CAQH CORE℠

WHITE PAPER

The Connectivity Conundrum:

How a Fragmented System Is Impeding Interoperability and How Operating Rules Can Improve It

CAQH CORE℠

The Connectivity Conundrum: How a Fragmented System Is Impeding Interoperability and How Operating Rules Can Improve It

CONTENTS

Executive Summary

Connectivity is essential for successful interoperability as it enables the transport of information to support data exchange. It encompasses the capacity to connect applications, computers, systems and networks to one another in a coordinated manner, within and across organizations. Perhaps the most critical component of connectivity is the use of communication protocols, which are the set of rules and standards by which data is transported, messaged, secured, authenticated and acknowledged.

In the healthcare industry, stakeholders have implemented a multitude of connectivity methods, based on open standards and proprietary approaches, to facilitate the exchange of administrative and clinical healthcare data. This has created a fragmented connectivity ecosystem where senders and receivers of electronic data are required to support multiple communication channels and protocols. The connectivity environment of today adds additional levels of operational complexity and elevated costs for stakeholders.

This burden is amplified by transactions, such as prior authorization, that require the intersection of administrative and clinical data. Further, the need to support multiple connectivity methods dissuades interoperability goals set forth by the 21st Century Cures Act[1] and interoperability rules proposed by the Office of the National Coordinator for Health Information Technology (ONC)[2] and the Centers for Medicare and Medicaid Services (CMS).[3]

To address the industry need to align on a common set of communication protocols, CAQH CORE developed and published three operating rules addressing connectivity and security of data exchange to establish a national base guiding healthcare communication of administrative data:

- Phase I CAQH CORE Connectivity Rule
- Phase II CAQH CORE Connectivity Rule
- Phase IV CAQH CORE Connectivity Rule

The CAQH CORE Connectivity Rules drive industry alignment by converging on common transport, message envelope, security and authentication standards to reduce implementation variations, improve interoperability and advance the automation of administrative data exchange.

In 2013, the Phase I and II CAQH CORE Connectivity Rules were nationally mandated by the Department of Health and Human Services (HHS) per Section 1104 of the Affordable Care Act (ACA). The Phase IV CAQH CORE Connectivity Rule was published in 2015. As a result of the federal mandate, a large industry installed base of the Phase II CAQH CORE Connectivity Rule exists among HIPAA-covered entities that exchange administrative transactions. Further, as tracked via CORE Certification, health plans representing 188 million covered lives in the United States have publicly certified they can exchange healthcare data via Phase II CAQH CORE Connectivity, in

addition to nearly 100 clearinghouses and vendor products. As such, a strong industry foundation for communication interoperability has been set by the CAQH CORE Connectivity Rules.

As the healthcare industry progresses towards achieving alignment and interoperability across administrative and clinical systems, common methods of connectivity could ease the burden of data exchange. The industry is beginning to gravitate to Application Programming Interfaces (API) and Representational State Transfer (REST) as methods for connectivity and data sharing. In 2020, CAQH CORE participating organizations will consider updates to the CAQH CORE Connectivity requirements to move the industry towards a common set of Safe Harbor connectivity methods that address existing and emerging standards and protocols to support the intersection of administrative and clinical data exchange. CAQH CORE Operating Rules, which can be federally mandated for all HIPAA-covered entities, can serve as a bridge between existing and emerging standards, while ensuring connectivity alignment and common data content across exchanges.

CAQH CORE: Driving Automation

As stakeholders first began to implement HIPAA electronic transaction standards in the early 2000s, no operating rules existed to guide implementation. Health plans, healthcare providers and vendors were left to decide for themselves how to define key terms or the specific protocols for sharing data. Non-uniformity quickly became the norm. The use of proprietary systems and workarounds had an effect opposite that intended by HIPAA administrative simplification provisions. Administrative complexity rose sharply.

The industry solution was to establish CAQH CORE and task it with driving the creation and adoption of healthcare operating rules[4] that support standards, accelerate interoperability and align administrative and clinical activities among providers, payers and consumers. Beginning in 2005, the organization broke new ground with a consensus-driven process that brought diverse stakeholders together to iron out the "rules of the road" for implementing HIPAA and other standards.

In its first three phases of operating rules, CAQH CORE addressed interoperability challenges for eligibility and benefit verification, claim status, claim payment and remittance advice. It also launched a successful certification program. During this period, adoption of the rules was entirely voluntary, yet many organizations implemented the rules because they saw the value.

This experience led the Secretary of HHS to tap CAQH CORE in 2012 as the designated authoring entity for federally mandated operating rules under Section 1104 of the ACA.[5] HHS also adopted the first three phases of CAQH CORE rules, originally voluntary, as mandatory for all HIPAA-covered entities under the ACA. Since that time, CAQH CORE has authored additional rules addressing claim submission, prior authorization, enrollment/ disenrollment and premium payment.

Most recently, the scope of CAQH CORE has expanded to include improving the collective exchange needs of value-based payment and medical documentation. In 2018, the organization published results of an expansive study[6] drawing parallels between the administrative and operational challenges associated with value-based payment today and those experienced in the early 2000s with fee-for-service. Further, in 2019, a report on medical documentation[7] was published identifying opportunity areas to improve and automate the sharing of documentation by bridging administrative and clinical systems. CAQH CORE participating organizations are actively developing operating rules to help ease value-based payment and medical documentation burdens.

Since 2007, operating rule implementers have had a means to voluntarily validate and demonstrate that their systems are operating in conformance with the rules through CORE Certification. CAQH CORE has awarded more than 370 certifications to healthcare organizations. Today, these organizations collectively cover 80 percent of commercially insured lives, 77 percent of Medicare Advantage lives and 50 percent of Medicaid covered lives in the United States. In addition, nearly 100 clearinghouses and vendor products have achieved CORE Certification.

1. Connectivity: Enabling Healthcare Interoperability

As the healthcare industry progresses towards achieving alignment and interoperability across administrative and clinical systems, the ability to quickly, reliably and affordably connect systems is critical. The CAQH CORE Connectivity Rules address connectivity and security of administrative data exchange and establish a national base guiding healthcare communication. In 2020, CAQH CORE participating organizations will consider updates to the CAQH CORE Connectivity requirements to move the industry towards a common set of Safe Harbor connectivity methods that address existing and emerging standards and protocols to support the intersection of administrative and clinical data exchange. This white paper describes the current state of CAQH CORE Connectivity, its value to the industry and future opportunities for operating rule enhancements. CAQH CORE Connectivity, which can be federally mandated for all HIPAA-covered entities, can serve as a bridge between existing and emerging standards, while ensuring connectivity alignment and common data content across exchanges.

DEFINING CONNECTIVITY

Connectivity is a generic term for connecting devices such as computers, information systems or networks to each other to facilitate data access and exchange. It enables organizations to access, collect, share and utilize data within and across disparate enterprises. Further, connectivity is essential for interoperability as it provides the ability to exchange and integrate information across different information systems.[8]

Connectivity addresses a variety of protocols and standards including transport, message envelope, security, authentication, communication errors and acknowledgements. Key features that are encompassed by connectivity are defined in Figure 1 on the next page.

Today, connectivity in healthcare employs a variety of communication modes, e.g., dial-up, file transfer protocol (FTP), virtual private network (VPN), frame relay, Internet, etc., each of which has its own set of protocols or standards. Stakeholders often support multiple connectivity methods to connect to different health plans, clearinghouses, provider organizations and others to electronically access and exchange information. Further, within an organization, systems and applications have a need to connect and integrate with each other to facilitate data exchange, such as in the case of bridging administrative and clinical systems to support prior authorization.

Figure 1: Key Components of Connectivity

Features	Definitions	Examples
Payload(s)	Transmitted data that is the actual intended message	ASC X12 Administrative Transactions NCPDP, HL7 v2.x or v3 Messages Other
Submitter (Client) Authentication	Verification that submitting system credentials match the credentials for the receiving system	X.509 Digital Certificate Tokens/OAuth Username + Password
Message Interactions	Methods computers use to communicate with each other	Real Time, Batch, Generic Push and Pull Interactions
Message Envelope Metadata	Information about the sender, receiver and destination of a message	CORE-specified Message Envelope Metadata
Message Envelope(s)	Specification for enclosing transmitted data	MIME Multipart SOAP + WSDL
Transport Security	Protocol used to secure web (HTTPS) connections	Secure Sockets Layer (SSL) Transport Layer Security (TLS)
Transport Layer	Ensures the reliable arrival of messages and responsible for end-to-end communication over a network	HTTP over TCP
Network	A group of two or more computer systems linked together	Public Internet

CONNECTIVITY USE CASE: PRIOR AUTHORIZATION

Prior authorization is a process to obtain health plan approval for provision of specific healthcare services to a patient covered by the health plan. For prior authorization, there is a need to facilitate access to or exchange of administrative data to determine if a prior authorization is required and to identify what clinical documentation may be needed to prove medical necessity and obtain approval for a service. On the provider end, connectivity and integration should be in place between administrative systems (e.g., practice management systems) and clinical systems (e.g., electronic health records) to ensure clinical data can be retrieved and used in an automated fashion with the corresponding prior authorization request. Administrative and clinical data needed to support prior authorization are typically stored and shared across different system environments and are exchanged across multiple interactions. To reduce manual burden and ease access to administrative and clinical data, there is a need for these systems to align and support common connectivity methods.

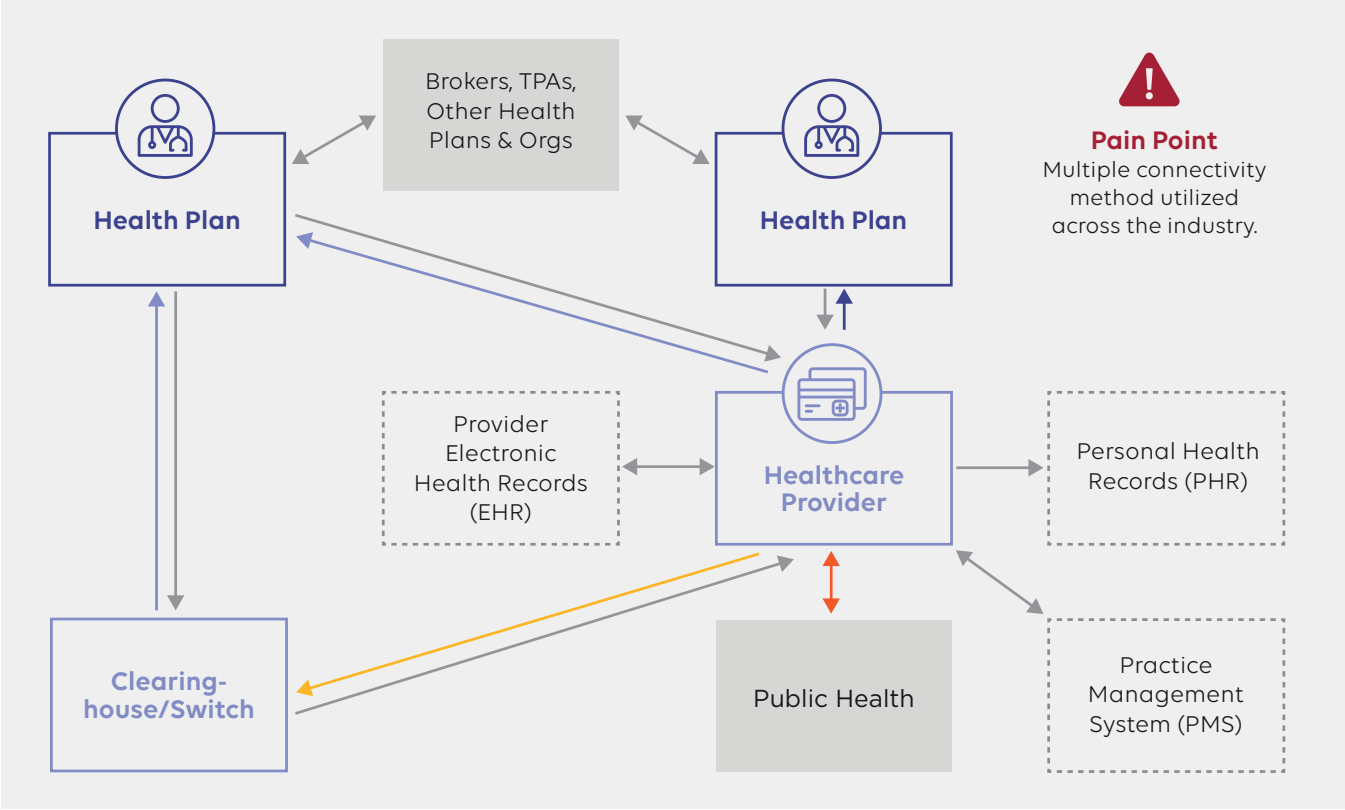
A MULTITUDE OF METHODS: A BARRIER TO INTEROPERABILITY

Currently, numerous connectivity methods – some based on open standards, others on proprietary approaches – are in use to exchange administrative and clinical information across the healthcare industry. A fragmented connectivity environment requires both senders and receivers of electronic data to support multiple connectivity methods, adding additional levels of operational complexity and elevated cost that dissuade interoperability, as in the case of prior authorization.

The diversity of connectivity methods used to exchange healthcare data ranges from high-speed, dedicated lines to low-speed, dial-up lines into bulletin board/web portal-type systems, as well as FTP, VPN, Hypertext Transfer Protocol Secure (HTTPS) and Web Services over the Internet. Each

of these connectivity modes can be either direct between trading partners or to intermediaries, such as clearinghouses, that serve as switches/hubs or provide other services for both providers and health plans. Figure 2 highlights common connectivity implementations in healthcare, each architected with a variety of standards and protocols to facilitate communication across trading partners.

Figure 2: Common Connectivity Implementations



HIPAA provided a foundation for standardizing administrative data interactions between healthcare 7 stakeholders. However, the manner and consistency in which these data interactions initially occurred, from a business perspective, were inconsistent and variable. The CAQH CORE Operating Rules build upon the standard transactions adopted by HIPAA,[9] which guide how data should be formatted. The operating rules support the end-to-end workflow to make electronic data transactions more predictable and consistent, regardless of technology. A key pillar of the CAQH CORE Connectivity Rules is the concept of Safe Harbor, which addresses the business issue of industry needing to support multiple modes of connectivity to enable interoperability. The intent of Safe Harbor is to establish a common, base set of connectivity requirements for industry to implement, while including provisions that account for different levels of industry maturity. The CAQH CORE Connectivity Rules have been successful in promoting interoperability for the exchange of administrative data, however, more work is needed to update and expand these rules to bridge connectivity and interoperability barriers between administrative and clinical systems.

SUPPORTING INTEROPERABILITY

Health information technology interoperability exists on four levels, each characterized by the needs and opportunities of a particular segment of the data exchange:[10]

- **Foundational interoperability** is the capability of a system to transfer data to and receive data from another system.
- **Structural interoperability** refers to the capability of a system to preserve the original composition or syntax of healthcare data as it moves between systems and to ensure that the clinical or operational context are fully retained. Structural interoperability is needed to support analysis of transferred data at the data field level. Importantly, the use of accepted data standards by all parties to the data exchange is needed to achieve structural interoperability.
- **Semantic interoperability** is the capability of two or more systems to enter a data exchange and use the information transferred. It leverages data structure against a common vocabulary made up of data sets, code sets and data definitions, a process known as codification of the data, to support data analysis.
- **Organizational interoperability** refers to the policies and governance needed to support the smooth exchange of data between organizations, stakeholders and patients.

Connectivity is fundamental for systems to interoperate. It enables data exchange and allows for subsequent processes to occur, presenting data in ways that can be easily understood by an end user. Despite progress made by the healthcare industry to resolve structural and semantic interoperability challenges, the presence of a fragmented foundational connectivity ecosystem for the intersection of administrative and clinical data continues to inhibit successful, industry-wide interoperability.

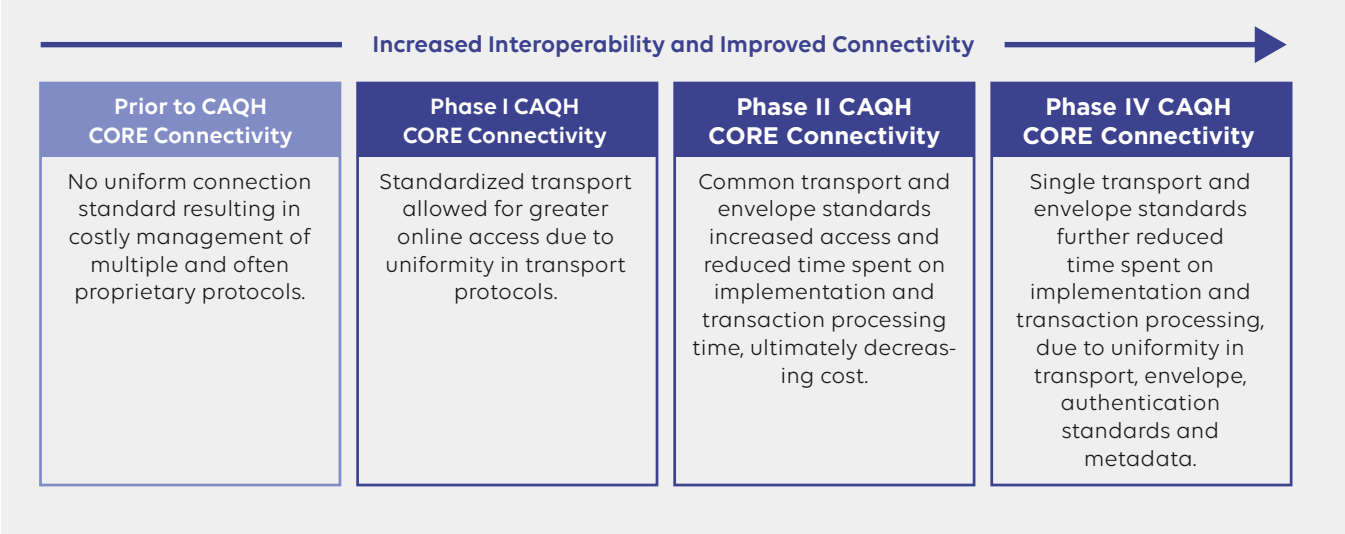
A major goal of the 21st Century Cures Act is to achieve nationwide interoperability.[11] To help realize this goal, ONC and CMS published proposed rules to facilitate patient access to information through HL7 FHIR APIs including administrative data, such as claims data, that has historically been shared between health plans and providers through different methods.[12, 13] Common, uniform and consistent connectivity approaches, including the use of APIs, could support a broader range of use cases connecting clinical and administrative data across stakeholder groups including patients, providers, health plans and vendors to achieve industry-wide interoperability.

2. CAQH CORE Connectivity: A Uniform Approach

OVERVIEW OF THE CAQH CORE CONNECTIVITY RULES

To promote interoperability, CAQH CORE developed three operating rules (Phase I CAQH CORE Connectivity Rule, Phase II CAQH CORE Connectivity Rule and Phase IV CAQH CORE Connectivity Rule) addressing connectivity and security of administrative data exchange to establish a national base guiding healthcare communication (Figure 3). Specifically, the CAQH CORE Connectivity Rules address the transport of transactions such as eligibility, claim status, healthcare claims, remittance advice and prior authorization between stakeholders. From a technical perspective, the rules streamline industry connectivity by converging on common transport, envelope, security and authentication standards to reduce implementation variations and improve interoperability and efficiency of administrative transactions.

Figure 3: Evolution of CAQH CORE Connectivity



The CAQH CORE Connectivity Rules enable a framework for interoperability that is universal, easy to implement, low cost, secure, trusted, meaningful and industry recognized. Benefits include:

- Specifying a **"Safe Harbor"** enabling baseline expectations for connectivity while **promoting flexibility** and supporting organizations at different levels of technology maturity.
- Establishing a **secure and trusted method** for exchange of information over the Internet by providing security and authentication protocols.
- Enabling connectivity and its associated requirements to be **payload agnostic**, supporting a variety of data types and allowing for compatibility with existing and emerging standards.
- Supporting **error handling** using standard error codes to notify all parties whether a communication has occurred successfully.
- Promoting **ease of implementation** with connectivity schemas available at no cost.
- Enabling **direct lines of communication** with trading partners minimizing complexity and cost.

Connectivity and security protocols and standards identified in the CAQH CORE Connectivity Rules for 9 implementation are identified and voted on **for industry by industry**.
- **Widely implemented and accepted** across the industry.

MARKET ADOPTION OF CAQH CORE CONNECTIVITY

HIPAA regulations adopted specific standards for electronic healthcare claims, eligibility/benefits inquiries, prior authorization and other transactions. These standards include those specifying the structure and data (X12 and NCPDP) for a transaction as well as certain medical and non-medical code sets (CPT, ICD-10, etc.). Fulfilling part of its requirement under Section 1104 of the ACA, HHS adopted the Phase I and II CAQH CORE Operating Rules to support adoption of these transactions, making the CAQH CORE Connectivity Rules nationally mandated with an implementation deadline of January 1, 2013. CAQH CORE published the Phase IV CAQH CORE Connectivity Rule in 2015. All three CAQH CORE Connectivity Rules are included in the Interoperability Standards Advisory, maintained by ONC, which serves as a catalogue of interoperability standards and implementation specifications for use in healthcare.[14]

Per the federal mandate, implementation of the Phase II CAQH CORE Connectivity Rule is a requirement for all HIPAA-covered entities. Thus, a large installed base of CAQH CORE Connectivity exists among HIPAA-covered entities that exchange administrative transactions. This means the industry already has a strong foundation in place that supports common and uniform methods for connecting health IT systems together to exchange healthcare transactions with agreed-upon transport, enveloping, security and authentication protocols.

In addition to this, the CORE Certification program provides further evidence of deep market penetration by the CAQH CORE Operating Rules, including CAQH CORE Connectivity. More than 370 certifications have been awarded across the private and public sectors establishing a foundation where:

- 80 percent of commercial lives are in health plans that are CORE-certified.
- 77 percent of Medicare Advantage lives are in health plans that are CORE-certified.
- 50 percent of Medicaid lives are in health plans or state fee-for-service programs that are CORE-certified.

Additionally, nearly 100 clearinghouses and vendor products have achieved CORE Certification. Overall, CORE Certification market share indicates that healthcare data for most covered lives in the U.S. can be exchanged via Phase II CAQH CORE Connectivity; reinforcing the strong foundation set by the CAQH CORE Connectivity Rules to facilitate the exchange of administrative data.

COMPONENTS OF CAQH CORE CONNECTIVITY

There are five primary components of the CAQH CORE Connectivity Rules: Safe Harbor, transport, message envelope, security and authentication. These components are reflective of the types of communication elements needed to support interoperable exchanges of data. The connectivity rules define conformance requirements for stakeholders based on a typical role (client, server) for message envelope and authentication standards.

Safe Harbor

The CAQH CORE Connectivity Rules use the public internet and HTTPS to facilitate information exchange, establishing a Safe Harbor connectivity method that vendors, providers and health

plans can be assured will be supported by any HIPAA-covered entity. This means that an organization should be capable and ready at the time of a request by a trading partner to exchange data using a CAQH CORE Connectivity Rule.

Transport

Methods computers use to communicate with each other are often referred to as message interactions or message interaction patterns which describe how connections are established and used for handling requests and responses. The CAQH CORE Connectivity Rules address synchronous and asynchronous message interaction patterns.

- Synchronous: Entity initiates a new connection to send a request; the same connection is used to receive the response for the request. Typically associated with a Real Time mode of processing the message payload.
- Asynchronous: Connection is established to send a request; response is sent on a separate connection. Typically associated with a Batch mode of processing the message payload.

Message Envelope

An envelope or message envelope is a specification for enclosing transmitted data and includes information about the sender, receiver and destination of a message. It also provides a container for electronic documents (e.g., X12 278) to be transmitted from the sender to receiver. Message envelope metadata includes information to identify the sender/receiver and ensures that documents are delivered to the receiver. The CAQH CORE Connectivity Rules include a well-defined structure for organizing and formatting message envelope metadata. This helps message receivers route messages for internal processing without opening the envelope, reducing costs and improving response times. The Phase II CAQH CORE Connectivity Rule supports two envelope standards: SOAP + WSDL and HTTP + MIME Multipart. The Phase IV CAQH CORE Connectivity Rule converges to a single envelope standard: SOAP+WSDL.

- SOAP+WSDL
  - SOAP (Simple Object Access Protocol) is a protocol specification for exchanging structured information based on XML using web services.
  - XML (Extensible Markup Language) is a meta-language that allows users to define their own customized way to describe data; the language used in CAQH CORE Connectivity to create COREspecific metadata.
  - Web Services Description Language (WSDL) is a document written in XML to describe a web service (the software system to support machine-to-machine interactions over a network).
- HTTP+MIME Multipart
  - Multipurpose Internet Mail Extensions (MIME) is an Internet standard that extends the format of email to support text in character sets other than ASCII; Non-text attachments such as audio, video, images, application programs etc.; and message bodies with multiple parts.[15]
  - Multipart/form-data is used to express values submitted through a form; it is most commonly used for submitting files via HTTP.

Security

Transport Layer Security (TLS) is a cryptographic security protocol used over the Internet to keep data transmissions private. This includes data transfers when the Internet is used for browsing, to access applications and to communicate. Its predecessor, the Secure Socket Layer (SSL) protocol, uses a system of keys to guard data transmissions.[16]

The Phase II and Phase IV CAQH CORE Connectivity Rules require communications using a secure and encrypted 11 transport protocol such as SSL 3.0 or TLS 1.0 or higher.

Authentication

The most foundational aspect of security relates to the ability to accurately identify people, places and things, such as organizations. Most applications of security protocols, whether authentication, access control, digital signatures, etc., rely on the correct mapping between the relevant resources and the underlying systems. The Phase II CAQH CORE Connectivity Rule requires communications to be authenticated by the submitter via username and password or through a digital certificate and be sent by a secure and encrypted transport protocol such as SSL or TLS. The Phase IV CAQH CORE Connectivity Rule converges to a single and more secure authentication requirement, by requiring the use of X.509 Client Authentication (mutual authentication).

CAQH CORE CONNECTIVITY USE CASE: PRIOR AUTHORIZATION

The CAQH CORE Prior Authorization Rules[17, 18] promote automation of the prior authorization process. These rules, recently approved by the industry, standardize the data shared between plans and providers, eliminating unnecessary back-and-forth, accelerating adjudication timeframes and freeing staff resources spent on manual follow up. In particular, the rules standardize data to provide direction on status and clinical documentation needs and offer providers a more consistent, efficient and predictable process across all the plans with which they participate. To set a foundation for this data exchange to occur, the rules set uniform connectivity expectations when exchanging the HIPAA-mandated X12 278 (prior authorization) transaction. In alignment with key concepts of connectivity, the prior authorization rules today require the following:[19]

Transport – Requires use of Synchronous or Asynchronous connections, or both, for sending prior authorization transactions.

- Message Envelope – Requires the use of SOAP+WSDL messages and specific message envelope metadata (e.g. Sender ID, Receiver ID, Payload ID, Payload Type) to ensure prior authorization transactions are successfully delivered.
- Security – Requires that prior authorization exchanges between sender and receiver be secured and protected with TLS 1.1 or higher.
- Authentication – Requires submitters to authenticate prior authorization exchanges through the use X.509 Digital Certificates over TLS 1.1 or higher to ensure the data being exchanged is coming from a trusted source and over an encrypted channel.

Although a common set of communication protocols exists via CAQH CORE Connectivity to exchange the prior authorization transaction, the data within this exchange is primarily administrative. As described in the prior authorization use case, clinical data is often requested by the health plan to support a prior authorization request. As such, a gap exists today to support the exchange of this clinical data. As the HHS-designated operating rule author, CAQH CORE is currently working with the industry to develop operating rules to streamline the exchange of medical documentation across a variety of use cases including prior authorization. In addition, in 2020 CAQH CORE participating organizations will consider updates to the CAQH CORE Connectivity Rules to support the convergence of administrative and clinical data exchange.

3. Support for Emerging Technologies, Standards and Industry Needs

The need for common methods of connectivity aligned across administrative and clinical systems is imperative as the healthcare industry strives to achieve interoperability. The transition to value-based care compounds the critical importance of seamless data exchange. The five components of CAQH CORE Connectivity - Safe Harbor, transport, envelope, security and authentication - are foundational to existing and new approaches for electronically exchanging data. In 2020, CAQH CORE will engage the industry to consider updates to the CAQH CORE Connectivity requirements to move the industry towards a common set of Safe Harbor connectivity methods that address existing and emerging standards and protocols to support alignment needed for administrative and clinical data exchange.

REST OR SOAP?

REST and SOAP are methods of communication between applications that are often compared. REST communications are inherently data-driven, while SOAP communications are primarily operational with regard to the transfer of information.

- REST is an architectural style that is centered around the transfer and representation of resources through GET/POST/PUT/DELETE requests over HTTP. In REST, data and functionality are considered resources and are accessed over the web using Uniform Resource Identifiers (URI).20 Resources are acted upon using stateless communication which means when a client sends a request to a server it must contain all information necessary for a server to respond. Each request is standalone and independent from previous client-server interactions, a feature that enables scalability and uniform accessibility.
- SOAP is a standardized protocol that operationally defines how to exchange messages over HTTP or any other transfer protocol. SOAP messages are very structured and consist of four elements: envelope (defines start and end of a message), header (contains optional attributes of the message, typically used for processing) , body (contains the payload or data being sent) and fault (provides information about errors).21 SOAP is viewed as a neutral protocol of message interactions between sender and receiver which can be made independent of platform and language, a feature that enables data to be exchanged over distributed and decentralized environments that involve multiple trading partners.

REST may improve performance, provide simplicity and could have a low entry barrier for implementers. Yet flexibility within the REST architecture style can leave room for different implementation interpretations, which may lead to incompatibility among loosely coupled systems. In some instances, the implementation of web services built upon a REST architectural style may vary. In comparison, SOAP implementations are well-defined by standards-based interface capabilities which are valuable for enterprise-level communications. As such, SOAP exchanges take longer to setup and may require more bandwidth in order to share information due to its dependency on protocols and strict message structures. CAQH CORE Connectivity Rules have addressed these barriers to ease the burden of SOAP implementations by defining a uniform message structure for industry to use when exchanging the HIPAA-mandated administrative transactions. As implementations of REST become more prominent in the healthcare industry,

CAQH CORE can take a similar approach in a future connectivity rule to build uniform guidelines to coordinate REST exchanges of clinical and administrative information between health plans and providers.

WHAT ABOUT APPLICATION PROGRAMMING INTERFACES (APIS)?

An Application Programming Interface (API) is a communication protocol, designed using REST or SOAP, that allows multiple applications or systems to interact to share information. From a technical perspective, an API provides developers with a way of communicating instructions between a client and server. Essentially, APIs are a simplified way for organizations to connect into their own system environments and share data with external stakeholders using a defined set of specifications and protocols.

HL7 FHIR APIs are a hallmark of the proposed CMS and ONC interoperability rules to provide patient access to information historically exchanged between plans and providers such as claims data. Although the proposed rules are scoped around consumer access to healthcare data via APIs, they provide an opportunity for the industry to leverage an API framework and align administrative and clinical data exchanges between providers and health plans.

HL7 FHIR is an emerging electronic standard that supports REST APIs.[22] HL7 FHIR specifies data formats and elements in an API for the exchange of healthcare data. The foundational connectivity concepts of transport, message envelope, security and authentication apply to information exchanged via the HL7 FHIR paradigm:

- Transport - A communications protocol responsible for establishing a connection and ensuring that all data has arrived safely. HL7 FHIR communications can occur synchronously or asynchronously.
- Message Envelope – A key aspect of HTTP and foundational to how data is exchanged over the World Wide Web. In a HL7 FHIR exchange, resources can be represented in the following formats: XML, JavaScript Object Notation (JSON) and Terse RDF Triple Language (Turtle).[23]
- Security – Enables privacy, integrity and protection for data transmitted between different nodes on the Internet. HL7 FHIR specifies that data exchange communications should be secured using TLS 1.2 or higher.
- Authentication – A foundational competency for any security system. HL7 FHIR recommends that OAuth 2.0 be used when user/clients need to be authenticated. Further, HL7 FHIR recommends the use of the SMART Launch App Framework[24] to establish authorization access and permissions when third party applications connect to Electronic Health Record data.

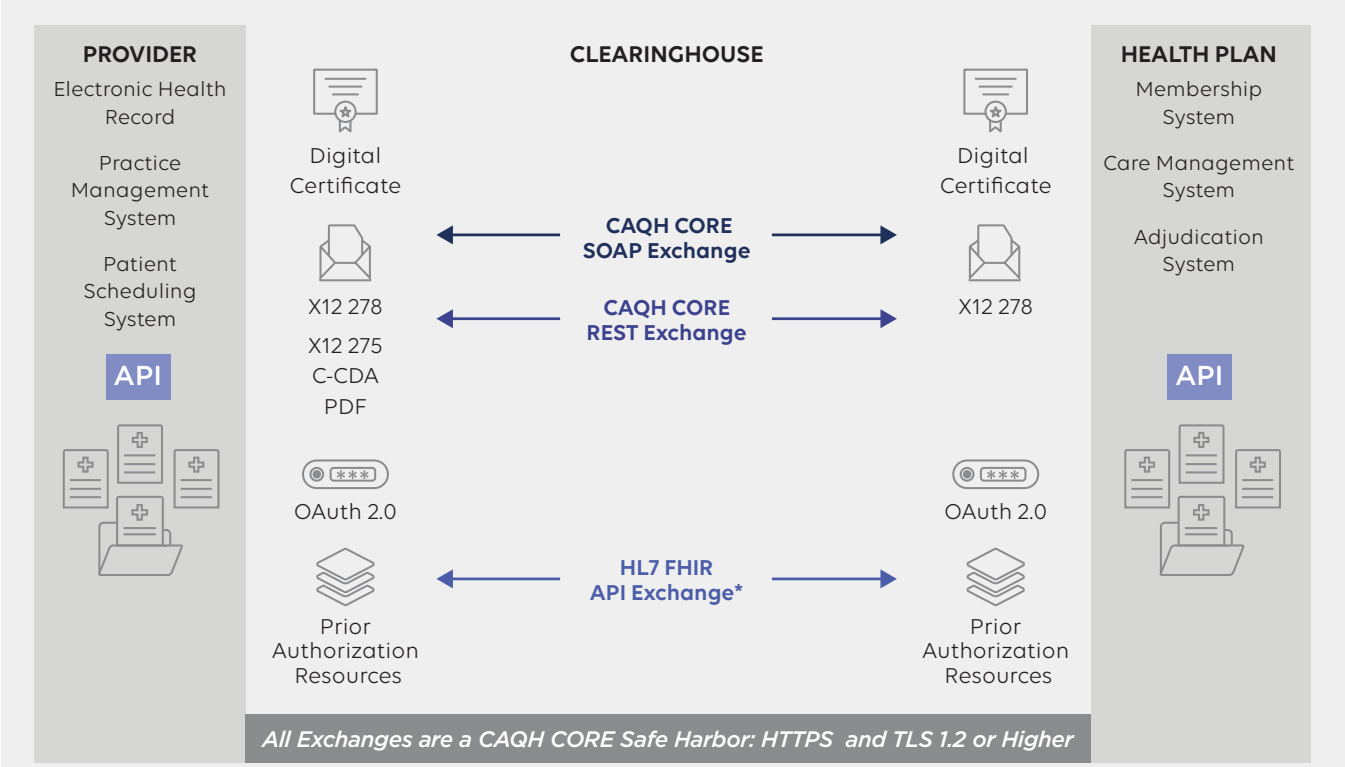
4. Future Vision for CAQH CORE Connectivity

The next version of the CAQH CORE Connectivity Rule can serve as a bridge between existing and emerging standards and protocols to ensure industry interoperability needs are met to support the intersection of administrative and clinical data. CAQH CORE Connectivity requirements are payload agnostic and can be updated to accommodate APIs for SOAP, REST and HL7 FHIR to support the exchange of data in a variety of data formats. For example, incorporating REST, SOAP or HL7 FHIR may not be an and/or decision, but rather a when/why consideration as to which is the most appropriate technology available and to be used for the best business outcome. As such, there is opportunity through CAQH CORE Connectivity Rules to add support for REST and HL7 FHIR APIs, aligning the specification to existing communication features, such as SOAP, to drive a more flexible and coordinated approach for information exchange.

FUTURE CAQH CORE CONNECTIVITY USE CASE: PRIOR AUTHORIZATION

Using prior authorization as an example, Figure 4 below shows a future vision of how CAQH CORE Connectivity could enable progress in the automation of prior authorization and support the convergence of clinical and administrative data. Updated rule requirements could include stakeholder support of APIs, enabling access and data sharing between administrative and clinical systems, creating a shared connectivity environment within and across organizations. Further, the rule could require a Safe Harbor for industry to support SOAP, REST and HL7 FHIR exchanges with associated authentication methods, with expectations that data should be exchanged securely over the public internet.

Figure 4: Examples of Future Approaches for CAQH CORE Connectivity



*The Prior Authorization Resource must be converted to the X12 278 data standard for HIPAA compliance.

Figure 4 depicts three different connectivity approaches to exchanging healthcare data between providers and health plans to support prior authorization. These are meant to serve as examples of potential exchanges that CAQH CORE participating organizations could address in the next version of CAQH CORE Connectivity.

Using APIs, data on internal systems can be accessed, transmitted and integrated in multiple ways to external systems, eliminating the need to map to a specific data and exchange format. An API-driven approach for data exchange could be designed to align with HIPAA mandates and CMS and ONC interoperability rules to support provider to payer exchanges. For example, administrative data from a practice management system could be formatted to a set X12 HIPAA-mandated transaction data standard and exchanged via API, and clinical data

from an electronic health record could align to the United States Data for Interoperability Standard (USCDI)[25] as a method for sharing data via a HL7 C-CDA or HL7 FHIR Resource exchanged via API. This is one of many approaches that could be leveraged for administrative and clinical data exchange, as APIs provide needed flexibility to exchange information in a structured, yet open framework.

Inclusion of APIs in the next CAQH CORE Connectivity Rule could help to resolve challenges associated with data access and integration by aligning how administrative and clinical data connects within a workflow. As an example, operating rules could set base expectations for API design, such as specifying a minimum set of administrative and clinical data standards for APIs to support. In the case of prior authorization, clinical and administrative data could be extracted

via APIs from various systems and packaged into an X12 278 + X12 275 or a Prior Authorization Resource. From there, prior authorization data could be exchanged from provider to payer via SOAP, REST or HL7 FHIR as described below:

- The **CAQH CORE SOAP Exchange** is supported by the currently published CAQH CORE Connectivity Rules and requires the use of Digital Certificates for authentication.
  - *Prior Authorization Use Case – CAQH CORE SOAP Exchange:* In this exchange, a provider formats administrative prior authorization data into an X12 278 Request and attaches supporting medical documentation such as a HL7 C-CDA aligned to the USCDI, PDF or JPEG within an X12 275 transaction. The data is embodied in a message envelope and exchanged via SOAP. A health plan then processes the data received and generates an X12 278 Response to communicate the prior authorization decision to the provider.

- The **CAQH CORE REST Exchange** represents a potential CAQH CORE Connectivity Rule which addresses the use of REST for the conduct of an X12 transaction, a HL7 FHIR Resource or any other data format, including HL7 C-CDAs, PDFs or JPEG. This exchange type could require the use of Digital Certificates or OAuth 2.0 for authentication.
  - *Prior Authorization Use Case – CAQH CORE REST Exchange:* In this exchange, a provider formats administrative prior authorization data into an X12 278 Request and attaches supporting medical documentation such as a HL7 C-CDA aligned to the USCDI, PDF or JPEG within an X12 275 transaction. The data is exchanged via a REST API. A health plan then processes the data received and generates an X12 278 Response to communicate the prior authorization decision to the provider.

- The **HL7 FHIR API Exchange** is organized as HL7 FHIR Resources and transmission occurs over the internet via REST. HL7 FHIR standards and the proposed CMS and ONC interoperability rules recommend the use of OAuth 2.0 for authentication. A potential CAQH CORE Connectivity Rule could support alignment of X12 HIPAA data standards and HL7 FHIR Resources through an API envelope.
  - *Prior Authorization Use Case - HL7 FHIR API Exchange:* In this exchange, a provider formats and bundles administrative data and clinical data aligned to the USCDI into HL7 resources. The data is exchanged via a HL7 FHIR API. Along the exchange, administrative data is mapped to an X12 278 Request to ensure HIPAA compliance. A health plan then processes the data received and generates a response organized as a resource, which is then mapped back as an X12 278 Response and communicates the prior authorization decision to the provider.

All three approaches could become components of a Safe Harbor in a future CAQH CORE Connectivity Rule. Allowing data exchange over APIs using HTTPS and TLS 1.2 or higher standards, could establish an updated national floor for connectivity to support alignment of administrative and clinical data exchange.

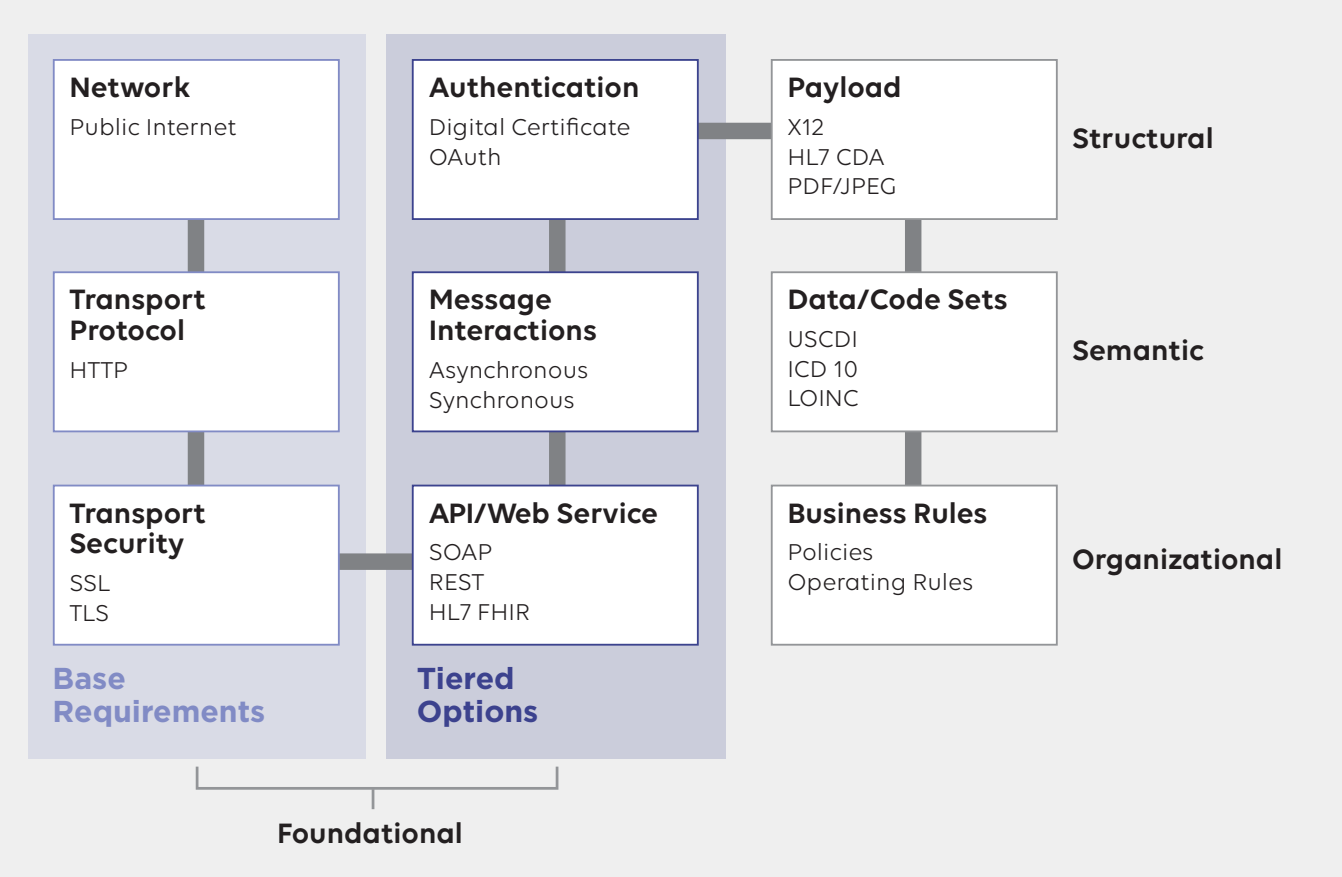
CAQH CORE CONNECTIVITY APPROACH FOR INTEROPERABILITY

An updated CAQH CORE Connectivity Rule could establish a Safe Harbor that aligns to existing IT implementations and supports emerging approaches for exchanging data. As a result, the framework for such a rule could be structured, yet flexible, by requiring industry to implement a base set of mature standards and providing tiered optionality for emerging standards. Although a different approach from prior CAQH CORE Connectivity Rules where all Safe Harbor requirements are required for implementation, the addition of tiered options as part of a new connectivity

rule could be positioned to align with business needs and use cases. For example, connectivity requirements could remain the same for electronic transactions that are highly adopted or perhaps only touch one system, such as eligibility, whereby SOAP would only be required. However transactions that are poorly adopted or touch multiple systems, such as prior authorizations and attachments, may benefit from the support of multiple connectivity methods such as SOAP, REST and HL7 FHIR. Overall, the goal of Safe Harbor remains the same which is to build alignment across trading partners and support opportunities for interoperable data exchange.

Figure 5 below illustrates an example of an end-to-end interoperable exchange, with a focus on foundational interoperability, and how a future CAQH CORE Connectivity Rule could establish base and tiered options in order to build a connected healthcare ecosystem.

Figure 5: CAQH CORE Connectivity – Interoperability Approach



To support industry progress towards national interoperability goals, a future CAQH CORE Connectivity Rule, at the foundational level, could establish a base set of requirements for all industry to implement, then use a tiered approach to accommodate SOAP, REST and HL7 FHIR APIs discussed earlier. For example, all communications involving HIPAA-mandated transactions could be conducted over the public internet using HTTP and be secured using SSL or TLS. Stakeholders could then use APIs to engage in data sharing, but be offered the choice to exchange via SOAP, REST or HL7 FHIR. Communication expectations for synchronous and asynchronous message interactions could differ depending on business needs. Data exchanges could be authenticated using methods such as Digital Certificate or OAuth.

CAQH CORE Connectivity is an established method for data exchange in the industry, and by building upon its existing set of requirements through a tiered approach, a future rule has the potential to address many foundational interoperability challenges. As the next version of the CAQH CORE Connectivity Rule is developed, the industry will need to find common ground to align on a designated set of specifications that considers existing and emerging connectivity approaches to address the challenges associated with administrative and clinical data exchange.

5. Next Steps

Healthcare stakeholders are united around the common goal of building an interoperable healthcare ecosystem; yet they continue to struggle with how to align across diverse systems and stakeholders. There is an opportunity for operating rules to bridge the gap between existing and emerging standards and achieve alignment to support administrative and clinical data exchange. In its role as the HHS-designated operating rule authoring entity, CAQH CORE and its operating rules can serve as an essential mechanism to set the course for long-term industry interoperability.

Achieving this vision requires industry collaboration and common agreement among public and private sector stakeholders. As demonstrated in this report, an opportunity exists through CAQH CORE Connectivity to bring industry stakeholders together to address this challenge. Already a trusted method for data exchange, nationally mandated and widely implemented, the next version of CAQH CORE Connectivity can provide a new baseline for connectivity protocols. This can include APIs to support organizations at various levels of maturity while improving interoperability across the industry, particularly for use cases like prior authorization that require the intersection of administrative and clinical data exchange.

To ensure that the evolving needs of health plans, providers and consumers are met, CAQH CORE will apply its integrated model of rule development. It will launch work groups, engage in discussions and consider pilot projects in 2020 to advance updated connectivity rule requirements to propel the industry toward a more optimized approach to data exchange.

In addition, CAQH CORE continues to educate industry participants about the need for action and on the progress of its initiatives to advance interoperability. To become involved or to ensure that you receive future information about this and other initiatives, please send an email to core@caqh.org.

End Notes

1 "H.R.34 – 21st Century Cures Act," Congress.gov website, accessed October 30, 2019, https://www.congress.gov/ bill/114th-congress/house-bill/34/text.

2 "21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program," regulations.gov website, accessed October 30, 2019, https://www.regulations.gov/document?D=HHS-ONC-2019-0002-0001.

3 "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," federalregister.gov website, accessed October 30, 2019, https://www.federalregister.gov/documents/2019/03/04/2019-02200/medicare-and-medicaid-programs-patient-protection-andaffordable-care-act-interoperability-and.

4 "Operating Rules" are defined by the ACA as "the necessary business rules and guidelines for electronic exchange of information specifications," CMS.gov website, accessed October 30, 2019, https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/Operating-Rules/OperatingRulesOverview.html.

5 Letter designating CAQH CORE as the operating rule authoring entity, CAQH CORE website, accessed October 30, 2019, https://www.caqh.org/sites/default/files/core/hhs-response-ton-cvhs-12122009.pdf.

6 CAQH CORE, "All Together Now: Applying the Lessons of Feefor-Service to Streamline Adoption of Value-Based Payments," CAQH CORE website, accessed October 30, 2019, https://www.caqh.org/core/value-based-payments.

7 CAQH CORE, "CAQH CORE Report on Attachments: A Bridge to a Fully Automated Future to Share Medical Documentation," CAQH CORE website, accessed October 30, 2019, https://www.caqh.org/sites/default/files/core/core-attachmentsenvironmental-scan-report.pdf?token=qLyOezlD.

8 HIMSS, "Interoperability in the Health Ecosystem," HIMSS.org website, accessed October 30, 2019, https://www.himss.org/library/interoperability-standards/what-is-interoperability.

9 CMS "Transactions Overview," CMS.gov website, accessed October 30, 2019, https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/Transactions/TransactionsOverview.html.

10 HIMSS, "What is Interoperability," HIMSS.org website, accessed October 30, 2019, https://www.himss.org/library/ interoperability-standards/what-is-interoperability.

11 "H.R.34 – 21st Century Cures Act," Congress.gov website, accessed October 30, 2019, https://www.congress.gov/bill/114th-congress/house-bill/34/text.

12 "21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program," regulations.gov website, accessed October 30, 2019, https://www.regulations.gov/document?D=HHS-ONC-2019-0002-0001.

13 "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," federalregister.gov website, accessed October 30, 2019, https://www.federalregister.gov/documents/2019/03/04/2019-02200/medicare-and-medicaid-programs-patient-protection-andaffordable-care-act-interoperability-and.

14 ONC "2019 Interoperability Standards Advisory," HealthIT.gov website, accessed October 30, 2019, https://www.healthit.gov/isa/sites/isa/files/inline-files/2019ISAReferenceEdition.pdf.

15 Jon Brodkin, "History of MIME," networkworld.com website, accessed October 30, 2019, https://www.networkworld.com/article/2199390/the-mime-guys--how-two-internet-guruschanged-e-mail-forever.html.

16 Zeus Kerravala, "What is Transport Layer Security (TLS)?" networkworld.com website, accessed October 30, 2019, https://www.networkworld.com/article/2303073/lan-wan-what-istransport-layer-security-protocol.html.

17 CAQH CORE, "Phase IV Health Care Services Review – Request for Review and Response (278) Infrastructure Rule", CAQH CORE website, accessed October 30, 2019, https://www.caqh.org/sites/default/files/core/phase-iv/452_278-infrastructurerule.pdf.

18 CAQH CORE, "CAQH CORE Phase V Operating Rules," CAQH CORE website, accessed October 30, 2019, https://www.caqh.org/core/caqh-core-phase-v-operating-rules.

19 CAQH CORE, "Phase IV Connectivity Rule," CAQH CORE website, accessed October 30, 2019, https://www.caqh.org/sites/default/files/core/phase-iv/470-connectivity-rule.pdf.

20 Oracle, "What Are RESTful Web Services?" github.io website, accessed November 5, 2019, https://javaee.github.io/tutorial/jaxrs001.html.

21 Tutorials Point, "SOAP – Message Structure," Tutorialspoint.com website, accessed November 5, 2019, https://www.tutorialspoint.com/soap/soap_message_structure.htm.

22 HL7, "RESTful API," HL7 FHIR website, accessed November 22, 2019, https://www.hl7.org/fhir/http.html.

23 HL7, "Resource Formats," HL7 FHIR website, accessed November 8, 2019, https://www.hl7.org/fhir/formats.html.

24 HL7, "SMART App Launch Framework," HL7 FHIR website, accessed October 30, 2019, http://hl7.org/fhir/smart-applaunch/.

25 The Office of the National Coordinator for Health Information Technology, "U.S. Core Data for Interoperability (USCDI)," healthit.gov website, accessed November 14, 2019, https://www.healthit.gov/isa/us-core-data-interoperability-uscdi.

Connect. Solve. Transform.℠

CAQH CORE℠

www.caqh.org | core@caqh.org