Where **Interoperability** Intersects with the Cloud

Breaking down data siloes to achieve
patient and business outcomes

ClearDATA
SECURE · HEALTHCARE · CLOUD

Where Interoperability Intersects with the Cloud

Table of Contents

It's no secret that interoperability is one of the biggest challenges hindering health IT effectiveness today. We're information rich, but beyond the four walls of our independent organizations, we're largely ineffective at optimizing the integration and application of the data we gather. There's a prevailing, legacy healthcare IT mindset dictating that data be protected, because possession equals control and control equals data security. But, a host of factors and forces affecting the dynamics of healthcare data usage and exchange is challenging this legacy approach, creating problems for healthcare providers on a number of fronts:

- As data volume swells, healthcare providers are realizing that the internal computing equipment, storage, IT staffing, and physical space investments necessary to accommodate growing volumes of electronic health records are cost prohibitive and unsustainable.

- Legacy and proprietary systems result in siloed, system and facility-specific patient data management, which creates a significant roadblock as we transition to the outcomes/value-based reimbursement structure central to the Affordable Care Act (ACA). To achieve the positive patient outcomes that will drive provider success in the immediate future, multiple and disparate providers and devices (hospitals, providers, urgent care centers specialists, at-home devices, etc.) must have clear visibility into standardized electronic health records. That's difficult and costly – if not impossible – to achieve in the current, largely siloed health data systems environment.

- On a larger scale, population health initiatives – which play an integral role in achieving the new standard of value-based patient outcomes – are encumbered by disparate data standards, and proprietary and legacy systems architectures.

- Healthcare remains the single largest expenditure and percentage of GDP, and it continues to grow at an unsustainable rate. And, even as healthcare costs rise in part

due to a lack of data interoperability and the inefficiencies created by that disparity, the quality of care in the U.S. has begun to lag other democratic and industrialized nations.

• Politics aside, the ACA and, more specifically, the Centers For Medicare and Medicaid Services (CMS) have provided the framework for an outcomes-based reimbursement model, investment in healthcare technology, and meaningful use (use of certified EHR technology to improve quality, safety, efficiency, and reduce health disparities). But, as meaningful use reaches its last stage, market dynamics will take over. Competition will increase and innovative providers will rise to the top. Interoperability – or a costly lack thereof – will play a determining role in the success or failure of the healthcare provider, and ultimately, the patient and consumer experience.

The issue of interoperability will determine whether or not the healthcare system can achieve its vision of creating a universal electronic health record that travels with the patient regardless of provider. While a single provider can be "interoperable" within its own enterprise, the whole ideology breaks down the instant that provider needs to exchange data outside its four walls with another provider and can't. It's not about success or failure of a single provider. It's about the success or failure of the entire system.

Findings from a 2014 National Health Information Exchange and Interoperability Landscape report underscore the value of health data interoperability. According to the report, 80 percent of healthcare providers reported that electronic data exchanges increase their practice's efficiency, and 89 percent of providers said electronic data exchanges improve the patient's quality of care. Those are important benchmarks on the road to interoperability, but HIEs aren't without fault. According to a recent ONC Privacy Security Survey referenced in the report:

• 1 in 3 individuals experienced at least one gap in health information in 2013. The most common of those gaps dealt with the sharing of medical histories among providers (18 percent) and the delivery of medical exams or tests to doctors and specialists (18 percent).

- Just 47 percent of physicians have the capability to incorporate structured lab results into EHR.

- Fewer than half of U.S. hospitals reported the routine electronic notification of a patient's primary care provider upon patient entry into their ER.

Clearly, while Meaningful Use Stage 1 (data capture and sharing) and Stage 2 (advance clinical processes) have paved a path toward improvement in EHR exchange and coordinated care, there remains a vast amount of room for interoperability improvement before Stage 3 (improved outcomes) will be achieved.

Improving Interoperability via The Cloud

Generally speaking, interoperability in healthcare is defined as the degree to which diverse systems and/or device components can successfully work together. IEEE and ISO define interoperability as the ability for two or more systems, devices, or applications to exchange, and mutually use, information.

In the context of cloud computing, interoperability is viewed as the capability of public clouds, private clouds, and other diverse healthcare systems to understand each other's application and service interfaces, configuration, forms of authentication and authorization, and data formats in order to cooperate and interoperate with each other.

In most cases, healthcare data – whether in text, note, number, image, formula, date, or other unstructured form – is being created faster than it can be processed. The cloud holds great potential as the medium by which this data can move and be exchanged; its proven proficiency at breaking down barriers to massive amounts of centralized, unstructured data – Big Data, if you will – makes it a data access and exchange enabler.

If we can break down data silos in a way that protects the privacy and security of each patient's data, business insight and improved health outcomes can be achieved more efficiently, and healthcare

executives can begin to explore use cases that have yet to be contemplated. In contrast, where data exists inside silos – in an on-premise physical environment that's not built to enable secure access and sharing, for example – providers have lost an opportunity to achieve patient outcomes, comply with current and dynamic standards, and compete on the innovation necessary to succeed in the new consumer-centric healthcare environment.

But simply porting data – whether clinical health data in an EHR, protected health information (PHI), or financial data in a financial management system – to the cloud and enjoying its benefits won't happen overnight. Due to competitive considerations and confidentiality risks, there must be a level of trust in the quality and security of the receiving organization's health data management systems for the data owner to be willing to share it. No one wants to risk a HIPAA privacy or security violation at the hands of another entity, whether a coordinated care provider or a third-party IT solutions vendor.

To a lesser degree, ubiquitous cloud interoperability in healthcare will also require further development and adoption of common data standards and protocols, and architectures. In simplest form, cloud integration is the process of configuring multiple application programs to share data in the cloud. In a network that incorporates cloud integration, diverse applications communicate either directly or through third-party software. The cloud still uses APIs (application program interfaces) and integration methods, it simply enables them to work in a common, scalable, and low-cost computing environment.

Speaking the Same Language

As application-to-application integration continues to evolve, common languages, interfaces and subsystems are showing signs of increased convergence. For example, FHIR (Fast Healthcare Interoperability Resources) is is the latest standard to be developed under the HL7 organization, combining the best features of HL7 V2, HL7 V3, and CDA (Clinical Document Architecture), while leveraging RESTful web services in a canonical data model (a design pattern used to communicate between different data formats).

In contrast to the majority of exchange profiles based on SOAP web services, RESTful web services enable basic HTTP operations including create, read, update and delete functionality. But, to extend these functions beyond the individual facility to the greater healthcare community, the healthcare providers and IT solutions providers that use these advanced protocols and architectures also need a purpose-built data environment that facilitates the approach. Proprietary ERP-like systems designed for use within a single organization's four walls are not that environment.

The cloud environment, on the other hand, offers the advantages of real-time, secure access to virtually any data format using highly elastic compute, bandwidth, and storage capacities that are based on the needs and demands of the use case. That architecture is perhaps best conveyed in diagram form:
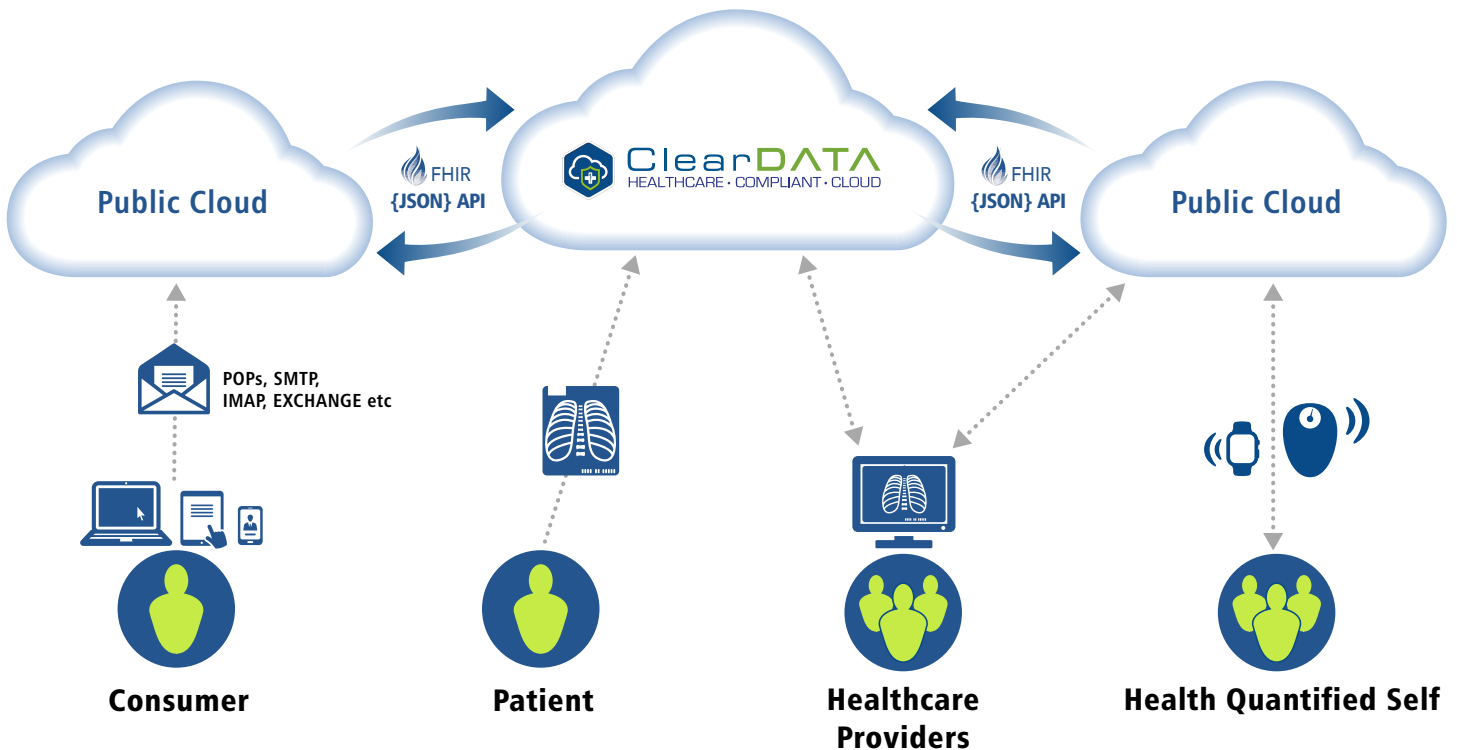
A similar architecture has been successfully adopted to accommodate information exchange in other data security intensive industries. In retail, for instance the PCI SSC (Payment Card Industry Security Standards Council) oversees retailers' efforts to manage payment card and personally identifiable information in the cloud, and real-time, unstructured customer, inventory, and human

resource data is exchanged with myriad enterprise, third-party, and partner systems in the cloud.

That parallel ends, however, where the stakes are concerned. In retail, the impact of interoperability is ultimately measured in sales dollars. Indeed, profitability is important in healthcare too – and the cloud enables it. But in the healthcare industry's new value-based care and reimbursement paradigm, the impact of interoperability is measured by a far more important metric. It's measured in patient outcomes.

Easing Cloud Security Concerns

Back in 2011, the Centers for Disease Control and Prevention reported that close to 41 percent of healthcare providers were using cloud computing in their practices and facilities. By 2012, MarketsandMarkets predicted that cloud computing would grow at a 20% rate in healthcare through 2017.

That growth is due, in part, to the shared liability that cloud healthcare computing providers must take on per the HIPAA BAA (Business Associate Agreement) Provision. According to HIPAA, a provider's "business associates" are defined as "a person or entity, other than a member of the workforce of a covered entity, who performs functions or activities on behalf of, or provides certain services to, a covered entity that involve access by the business associate to protected health information." That definition encompasses healthcare cloud computing providers, who become directly liable under HIPAA rules and are thus subject to civil, and in some cases criminal, penalties for making uses and disclosures of protected health information that are not authorized by contract or required by law.

As cloud healthcare IT providers demonstrate solutions that manage the security infrastructure in compliance with the HIPAA BAA Provision – by encrypting PHI in motion and at rest, for instance – provider concerns about the security of the cloud and its compliance with HIPAA standards are giving way to increased adoption of cloud computing. In fact, because modern cloud-based healthcare IT solutions are commonly more secure than legacy

systems, security and compliance have become as important an argument for the cloud as IT cost savings and decreased implementation time.

Healthcare data transfer and interoperability holds many great promises, business efficiency improvement and security compliance among them. Most importantly, it promises improvement in the coordination of patient care among healthcare providers, which has a direct impact on the quality of the care provided. As the value-based reimbursement model takes hold, that's never been more important than it is today.

About Us

ClearDATA is the nation's fastest growing healthcare cloud computing company. More than 310,000 healthcare professionals rely on ClearDATA's HIPAA compliant cloud computing HealthDATA platform and infrastructure to store, manage, protect and share their patient data and critical applications.

For more information

1600 W. Broadway Road, Tempe AZ

(800) 804-6052

www.cleardata.com

ClearDATA
SECURE · HEALTHCARE · CLOUD