CARIN Alliance
Addressing Concerns with the Use of Standards-Based APIs in Health Care

The CARIN Alliance is a multi-sector group of stakeholders representing numerous hospitals, thousands of physicians and clinicians, and millions of patients and other consumers and caregivers. Specifically, we are promoting the ability for consumers and their authorized caregivers to gain digital access to their health information via the open Application Programming Interfaces (APIs).

Although a large and growing number of providers, technology, and patient groups continue to stress the benefits of current federal mandates and private sector initiatives for use of an API infrastructure to make available patient information, consistent with HIPAA protections and obligations, some health care stakeholders remain concerned about the speed and scope of this effort as being too fast and too much. We also understand that there are concerns and questions about the patient need for such access, security of the APIs, the costs of implementing new technology, accurate identification of patients and trusted applications, and the status of standards for using APIs. This document addresses these concerns.

- **Patient education and patient need**: Patients are highly interested in accessing their information electronically, using it to make health decisions and track progress toward their goals. According to the most recent HINTS survey, more than 50% of patients accessed their electronic health information in the last year.[1] Despite recent policies and technologies, it is still exceedingly difficult for most people to access medical records. That same survey indicates that 1 in 3 patients experienced a gap in the information exchanged among providers. APIs have the potential to change the ways patients and caregivers engage with health information. APIs make it possible to pull in health information from multiple health care providers and hospitals using a patient or caregiver's preferred apps, which can help them better organize, understand and act on their health data. This process is significantly cheaper for the individual consumer than the alternative aggregation processes that have been identified at other times. Increasing consumer education about how their information may be collected, shared and used by apps will be foundational to securing and bolstering consumer trust.

- **Security:** Some individuals and organizations have stated that APIs are more susceptible to attack and breach than other forms of data transfer, including portal access, fax, or mail. We disagree. First, most API access is still based on users' initial usernames and passwords, similar to traditional portals, which have become ubiquitous across health care. Additionally, the Open Authorization (OAuth) standard, which is commonly used with HL7 FHIR®-based APIs, enables token-based access, which can be deleted or revoked at "any time for any reason - a security breach, misuse or even if the user decides they no longer want that service to have access to their account." Access to these tokens, built on appropriate identity proofing and patient authorization, can also restrict permissions for specific API access purposes or limit access within an application.[2] In addition, the FTC has exercised its authority to require commercial entities to adopt reasonable security safeguards and to notify consumers and federal regulators in the event of breaches. The use of restful, standard-based APIs is ubiquitous across numerous industries in addition to health care. API security in these other consumer and business contexts has not generally been an issue. Finally, we recognize that the use of APIs with EHRs is somewhat of a new concept. Providers and EHR vendors

[1] HINTS 5, Cycle 1 (2017)
[2] MuleSoft: How to Maximize Your API's Security; https://www.mulesoft.com/resources/api/api-security

will need some level of flexibility while working to implement consumer facing APIs, including app vetting and API surveillance.

- **Patient Identification and Authentication**: While much work continues to be done, health IT developers and health information professionals have made significant headway in advancing individual identification and authentication for API-based access. In addition to the previously referenced use of OAuth, the National Institute of Standards and Technology (NIST) published recommendations known as NIST Special Publication 800-63-2, or "Electronic Authentication Guideline" in 2013 as a common model for strong identity and authentication. In 2017, updated version 800-63-3 was published as the current specification for digital identities across the United States.[3]

- **Cost:** We understand that there has been a significant investment made to digitize medical records. One benefit that many policymakers anticipated was free flow of information, including consumer, patient, and caregiver access to their information. Nonetheless, there are additional requirements and we recognize the incremental costs to providers, payers, and EHR manufacturers from these requirements. Nonetheless, the use of FHIR was designed to maximize what can be done from existing technology. EHRs with standard-based API capabilities are in wide use according to recent ONC data and must be used for CMS incentive programs in 2019.[4] API-based access using the HL7® FHIR® standard, which is being used by developers implementing the ONC certification requirements, are by design, intended to enable lower-costs and enable non-proprietary interoperability between different health IT systems.

  Notwithstanding the availability of this technology in many care settings, consideration may also need to be given to those providers who have not yet been part of CMS' incentive programs.

- **Immature standards and inexperience using APIs:** Some argue that health care's experience with the relevant technology and standards is too new for the broad mandate established in recent law and regulation to use APIs and further, that there are not uniform standards for API deployment in healthcare. While standards and technology continue to evolve, much of health care has already agreed on a number of standards. Using such standards and implementation resources as HL7 FHIR®, SMART, and the Argonaut implementation guide, numerous health care entities are already moving significant amounts of data with very limited friction using the initial set of standards.[5] It is true that the current FHIR version is a Standard for Trial Use (STU), but it is being rapidly accepted as is the case with many healthcare STUs. Indeed, an STU is a standard fully approved and fit for production, with the indication that vendors should plan to make changes in the future as the standard evolves. Current adoption by multiple providers and technology vendors confirms this perspective. Iterations of deployment and standards improvements are expected to rapidly yield a richer data set, including CARIN's ongoing initiative to establish guidance for payers similar to previous Blue Button 2.0 work. Additionally, the API being activated in 2019 is a cautious and prudent approach because it is only allowing a single patient, or their proxy, read only access to that one patient's information. This access is only for the data fields defined in the common clinical data

[3] Additional information is available in the CARIN White Paper, "Patient Identity Proofing"
[4] https://www.healthit.gov/buzz-blog/interoperability/heat-wave-the-u-s-is-poised-to-catch-fhir-in-2019/
[5] Over 150 organizations are currently using the Argonaut Implementation Guide and FHIR standards to move data through Apple "Health Records" function; Similarly, over 200 applications have certified to Medicare's Blue Button 2.0 framework.

set, not all data. Queries for multiple patients, full open notes access, or the ability for patients to write back to the EHR are all functionality that may have great benefits but are out of the initial scope. In sum, the FHIR STU and quantity of information is a prudent and appropriate beginning for development and additional access.

- **Increased provider burden due to patient concern:** Many providers have expressed concern that giving patients widespread access to their own clinical data will result in a significant burden on health systems who must deal with an influx of queries related to inaccuracies or lack understanding of their health records. This issue has been studied as part of the OpenNotes initiative[6], which found that "the volume of electronic messages from patients did not change" and that "99% of patients wanted open notes to continue and no doctor elected to stop." Furthermore, improved access to notes resulted in 77%-87% of patients feeling more in control of their care.

Many CARIN participants experience challenges in implementing new technology, facilitating data exchange, and building new solutions. However, we are unified in our belief that more data can be moved throughout the ecosystem, with less friction, if standards-based APIs are the industry's preferred way for consumers and caregivers to access their data, appropriately incented through rulemaking. Consumers, above all, will be empowered to move their data where they desire and reach their health goals.

About CARIN

We are committed to enabling consumers and their authorized caregivers to have easy electronic access to their personal health information, especially information maintained in provider health IT systems. Specifically, we are promoting the ability for consumers and their authorized caregivers to gain digital access to their health information via the open Application Programming Interfaces (APIs) mandated under MACRA/MIPS and the HITECH/EHR Incentive Program and the Promoting Interoperability objective "Provider to Patient Exchange". The requirements for these APIs are defined in the 2015 Edition ONC certification criteria. They are intended to enable consumers to have their digital health information made available electronically, via an API, or any third-party application they choose.

Working collaboratively with government leaders, the CARIN Alliance seeks to rapidly advance the ability for 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. With a membership composed of consumers and patients and caregiver organizations, health care entities, health information technology developers and others, this alliance is uniquely positioned at the intersection of public and private organizations to advance the development of person-centered, value-driven health care through the adoption of consumer-directed health information exchange.

[6] http://annals.org/aim/fullarticle/1363511/inviting-patients-read-doctors-notes-quasi-experimental-study-look-ahead