AHLA

Health Care Organizations as Data Owners and the Intellectual Property Associated with Health Care IT Contracts

Executive Summary, December 2016

Sponsored by the Health Information and Technology Practice Group. Co-sponsored by the Business Law and Governance Practice Group.

AUTHORS

Amy Jo Davis

Lumeris/Essence Healthcare

Maryland Heights, MO

Seth M. Wolf

University Hospitals Health System Inc.

Beachwood, OH

There has been a tremendous increase in the amount of data captured, processed, stored, and analyzed by health care providers, payers, and accountable care organizations, especially after federal incentives for electronic health record adoption were initiated. Drivers for this trend include the increased capability and decreased cost, of IT infrastructure (bandwidth, processing power, storage, and the ability to share computing resources in order to flex up and down with need), as well as government stimulus through meaningful use payments and programs designed to foster interconnectivity and interoperability of health care data systems. Perhaps the largest driver is the need of healthcare organizations, both for internal analytics and for external reporting, for the type of actionable insights that can only be generated after large amounts of data from disparate sources are captured, normalized, parsed, and analyzed.

Advanced payment models, such as accountable care and bundled payment initiatives, are dependent upon successfully capturing and analyzing data to improve both quality and efficiency. Population-based efforts to improve health outcomes are likewise dependent upon the quality of data obtained from a given population, and the ability to process that data into useful insights and beneficial health interventions. Data can also be utilized to drive countless clinical interventions, ranging from prescribing medications most appropriate to a given patient's unique genome, to identifying patient-specific interventions likely to reduce the risk of hospital readmission or classifying a previously undiagnosed comorbidity. In developed countries, the future of health care will be guided by the development and application of new approaches to harness the power of health care data.

In order to assist health care organizations, numerous information technology vendors have developed innovative tools to capture, process, and use health care data. Some of these products function on a standalone and organization-specific basis, while others utilize the data of numerous health care sources, which can often be de-identified and combined to offer benchmarking, clinical decision support, or other useful evidence-based insights.

Amid this activity, many health care organizations are now asking basic questions about the data they generate and share with other entities and businesses:

- Does the data have intrinsic value separate and apart from any specific product or use? Should it be protected as a corporate asset in much the same way as undeveloped land or a raw material is protected? What elements of a health care IT product or platform would be considered a vendor's assets?
- In the context of contractual relationships, who owns the data? How is ownership of the data determined between health care providers, patients, health plans, etc.? Does ownership change as data is manipulated into new forms or new data is created that didn't previously exist? Who has the right to use data for particular purposes? Who exerts control over future uses?
- What actions and policies should health care organizations consider taking to protect themselves and maximize the value of their own data? What actions and positions will vendors advocate to protect the value of their products and services?

Should Data be Viewed as an Asset?

It is clear that vendors serving health care organizations ascribe significant value both to existing aggregations of data, as well as the opportunity to obtain access to more data in the future. For example, in connection with IBM's purchase of Truven for $2.6 billion, IBM focused on the data it was obtaining:

> "Upon completion of the acquisition, IBM's health cloud will house one of the world's largest and most diverse collections of health-related data, representing an aggregate of approximately 300 million patient lives acquired from three companies. IBM plans to integrate Truven's extensive cloud-based data set

spanning hundreds of different types of cost, claims, quality and outcomes information with its existing data sets."[1]

Most health care organizations are also familiar with the range of contracts that in one way or another require data contributors (often health care providers or health plans) to: (1) grant a license to a third party for the use of the data, and (2) often grant broader rights to the third party to utilize de-identified data. These include contracts in which a health plan partnered with a provider group can benchmark provider performance against a peer group; contracts in which a vendor facilitates the transfer of clinical information such as prescriptions; contracts for tools and services to calculate quality metrics and assist providers with achieving results under accountable care arrangements; and numerous other examples. In some cases, the consideration the provider group receives takes the form of free or reduced-cost use of the applicable software, rather than a direct payment.

From an economic perspective, a health care organization's data possesses the characteristics of an asset. A market does exist in which data is sold or exchanged, and in this market counterparties are willing to provide something of value in order to acquire it. Likewise, the derived data that health care IT vendors are able to create from the often non-standard and unstructured raw data of a health care organization possesses its own intrinsic value with market demand.

If data is viewed as an asset, the health care organization is nearly always the origination point in a series of transactions that affect that asset. This is because no health care IT company can create the raw data itself, as raw health care data is typically data created at the point of care by a health care practitioner or claims data sent to and processed by a payer. Raw data is data that a health care organization necessarily creates as part of its own operations concerning the care of its patients or members. Consider raw data concerning two different patients: (1) the first patient was discharged from the hospital to home with poorly-controlled blood sugar, and was

[1] IBM Press Release, February 18, 2016, *available at* https://www.03.ibm.com/press/us/en/pressrelease/49132.wss.

readmitted to the hospital three days later; while (2) the second patient was also discharged to home with poorly-controlled blood sugar, but had three home health visits from a nurse during the first week after discharge and was not readmitted to the hospital. This data, which could be aggregated with other data to generate insights about strategies to avoid readmissions, first exists only in the systems of the health care providers involved in the care of these patients (e.g., the electronic medical record (EMR) system utilized by the hospital and home health agency). The data cannot be created or inferred by an outside party. It is a raw material that can be processed into various useful things, and those secondary organizations that wish to do the processing must first acquire rights and access to the raw data.

On the other hand, as changes in health care delivery and management have taken hold, the use of “big data” in health care has ignited, and most sophisticated health care organizations are seeking ways to glean insights and develop care improvement techniques from raw data that was previously siloed in distinct systems. Health care IT companies have emerged to meet this need, and many have devoted substantial time and resources to developing proprietary tools and software that can transform disparate sources of raw data into a comprehensive view of patient information that often brings to light risk factors and other care opportunities that would previously have gone unnoticed. With respect to the data, the health care organization receives the benefit of receiving access to meaningful derived data, and the health care IT vendors receive the opportunity to further improving algorithms and pattern identification tools as the volume of source and reference data grows.

Given these developments, health care organizations should consider transactions in which their data will be shared to be, at least in part, like any other transaction in which the organization is selling or transferring rights to an asset. Data-specific transactions share the same high-level business considerations as any sale transaction: Is it a good deal? Does it make sense? Is there a better deal out there? In addition, health care organizations should be prepared for limitations on their rights to the data derivatives created by a health care IT vendor, as the proprietary mechanisms used to create these

derivatives are deemed highly valuable intellectual property in an increasingly competitive health care data industry.

How Might Health Care Organizations Protect This Asset?

Health care organizations are familiar with the need to institute physical controls to protect physical assets, such as an inventory of valuable pharmaceuticals. They are also familiar with the need to institute financial controls to protect financial assets, such as a series of validated approvals necessary to issue a check or initiate a wire transfer. If a provider's data should be viewed as a similar valuable asset, how should it be protected?

Controlling Approval Rights

In most organizations, there is a tiered structure used to determine what level of authority is needed to approve different contractual or financial transactions. A simple, low-value contract might be approved by a contracting agent, while the CEO or Board of Directors might need to approve a very significant transaction such as the purchase or sale of an entire facility.

As applied to the asset value of data, these approval mechanisms are often lacking. This is because it is rare to encounter a contract in which the provider is receiving outright payments in return for its data. Rather, it is most often the case that the provider's agreement to license its data to a vendor or other third party is ancillary (from the provider's perspective) to the primary purpose of the agreement. This situation may lead to the provider licensing or transferring enormous amounts of data without approval at the level within the provider's organization that corresponds to the value of the data.

Providers should consider creating or modifying their contracting policies for contracts in which the provider's data will be licensed or traded. The modifications would be provider-specific, but they should be considered, in part, based on the level of

sophistication required to analyze a transaction in which the provider's data will be transferred to a third party. Put another way, if every terabyte of data was instead viewed as $1 million sitting in a financial account, what level of authority would be required to move this asset to someone else?

Think Beyond Health Insurance Portability and Accountability Act (HIPAA) Issues

Health care providers understandably focus significant attention on HIPAA compliance. Likewise, nearly all vendors serving the healthmcare space have or should have a solid understanding of HIPAA and the particular obligations of business associates.

In the context of data and intellectual property ownership, HIPAA is less significant. At the point when a health care provider is transferring or licensing data to a third party for a use unrelated to specific patients, that data is most often de-identified in a manner that meets HIPAA's de-identification standard.[2] Upon de-identification in compliance with HIPAA, the de-identified data generally ceases to benefit from protection under HIPAA and such data typically ceases to be subject to the business associate agreement between the provider and the vendor. At the point of de-identification, the health care provider's interest in its data must be protected by other provisions in its contract, or it may have no protection at all.

Even when a business associate agreement continues to apply to data, a business associate agreement generally allows the information to be shared for the business associate's management and administration and for other HIPAA appropriate purposes such as treatment, payment, or health care operations. Under HIPAA, "healthcare operations" is defined broadly and includes data analysis to improve health and reduce costs.[3] For these reasons, the majority of health care IT vendor relationships will be permitted by HIPAA and any heightened restrictions on use, disclosure, or rights to the data will be beyond the scope of HIPAA's requirements.

[2] 45 C.F.R. 164.514.
[3] 45 C.F.R. 164.501.

It should be noted that HIPAA and state laws regarding identifiable health information often provide the individual (i.e., patient or health plan member) with an overarching right to access their information and prescribe limitations on the ways a health care organization may use and disclose their information. Any agreement contemplating the rights and limitations on another party's use of identifiable health information should ensure that these individual rights are not infringed upon.

De-Identified Data

Many general confidentiality provisions in contracts are insufficient to protect a provider's economic interest in de-identified data, and as mentioned above, de-identified data is not subject to HIPAA restrictions and typically not covered by a business associate agreement. Confidentiality provisions are typically written to protect information that a party to the agreement considers to have competitive significance such as pricing or business strategy, or information that might threaten an organization's reputation such as problems affecting patient care. As applied to de-identified data, which does not allow for the identification of the provider/payer or any particular patient, it is often the case that the general confidentiality provision is not written in a manner that clearly protects the health care organization's economic interests in that data. For example, consider a confidentiality provision that focuses on the protection of "Confidential Information," with that term defined as information relating to, "the businesses, operations, strategies, assets, facilities, finances, contractual relationships, activities or services of the disclosing party." Does this definition capture a pool of de-identified data that contains nothing identifying a party, and that is incapable of being associated with the party that generated it? An argument may be made that it does not, especially given the difficulty of identifying competitive or reputational harm that might occur if such data was disclosed. Further, even if the health care organization can state a viable claim that the vendor's use of de-identified data breaches a confidentiality provision, it may be difficult to obtain, or even quantify, damages in the context of asserting an interest in confidentiality, rather than in the economic value of the data.

The issue is further complicated by the fact that de-identified data is generally created by a health care IT vendor, who must meet one of the two stringent standards set forth under HIPAA in creating such data.[4] In addition, in an effort to limit access to protected health information (PHI) and the associated risks, many health care IT companies will seek to utilize de-identified data in software development environments as they test and develop new or improved capabilities. For this reason, many health care organizations may determine that allowing the vendor to create and use de-identified data is preferable to a wholesale prohibition, which may lead to the use of the organization's PHI when a lower risk option is available. As a common ground, many vendors will agree to include terms that prohibit the use of de-identified data for sale to a third party or otherwise restrict the vendor's ability to use de-identified data beyond its own internal purposes.

Intellectual Property Protection

Health care organizations concerned about protecting their data as assets should use contractual provisions that specifically protect those assets as intellectual property. Those provisions should be used in addition to standard provisions relating to privacy, security, and confidentiality. While the specific language in this area will vary from transaction to transaction, health care organizations should consider the following key areas when negotiating contracts involving a vendor's use of data:

- *A Stated Economic Interest*. The language of the contract should clearly assert that the provider considers its data to have independent economic value as an asset, regardless of whether the data is de-identified, aggregated with the data of other entities, or otherwise parsed or manipulated. This concept will often need to be carefully parsed out as health care IT vendors are protective of the proprietary architecture, logic, and algorithms used to

[4] 45 C.F.R. 164.514(a)-(b); To meet de-identification standards under HIPAA, organizations must either remove 18 listed identifiers from the ePHI ("Safe Harbor" method); or obtain confirmation from a qualified statistician that the risk of identification is very small (the "Expert Determination" method).

provide services to clients, and will typically not allow a client to acquire ownership rights or assert superior rights in the reports, tools, templates, or software that support or comprise an element of the deliverables to the client.

- *A Stated Intellectual Property Interest*. A health care organization will often assert that (1) the data is the intellectual property of the provider; (2) the provider reserves all copyright, trade secret, and other intellectual property rights arising from the data, including any derivative works to the extent applicable; and (3) the provider only licenses the data pursuant to express and limited licenses upon the payment of adequate consideration (for a non-vendor relationship). Most health care IT vendors will agree that, as between the health care organization and the vendor, the health care organization retains the rights to the raw data being provided to the vendor. However, as noted previously, a vendor will normally not be willing to grant broad proprietary rights in the derived data or other deliverables. For these reasons, vendors will often require limitations on the use of the product and/or deliverables (including all underlying systems and derived data) and will allow the client to use derived data or other deliverables for the client's internal purposes, but prohibit reverse engineering, disclosure to a competitor, or creation of a competing product for commercial exploitation.
- *Unauthorized Uses*. A health care organization may include contract provisions that clearly prohibit the counterparty from using the data for any purpose other than providing products or services to the contracting health care organization under the terms of the contract. This language may specifically reference prohibition on using the data on a de-identified, aggregated, or other basis unless the health care organization has expressly granted a license or other permission for such use. A health care IT vendor will seek to ensure that the contract allows the vendor to de-identify the data for internal uses or otherwise use the data in a way that may improve the functionality and services provided to the client, but may not be considered direct services on behalf of the client (e.g., software development, benchmarking activities, testing changes in functionality against a

representative dataset, measuring the outcomes of a process change to reports or data loads, etc.).

- *Exclusivity*. A health care organization should as a general matter avoid any agreement to provide data exclusively to one vendor. From the health care organization's perspective, exclusivity agreements tend to be very difficult to police, and may unexpectedly foreclose the ability to transition to other vendors or pursue future opportunities. Under a similar rationale, most vendors will not agree to exclusivity provisions that limit their ability to provide the services and tools to other health care organizations, and thus expand their client base.
- *Address The Possibility of Provider Identification*. HIPAA does not protect data that is de-identified with respect to patients, but identified with respect to the provider. For example, a list of the provider's 10 most productive physicians is not, by itself, subject to HIPAA protection. If the provider chooses to license or transfer its data, it may want to consider drafting the vendor's agreement to use the data only in a way that cannot identify the health care organization, its providers, or any of the providers' staff if the data is disclosed outside of the contracting vendor's business.
- *Unstructured v. Structured Data*. Raw health care data is often in an unstructured form, meaning it contains free text and non-standardized narratives such as discharge summaries or physician observations. The data derived from raw health care data and data utilizing preset fields is often considered structured data, such as a standardized field in a software application that can only contain a date of birth. The process of converting unstructured data into structured data that can be analyzed and presented to provide clinical decision support involves a complex process involving validating data integrity, cleansing the data to remove duplicates or outliers, matching data, and normalizing the data around common medical vocabularies and terminology maps. The process required to create high quality structured data that can be further analyzed and de-identified is both

labor and technology intensive, and these are the reasons many vendors place a high value on these services and deliverables.

Regarding de-identification concerns, structured data is easier to parse and facilitates the removal of individual identifiers, while unstructured data, such as a textbox or clinical or transcribed notes within an EMR, is more difficult to de-identify as it may contain free text information that could identify the patient, such as the phone number of a patient's family member. If a health care organization seeks to transfer unstructured data, the organization should consider how the vendor's de-identification process addresses concerns regarding unstructured data.

Protecting the Health Care Organization's Operations

Health care organizations contracting for the licensing or transfer of their data often fail to recognize that they are in the business of providing health care services, not information technology. This is often the reason the health care organization is procuring a third party to provide data and IT related services instead of utilizing internal IT capabilities. Until very recently, most health care organizations generally did not create, store, or use data planning to eventually license that health care data to a third party, and many still do not. The organization's data may be incomplete or contain inaccuracies. The provider's own information technology staff may not have the time or the ability to gather or provide the data in the manner required by a contract. The provider may suddenly face an urgent situation (such as responding to a ransomware attack, government investigation, security breach, or other unexpected event) that diverts the attention of its staff for an extended period of time. Health care organizations transferring data should consider including contract provisions that recognize these possibilities. Examples include:

- A clear statement that the health care organization's obligations to provide data are limited to the provider's own information technology resources as they change over time, as well as an acknowledgement that the contract will

not be construed so as to require the provider to incur material expense in modifying its systems or staffing in order to provide the data. The health care organization may also require agreement by the vendor that the organization may alter or suspend its provision of data to the extent that this is necessary in order to accommodate the organization's other needs as they change over time, or to respond to an urgent organization need such as a security breach. It should be noted that these protections will often prompt the vendor to include provisions that offer protection from a client's claims of non-performance or failure to meet agreed upon expectations in the event a client fails to provide required data on a timely basis and in the agreed upon format. If fees or other milestones are dependent on data exchange deadlines being met and appropriate client engagement, the vendor will require that a client's failure to meet its obligations will excuse non-performance and may even result in additional fees if the vendor must incur additional expenses to accommodate the changes.

- A disclaimer of the accuracy and completeness of the data, including a statement that the data should not be used in a manner that substitutes for the clinical decision making of the patient's providers. This provision may also include indemnity from the vendor in the event that a third party with which the vendor contracts later asserts a claim against the organization supplying the data. Likewise, a vendor will often include contract terms explicitly stating the vendor makes no warranty to and excludes liability for the accuracy and completeness of data (including derived data), and that authorize the vendor to rely upon the accuracy and completeness of the data supplied by the client in its performance of services. In addition, a health care IT vendor will often require that the client warrant that vendors' use of the data will not violate a third party's intellectual property rights or otherwise be in violation of any agreement the health care organization may have with a third party.