Transforming Healthcare through API Governance

These days, digital information is gold. This is especially true in healthcare, where organizations strategically use health information to improve efficiency, reduce costs, and enhance the safety and quality of patient care. The American Health Information Management Association (AHIMA) defines information governance "as an organization-wide framework for managing information throughout its lifecycle and supporting the organization's strategy, operations, regulatory, legal, risk, and environmental requirements."

Information governance helps manage and control information by supporting the organization's activities and ensuring compliance with its duties. Information governance is what healthcare organizations need to not only tie together data from diverse departments, but to trust that the information is accurate, up-to-date, and privacy protected. This article will help to explain why Information Governance is an important component in connecting APIs to EHRs.

WHAT IS AN API?

Application Program Interfaces (APIs) help one application talk to another application. Why is this important? If the applications are sending data back and forth, you don't have to log into two systems to see overlapping information or, more importantly, document something twice. APIs are just a set of definitions and instructions that detail how to integrate with a system. As an example, think of a Spanish to English dictionary. You might need it to translate a document, but it isn't going to do the translation for you.

APIs act as bridges between two applications, allowing data to flow regardless of how each application was originally designed. For applications that function by pulling a constant stream of data from one or more sources, an API is especially important to decrease development time, save storage space on endpoint devices, and overcome any differences in the standards or programming languages used to create the data that lives at either end of the bridge.

API Governance

Governance of APIs can tie into several different categories including:

- Legacy Systems Governance
- Strategic Asset Management/Configuration Management
- Privacy and Security
- Quality Assurance
- Legal

Of course, all of these areas are interrelated and with governance processes, policies and procedures and oversight, APIs can improve interoperability, Let's look at each of these.

Legacy Systems Governance

Legacy systems create a myriad of challenges. First, they were not developed to support the implementation and adoption of modern technologies—whether it is mobile, cloud, or IoT, and

the number of digital transformation initiatives continue to grow. Moreover, existing legacy interfaces, developed in a world of daily batch calls, are not fit for purpose for today's real-time data needs. APIs hold the key to legacy modernization and, in turn, solving legacy system challenges. APIs expose data in a way that protects the integrity of legacy systems and enables secure and governed access to the underlying data. This allows organizations with older systems to adapt to modern business needs and, more importantly, quickly adopt new technologies and platforms. Nobody wants to keep creating new point-to-point code to endlessly keep up with new business objectives. So, organizations are now looking to address legacy system challenges and adopt new technologies for modernization in the long-term by adopting an integration strategy centered around reusable, purpose-built APIs.

Governance of APIs—Strategic Asset Management/ Configuration Management
Governance of APIs is an important component to ensure APIs are acquired, configured, implemented, and managed to decrease cost and improve patient care and outcomes. When purchasing or renewing contracts for EHRs and other Health IT projects, health care organizations should adopt common RFP language, specifying and requiring inclusion of a uniform healthcare API. Some examples of open standards include FHIR, OAuth2, OpenID Connect, RxNorm, SNOMED, and LOINC.

Ultimately, EHRs and other forms of digital health technology that can provide a highly usable App framework, enabling concurrent use of apps selected from a variety of "best of breed" sources will provide strong advantages not only in the marketplace, but to patients themselves. EHR vendors may begin to transform and retool their products into robust apps platforms to better support API calls with sub-second response times. Appropriate up-front due diligence and governance oversight will be necessary to ensure EHRs and APIs meet the needs of the stakeholders.

Standards are required for APIs to optimize interoperability and manage the flow of information between disparate systems. In the near future, software developers, public health agencies, payors, pharma, and startups may request access to health system data through common, open APIs, instead of through expensive and often untenable one-off integrations.

Governance of APIs—Privacy and Security
Standards for handling data privacy and security as well as rules for "good" app behavior will need to be developed as part of your governance of APIs. For example, an app should request the minimum dataset required to perform its function. And, in contrast to the vast majority of healthcare apps currently available for smart phones, clear and accurate privacy policies should be available to guide selection.

Standard agreements as part of your API governance plan should also be developed. Because the app may run on a computer outside the home institution housing the EHR, Health Insurance Portability and Accountability (HIPAA) business associate agreements (BAAs) may need to be in place between the App company and the clinical entity running the app.

Like any new technology, APIs provide opportunities that come with some risks. There are many concerns regarding APIs, from security to API vendor stability. There are fears that APIs may open new security vulnerabilities, with apps accessing patient records without receiving proper patient authorization. While access to health data via APIs does require additional considerations, privacy and security standards, and regulatory compliance needs, the truth is that if properly managed through your information governance program, the benefits by far outweigh the risks.

Governance of APIs—Quality Assurance

Data Quality and documentation guidelines must also be addressed for APIs. In a 2013 update to the 2007 guidance on EHR documentation integrity, a workgroup convened by the American Health Information Management Association (AHIMA) called for safeguards to ensure electronic documentation did not undermine patient care. According to the AHIMA workgroup, "Data quality and record integrity issues must be addressed now, before widespread deployment of health information exchange (HIE)." This also is necessary for EHR and API data exchange.

More recently, research has pointed to a potential disconnect between patient reported and provider recorded health data and this directly correlates to the potential disconnect in APIs. Researchers at the University of Michigan investigated whether patient-reported eye symptoms were recorded as part of clinical documentation in EHR systems. In comparing eye symptom questionnaires (ESQ) and EHR documentation, the researchers found a "substantial discrepancy" between the two. The study hypothesized that discordance in symptom reporting could be because of differences in terminology of symptoms between the patient and the clinician or errors of omission, such as forgetting or choosing not to report or record a symptom. The study also noted that "perhaps a more bothersome symptom is the focus of the clinical encounter, and other less onerous symptoms (e.g., glare) are not discussed (or documented). However, even for the exclusive sensitivity analysis, they show that the ESQ and the EMR are inconsistently documented." While discrepancies in patient- and provider-reported documentation were relatively harmless and did not directly impact patient safety, their existence does raise questions about data accuracy and completeness.

Governance of APIs—Legal

Governance of APIs must be considered from a legal perspective as well to ensure proper usage of corporate assets, especially when assets are being used by other businesses. Be prepared to answer:

- Who owns the data?
- Are all audiences entitled to access this data?
- What rights are you granting the consumer of the API to use the data provided?
- How will you communicate the terms of use to the API consumer?
- What is the required policy for data retention?
- What requirements do you have for attribution of the content or use of your brand? Do you need to give attribution to some other entity?
- How will you find out and deal with consumers who do not use the API appropriately?

- What are your liabilities?

Summary

APIs are the fastest growing, business-influencing technology in the IT industry today and the way we work and reach consumers/patients is evolving. We are seeing a fundamental shift from legacy systems and websites as being the information technology access mechanism for most organizations, to the rapidly growing ecosystem of interconnected devices that require APIs to improve business functions. Today, we have applications in cars, appliances, smartphones, game consoles, and other devices that communicate with back-end business functions through APIs and healthcare is one of the fastest growing industries embracing this new technology. Information governance is key to ensure APIs are integrated effectively in transforming our healthcare ecosystem to improve efficiency, reduce costs, and enhance the safety and quality of patient care.