply with HIPAA privacy and security requirements in 45 CFR part 164, 42 CFR parts 2 and 3, and other applicable law protecting the privacy and security of individually identifiable data;
(3) Must use the following content and vocabulary standards for data available through the API, where applicable to the data type or data element, unless alternate standards are required by other applicable law:
(i) Content and vocabulary standards adopted by the Secretary at 45 CFR 170.213 where such standards are the only available standards for the data type or element;

(ii) Content and vocabulary standards adopted by the Secretary at 45 CFR part 162 and 42 CFR 423.160 where required by law or where such standards are the only available standards for the data type or element; or
(iii) The content and vocabulary standards in either paragraph (c)(3) (i) or (ii) of this section 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 either paragraph (c)(3) (i) or (ii) of this section.
(4) May use an updated version of any standard or all standards required under paragraph (c)(1) or (3) of this section, where:
(i) Use of the updated version of the standard is required by other applicable law, or
(ii) Use of the updated version of the standard is not prohibited under other applicable law, provided that:
(A) For content and vocabulary standards other than those adopted at 45 CFR 170.213, the Secretary has not prohibited use of the updated version of a standard for purposes of this section or 45 CFR part 170;
(B) For standards adopted at 45 CFR 170.213 and 45 CFR 170.215, the National Coordinator has approved the updated version for use in the ONC Health IT Certification Program; and
(C) Where use of the updated version of a standard does not disrupt an end user's ability to access the data described in paragraph (b) of this section through the API described in paragraph (a) of this section.

CARIN response:
We strongly support ONC incorporating by reference standards and implementation specification included in the companion ONC proposed rule. With respect to that proposed rule and more generally, we vigorously support the use of standards and implementation specifications that are made publicly available through volunteer, private-sector based, industry-led consensus-based organizations such as the Argonaut project, DaVinci, and the CARIN Alliance. Once complete, these implementation guides can be adopted by standard development organizations (SDOs) such as HL7 and others. We believe the acceleration of standards development and use can be most effectively achieved through the use of these type of industry-led organizations who work hard to achieve consensus on a set of FHIR-based implementation guides so APIs can be implemented uniformly across systems. We believe this is the only way in which true innovation can occur where third-party start-up applications can develop a single interface to connect with multiple health plans in order to download member-specific information.

We have numerous developers of consumer-facing, third-party applications who are members of the CARIN alliance. While APIs are a new concept as it relates to health plans, it's been around in the provider sector for at least 3-4 years. Based on the ONC's research, the Argonaut project was able to achieve 82% market penetration within 3 years by having the industry come together to create an implementation guide and publish it for the public to use. We believe we will see similar adoption in the industry if CMS points to implementation guides being created by industry-led groups such as CARIN, Argonaut, and DaVinci.

CMS proposed language:
(d) Documentation requirements for APIs. For each API implemented in accordance with paragraph (a) of this section, an MA organization must make publicly accessible, by posting directly on its website or via publicly accessible hyperlink(s), complete accompanying documentation that contains, at a minimum:
(1) API syntax, function names, required and optional parameters supported and their data types, return variables and their types/structures, exceptions and exception handling methods and their returns;
(2) The software components and configurations an application must use in order to successfully interact with the API and process its response(s); and
(3) All applicable technical requirements and attributes necessary for an application to be registered with any authorization server(s) deployed in conjunction with the API.

CMS proposed language from the preamble:

"Under our proposal, the scope and volume of the information to be provided or made accessible through the open API would include: adjudicated claims (including cost); encounters with capitated providers; provider remittances; enrollee cost-sharing; and clinical data, including laboratory results (where available). We propose that these programs and organizations, with the exception of the QHP issuers in FFEs, would also be required to make information regarding provider directories and formularies available through the open API. Sections 1852(c), 1932(a)(5), and 2103(f)(3) of the Act require that MA organizations and Medicaid MCOs, and CHIP managed care entities provide basic information to their enrollees on how to get covered benefits in the plan and to facilitate decision making about plan choice, providers, and benefits."

CARIN response:

We believe CMS needs to stay aligned with the ONC in determining which standards to use for which type of data exchange. In the CARIN Alliance, we believe ONC (and hence CMS) should be using FHIR Release 4 as the baseline standard by which all health plans should exchange data with consumers. FHIR R4 is the first version to include normative content; such normative content is intended to be to be backwards compatible as it advances to future versions of FHIR.

CMS is proposing that plans expose USCDI v1 information including encounter and lab data (and other clinical data). This rule proposes to make financial data available to patients via a standard API. However, the USCDI does not include financial data types such as coverage or explanation of benefit. This is an example of an improvement that would need to be made to the USCDI for this reference approach to succeed.

The CARIN Alliance believes the USCDI (45 CFR 170.213) should be the 'source of truth' as it relates to the required data set for both the ONC and CMS rules but we also believe there is certain data that is actor-specific (i.e., providers may send different data than payers). As such, this variation in use case needs will require further guidance by CMS and the ONC regarding the USCDI data that should be made available within each data holder's system. CMS should recognize there are plans who may not have all of the clinical data that is available to providers and there are providers who may not have all of the claims data within their EHR.

We support making all data available to patients. However, "encounters from capitated providers" is somewhat ambiguous. HL7 FHIR has a specific view of an encounter, which is the metadata of a clinic visit or hospital admission (date, time, location, service type, etc. See more here: https://build.fhir.org/ig/HL7/US-Core-R4/StructureDefinition-us-core-encounter.html). The encounter does not automatically include the clinical data generated *within* that encounter. If the intent is to include all related data, those data elements (as represented within the USCDI v1, 45 CFR 170.213) should be enumerated individually to remove any ambiguity. The current text specifically highlights "laboratory results" but there are numerous other data types that could be included.

Since the announcement from CMS regarding Blue Button 2.0 in 2018, the CARIN Alliance has been working with numerous national and regional health plans to define what is meant by a Medicare Advantage and Commercial 'Blue Button 2.0' API for health plans. We have developed the CARIN Common Payer Consumer Data Set (CPCDS) which is posted on our website (https://www.carinalliance.com/our-work/health-plan/). We believe this is the data set that would satisfy the requirement CMS is requesting for releasing data to consumers. We are working with our members, the FHIR community, the CMS Blue Button 2.0 team, and HL7 to develop an implementation guide for the industry to freely use to standardize how the health plan data should be incorporated within an API that is available to consumers. The implementation guide uses FHIR R4 as its baseline to map the claims and explanation of benefit information to specific FHIR resources to ensure consistency across health plans.

The CARIN Alliance strongly believes it's important that all health plans use a similar implementation guide to develop their consumer-facing API to ensure consistency across plans. Without that consistency, the cost associated with connecting to multiple health plans who may use multiple standards will be prohibitive to the goals and objectives CMS has to empower consumers with access to their health information. We look forward to working with our members, CMS, and others to release an implementation guide later this year.

The proposed rule notes: "In requiring that this documentation is "publicly accessible," we expect that any person using commonly available technology to browse the Internet could access the information without any preconditions or additional steps beyond downloading and using a third-party application to access data through the API."

We support this approach and would suggest that CMS aligns the language here with the language in the ONC rule that "documentation should be accessible to the public via a hyperlink without additional access requirements, including, without limitation, any form of registration, account creation, "click-through" agreements, or requirement to provide contact details or other information prior to accessing the documentation." See 45 CFR 170.315(g)(10)(vii).

CMS language

(e) *Denial or discontinuation of access to the API.* An MA organization may deny or discontinue any third party application's connection to the API required under paragraph (a) of this section if the MA organization:

(1) Reasonably determines that allowing an application to connect or remain connected to the API would present an unacceptable level of risk to the security of protected health information on the MA organization's systems; and

(2) Makes this determination using objective, verifiable criteria that are applied fairly and consistently across all applications and developers through which enrollees seek to access their electronic health information, as defined at 45 CFR 171.102, including but not limited to criteria that may rely on automated monitoring and risk mitigation tools.

CARIN Response:

The proposed rule notes: "However, a covered entity is not expected to tolerate unacceptable levels of risk to the PHI held by the covered entity in its systems, as determined by its own risk analysis. Accordingly, it may be appropriate for an organization to deny or terminate specific applications' connection to its API under certain circumstances in which the application poses an unacceptable risk to the PHI on its systems or otherwise violates the terms of use of the API technology."

Because these circumstances could implicate information blocking as defined by Congress in statute and ONC in regulations, , we recommend referring to the information blocking definition and especially the exceptions in the ONC proposed rule (45 CFR 171.201) as the bases for establishing the criteria under which plans can deny or terminate API access for security reasons.

We would also reference the Office of Civil Rights FAQs which came out after this proposed rule that helps clarify individual right of access and APIs which can be found here (https://www.hhs.gov/hipaa/for-professionals/faq/health-information-technology---hit/index.html)

Specifically, the OCR included the following Q & A:

OCR's Question: "Can a covered entity refuse to disclose ePHI to an app chosen by an individual because of concerns about how the app will use or disclose the ePHI it receives?

OCR's answer: No. The HIPAA Privacy Rule generally prohibits a covered entity from refusing to disclose ePHI to a third-party app designated by the individual if the ePHI is readily producible in the form and format used by the app. See 45 CFR 164.524(a)(1), (c)(2)(ii), (c)(3)(ii). The HIPAA Rules do not impose any restrictions on how an individual or the individual's designee, such as an app, may use the health information that has been disclosed pursuant to the individual's right of access. For instance, a covered entity is not permitted to deny an individual's right of access to their ePHI where the individual directs the information to a third-party app because the app will share the individual's ePHI for research or because the app does not encrypt the individual's data when at rest. In addition, as discussed in Question 1 above, the HIPAA Rules do not apply to entities that do not meet the definition of a HIPAA covered entity or business associate.

The CARIN Alliance believes including a reference to these OCR questions and answers will be helpful for covered entities, including health plans, to reference when determining when and how data should be exchanged with entities not covered by HIPAA.

CMS language:
(g) *Enrollee resources regarding privacy and security.* An MA organization must provide on its website and through other appropriate mechanisms through which it ordinarily communicates with current and former enrollees seeking to access their health information held by the MA organization, educational resources in non-technical, simple and easy-to-understand language explaining at a minimum:
(1) General information on steps the individual may consider taking to help protect the privacy and security of their health information, including factors to consider in selecting an application, and understanding the security and privacy practices of any application to which they will entrust their health information; and
(2) An overview of which types of organizations or individuals are and are not likely to be HIPAA covered entities, the oversight responsibilities of OCR and FTC, and how to submit a complaint to:
(i) The HHS Office for Civil Rights; and
(ii) The Federal Trade Commission (FTC).
(h) *Applicability.* This section is applicable beginning on and after January 1, 2020.

CARIN Response:
The CARIN Alliance strongly supports CMS's intention to improve beneficiary education regarding how manage their health data in safe and secure ways. Helping people understand how their information may be collected, shared and used will be foundational to securing and bolstering consumer trust and confidence in the Administration's efforts to improve patient access and information sharing. Outreach and education efforts are a collective responsibility; all stakeholders have role to play, including governmental entities, health care providers, health plans, technology developers, and consumer advocacy organizations. We agree resources should be made available in non-technical consumer friendly language. We are eager to work with the Administration to explore how best to improve beneficiary awareness and education as the industry adopts standards-based APIs for patient access.

CMS is proposing that this provision of this rule goes into effect on 1/1/2020. While we believe it's important for health plans to develop and implement a consumer-facing API as soon as possible, we also believe CMS should establish a reasonable time frame for the industry to implement the rule once the rule is finalized later this year. We believe the timing for compliance with this rule should be linked to the effective date of the final rule. CMS should mirror what ONC has done and set a floor for the industry on the latest date the API should be available but allow the industry to move faster than the regulation. Health plans should be rewarded (i.e., Star Rating Program, etc.) for moving faster than the industry floor date for implementing the API standard.

For example, the Argonaut project was founded in January 2015 and it took approximately 18 months to publish the first version of the Argonaut Data Query Implementation Guide. EHR vendors then took approximately 6 months to 1 year to voluntarily update their systems to be in compliance with the implementation guide. In February 2017 at HIMSS, the CARIN Alliance was one of the first organizations to show how a third-party application could access patient-specific information using APIs that were built using the Argonaut implementation guide. By 2018, the ONC published a blog post which indicated 82% of hospitals and 64% of clinicians voluntarily used FHIR release v2 as a result of the work of the Argonaut Project. In January 2018, Apple Health Records announced support for the FHIR implementation guide developed by the Argonaut project which included the ability for millions of consumers to access their clinical data set. By January 2019 (a short 12 months later), our research indicates more than 197M Americans had the potential to access their health information through Apple's health records application using the Argonaut project's FHIR implementation guide. Finally in June 2018, Apple announced they would be making their API openly accessible to third-party developers. Many of our consumer-facing, third-party applications are using the Apple API for developers to gain access to health information for millions of consumers nationwide.

We believe this same approach is scalable to other sectors of the health care economy including health plans. Consensus-based, HL7 FHIR implementation guides can be developed by industry-led organizations and then can be made openly available to everyone so they can be rapidly implemented at scale by both public and private sector organizations.

Additional Suggestions to improve and promote interoperability

In addition to the suggestions above, the CARIN Alliance also believes the following suggestions would help to significantly improve interoperability across the country.

Government's Role: What actions can CMS/ONC/HHS take to encourage interoperability (e.g., definition of meaningful use, information blocking, etc.)? What timeframe is realistic based on these actions and how can we accelerate that timeframe?

- Adopt the CARIN Code of Conduct as the universally agreed upon set of principles all data holders will use for applications to self-attest to during the application registration process to enable the FTC and the private sector to enforce a common set of principles
- Develop a consistent regulatory approach across agencies (FTC, FDA, HHS, ONC, OCR) that promotes the ability for a consumer to access their health information:
    - Enforcement of the HIPAA right of individual access;
    - Implementation and guidance around the 2015 Edition Certified Health IT, especially the API module (ONC);
    - Develop a universal consent framework and approach across all federal agencies;

- Develop policies that create a “safe harbor” for covered entities who want to share data with consumers (i.e., OCR FAQs are a start. What more can be done?) to try and prevent both legal and reputational risk to the covered entity;
- Identify regulatory *incentives* to ensure the usability and interoperability of health IT APIs, i.e. encouraging, to the greatest extent possible, broad API conformity to technical specification such that third-party apps can be substituted and reused across and between health IT developer products without special effort;
- Ensure HIEs are subject to the same requirements as other covered entities and allow data sharing directly with consumers.

Technical standards and authentication*:* What is needed for full industry support, alignment, and adoption? What approaches/technologies can we use to verify identities (e.g., fingerprint scanning)? Will this vary by vendor or provider?

- Work with the Social Security Administration (SSA) to modify their SSA Privacy and Disclosure policy associated with the Federal Data Services Hub to allow third party commercial entities to access the API state exchanges use to identify that person exists; CMS should manage the data use agreement (DUA) (i.e., a digital version of the Consent Based Social Security Number Verification Service (CBSV) to identify (not authenticate) that a person with a given name exists);
- Help convene a public/private collaborative to co-create an open standard with the DMV for how they can, with your permission, digitally and remotely share your information with third parties (Real ID Act of 2005) (American Association of Motor Vehicle Administrators or AAMVA has a Driver’s License Data Verification Service (DLDV);
- Promote industry-led efforts like the Argonaut Project, the DaVinci Project, and the CARIN Alliance who are focused on developing industry standards for exchanging health information;
- Help fund HL7 and the FHIR foundation to ensure long-term sustainability of these private-sector, open source organizations;
- Technical standards and interoperability need to be defined in terms of a patient centric digital health information system connecting all the moving parts, not just EHRs;
- Promote and incentivize the use of the FIDO Alliance open authentication standard with EHR vendors and third-party applications;
- Request or incentivize EHRs, providers, and other health care organizations to publish their FHIR end points publicly in a centralized location;
- Encourage health IT vendors to securely expose more granular data via APIs---improving the usability and interoperability of EHR data for both patients and providers;
- When customers are requesting access to their electronic health information via the APIs, there should never be a charge to the application or the consumer;
- Help convene or fund a multi-sector, public/private collaborative to develop an open standard utility for record matching a patient’s existing health information outside the patient portal using data from installed FHIR resources;

Patient and physician engagement: How do we focus the solution to encourage participation (e.g., campaign around demand) and overcome obstacles, and address any issues such as HIPAA compliance?

- Promote current understanding among provider and patient/consumer communities of what information sharing is allowed under HIPAA; reinforce what is possible under current law;

- Measuring a patient's experience regarding access and use of the patient's digital health information to promote patient engagement;
- Increase demand from providers by supporting advance payment and delivery system models that excel with support of interoperable health information that engages the patient;
- Direct the Office of Civil Rights to develop additional educational campaigns that explain HIPAA privacy regulations user stories, vignettes, and other scenario-based examples;
- Encourage health IT vendors and health plans to proactively engage with their provider customers about the opportunities, considerations, and best practices when using new EHR functionality, i.e. APIs and Patient Generated Health Data (PGHD);
- Direct CMS to adjust MIPS program components and scoring, e.g. Improvement Activities and Advancing Care Information measures, such that providers are rewarded for utilizing a wider range of health IT not specifically tied to certified EHRs, i.e. telemedicine, remote patient monitoring, and provider/consumer facing apps.

Public/private partnership*:* How do we encourage private sector innovation? Can the government help to jump start with claims or other data? Who do we need to have on board; how do we best engage with the broadest possible group?

- Use the ONC's USCDI roadmap as a starting point to work collaboratively with industry regarding the development of open industry standards to create a 'single, longitudinal record' as required in 21st Century Cures that will include at a minimum: clinical physician notes (unstructured or semi-structured), claims (Blue Button API for Parts A, B, and D), radiology reports, diagnostic data, and more.
    - All of the data that is currently being provided in the patient portal should be provided to the consumer via an API;
    - All of the reporting data required by federal law should be required to be provided by APIs to the consumer.
- Use the savings from disbanding the mandatory bundled payment programs within CMMI to fund a health IT innovation fund to help solve interoperability and patient-centric, digital health models that promote the learning health care system.

Medicaid FFS, Medicaid Managed Care, and Social Determinants of Health: How do we engage the Medicaid sector to be more actively involved in data sharing with beneficiaries to improve patient outcomes?

- Eliminate the MITA 3.0 technology certification process for the enhanced federal match and move to a certified open API model using FHIR implementation guides developed by the private sector to reduce the burden on CMS, states, and vendors;
- Co-convene and help fund an industry-led effort to use existing industry led FHIR implementation guides like the CARIN Blue Button 2.0 API implementation guide and use it as a baseline for Medicaid to ensure consistency across the commercial, Medicare, and Medicaid lines of business;
- Develop an expedited state-based procurement process to ensure compliance with the CMS proposed rule deadline. (i.e., NASPO's multi-state procurement process may help);
- Require state Medicaid agencies to develop industry-leading, person-centric ways to establishing digital identities for beneficiaries that could be federated across systems (i.e., Healthcare.gov, Login.gov, etc.) and use that authentication 'widget' across all health care related portals;
- Co-convene and help fund industry-led initiatives to convene multiple states to standardize a standards-based SDOH API;

- Co-convene and help fund industry-led initiatives to help convene MCOs, hospitals, applications, and community-based organizations in a given region to access standards-based APIs to exchange social determinants of health (SDOH) information, especially at SAMSHA;
- Allow for the OMB A-87 cost allocation requirements and waiver to be renewed for work currently in flight and leverage a similar framework to enable states and the private sector to develop standardized eligibility and enrollment (E&E) open APIs;
- Align 42 CFR Part 2 with core HIPAA privacy and security requirements;
- Allow data sharing for case management after patient consent to entities not currently covered by HIPAA such as third-party applications;
- Eliminate the federal requirements that prevent the use of cloud services for certain data sets.