PLDW
HEALTH CARE

CLIENT ADVISORY:

MONETIZING HEALTH CARE DATA

Monetizing Health Care Data: Opportunities and Legal Concerns

Advances in technology have provided health care entities and their business associates with many exciting ways to monetize the health information they receive and store. While many entities could profit from a more thorough understanding of the ways in which health care data can be transformed into revenue, they must also be aware of the legal concerns created by these new opportunities.

A Range of Possibilities

Internal Use. Perhaps the easiest way to capitalize upon health care data is internally. For example, hospitals facing the increasing fiscal pressures of accountable and value-based care may use big data to identify deviations from operational or care-delivery standards. Institutions no longer have to rely upon the unpredictable presence of whistleblowers: variance from outcome norms can be the smoke that identifies the fires of best-practice deviations, which can in turn identify actionable intervention strategies. By turning big data into fast data, health care institutions can profit from lean and six sigma like never before.

Collaborative Use. Similarly, many providers and payors seek to monetize data collaboratively as they explore new models of integrated care delivery. Perhaps the most obvious model of collaborative monetization is that of the risk-bearing, multi-provider alliance sharing once-siloed patient records in an effort to reduce hospital admissions and keep patients in the less-costly home setting.

Transactional Use. Others seek to monetize data transactionally, either through direct sale or through exchange for something else of value. Payors or SaaS vendors who aggregate large amounts of patient data from many sources can aggregate and benchmark that data in very useful and profitable ways.

Criminal Use. Lastly, the headlines are increasingly rife with examples of individuals seeking to monetize data criminally. Hackers have turned to the health care industry in force as they've discovered that many health care entities simply do not have the sophisticated data security systems and protocols of the finance, banking, or even large retail industries. Most health care entities have still not grasped the reality that they are now essentially Information Technology companies whose downstream deliverable happens to be patient care. Further, every payor, provider or vendor that handles patient data shares one common but very real criminal threat: their own employees.

A Pyramid of Value

Like everything else in our market economy, data's value is a function of its marginal utility. The true value of data lies less in what it is than in what it can become.

As a rule, data, whether aggregated or integrated, is less valuable than analytics, which in turn is less valuable than prediction. As a simple example, a program that can identify the commonalities among high cost patients in a covered population is less valuable than one that can analyze the range of treatment regimens that might be effective.

Both are less valuable than one that can predict which regimens should be implemented on which patients at which times.

The Growth of Non-HIPAA Health Data

Data can be aggregated and utilized in ways unheard of just a short time ago. Historically, health care entities have viewed patient data in terms of the HIPAA privacy and security rules, with their definitions of "protected health information" produced by "covered entities" and sometimes shared with "business associates." Increasingly, however, patients' health-related information is not merely originated by covered entities (providers, payors, clearinghouses), but is also uploaded by individuals themselves into any number of digital health care applications.

The Future Lies in Sharing. Further, these applications increasingly allow that data to be shared. Apple, for example, has created HealthKit, which allows patients to upload personal health information into Apple's Health app, and then select other purpose-specific apps with which to share that information. While the traditional HIPAA-covered health care system struggles to overcome the inefficacies of decentralized medical records, the consumer-driven digital health ecosystem is moving rapidly toward openness and integration.

Utility May Beget Regulation. Of course, the innovation and openness of this new ecosystem creates many new legal concerns. A data management company that seeks to create value by moving up the "data-analytics-prediction" chain may create an application that delivers so much useful information to the consumer that it suddenly qualifies as a medical device, subject to FDA approval and oversight.

Further, the legal threshold at which this metamorphosis happens is not exactly what lawyers refer to as a "bright line." A wearable device that tells an office worker to get up and walk around every once in a while may receive very different treatment from one that uses real time biometric information to tell a person that they should take another dose of blood pressure medication and call their physician as soon as possible.

Dangers of Unexpected Use. Data that consumers understand to be collected for one purpose but which is also sold or used for another, unexpected purpose could subject the vendor to liability under FTC regulations and/or state laws barring unfair and deceptive trade practices. App developers seeking to find new revenue streams from the valuable health information they've amassed should not simply assume that they have carte blanche to use the information in whatever manner they see fit. Instead, they should anticipate the various categories of use by which they may seek to monetize that data, and ensure that their customers' initial use agreements authorize such additional use.

Privacy Outside of HIPAA. No discussion of the openness and sharing inherent in the consumer-generated health information ecosystem would be complete without a warning about privacy. It is now settled that a vendor's failure to deliver upon its claims of privacy or information security can qualify as an unfair or deceptive act under FTC regulations. Additionally, many states like Massachusetts have robust unfair and deceptive trade practice laws, which they enforce expansively and which may also apply to failures of a vendor's stated claims of information security.

Additionally, the FTC's Health Breach Notification Rule applies to web-based businesses that allow individuals to maintain medical information online. Like the HIPAA Breach Notification Rule, it requires companies that experience a security breach to notify all affected individuals and potentially the media, as well as the FTC directly.

Thus, even if the health data at issue is generated by the consumer and not governed by HIPAA, both state and federal law may be still implicated by a failure to maintain that data's security.

Monetizing HIPAA-Covered Health Data

The rise of consumer-generated health information provides physicians and other providers with new and potentially-useful means of diagnosing and treating their patients. However, for most providers, payors and business associates, the legal concerns surrounding the monetization of health care data will continue to arise under HIPAA and its state-law counterparts. Of note, once any consumer-generated info is brought into a covered entity's medical record system, the info in that record becomes subject to HIPAA's restrictions on access, use and disclosure.

What HIPAA Protects. To the surprise of many, HIPAA does not protect mere medical information. A stack of medical histories or MRI images left on the subway would not violate HIPAA if the patients involved could not be identified. What HIPAA protects is information that does or reasonably could identify the individual. Thus, PHI would include name, address, social security number, or even "the 104-year old woman in the ICU." Such individually-identifying information is referred to as Protected Health Information, or "PHI."

HIPAA violations carry the potential for fines of up to $1.5 million per year. Any entity seeking to monetize patient information generated by a HIPAA-covered entity must understand its rights to use and disclose that information. Also, entities increasingly find themselves paying significant fines under state law. While many state privacy laws track HIPAA closely, most states also have additional laws protecting HIV status, mental health and/or substance abuse, and genetic information.

Ownership. A question of more than passing importance concerns who owns the PHI that the law protects. There are only two ways by which an entity can legally monetize PHI: by the right of ownership or, in the alternative, by express grant from the actual owner. As regards the monetization of PHI, we will see that this legal distinction does indeed make a difference.

Typically, patient data belongs to the covered entity (provider, payor or clearinghouse) in whose record system the data resides. While the patient may have a right to access and receive a copy of that info, a patient's medical record belongs to the covered entity.

Transfers between covered entities give ownership to both covered entities. Accordingly, when an ancillary service provider treats a patient and forwards a copy of the treatment record to the patient's primary care physician, both the ancillary provider and the physician own their copies of that treatment record. The same is true for data transfers among providers, clearinghouses and payors.

By contrast, a transfer to a business associate generally does not give the business associate a right of ownership. Thus, it is important to understand the status in which an entity receives PHI: as a covered entity or as a business associate.

Under HIPAA, the right of a business associate to use PHI that it receives from a covered entity is limited to the purpose for which the business associate receives the information. Any additional use of the information must be made explicit in the parties' HIPAA-compliant business associate agreement, and may not include any access, use or disclosure from which the covered entity itself is precluded.

However, this rule is complicated by the special nature of certain business associates. HIPAA allows covered entities to be business associates of other covered entities. Further, one covered entity can receive PHI from a second covered entity when the first entity is acting both as a covered entity and as a business associate to that second entity. For example, a clearinghouse may receive PHI from physicians that it transmits to payors in its role as a covered entity, while also using that information to provide benchmarking or predictive analytics for those physicians as a business associate.

In such a case, numerous questions can surface. Are a clearinghouse's exemptions from HIPAA's normal notice and accounting requirements still valid if the clearinghouse also uses the info in its role as a business associate? In case of a reportable breach of information a covered entity received from another covered entity to which it is a business associate, must the breaching entity notify the affected individuals directly, or may it merely notify the originating covered entity? Being able to delineate the capacity in which an organization received information that was potentially breached, and the manner in which the breach occurred, can have important legal consequences.

Authorized Use. HIPAA generally requires patient authorization to access, use or disclose PHI. While the law does give broad authority to covered entities for the purposes of payment, treatment and health care operations, the sale or other commercial exchange of PHI generally requires written authorization of the patient.

Is De-Identification a "Use"? De-identified information is not PHI, so long as the information cannot reasonably be re-identified. If PHI is stripped of 18 specific individual identifiers (e.g., name, address, date of birth), it can be used under a statutory safe harbor, provided there is no basis to conclude that it can be re-identified.

As stated above, HIPAA does not restrict the use of all patient data, merely the type of individually-identifiable data that constitutes PHI. Thus, entities should keep a simple rule in mind. While the external monetization of actual PHI will likely require written patient consent, the sale or exchange of de-identified data has far fewer restrictions.

This leads to an interesting question: does creating a de-identified data set from PHI qualify as a HIPAA-governed "use" of that PHI? The answer is "yes," it does. The good news, however, is that HIPAA explicitly permits a covered entity to use PHI to create de-identified data, or to disclose PHI to a business associate for such purpose. Further, the law allows a covered entity to let a business associate de-identify PHI, even if the covered entity isn't going to use the de-identified info. Thus, a business associate can create a de-identified data set from PHI it receives from a covered entity.

Monetization by Business Associates. However, there is one catch. As noted above, a business associate does not own the data: it may only access, use or disclose PHI according to the terms of the parties' business associate agreement, and in accordance with their underlying contract and the law. Thus, business associates should be on notice that they are not at complete liberty to create and monetize de-identified data sets from PHI received by their covered entity partners. Unless they have also received the information in their role as a covered entity, business associates cannot create and monetize data sets without the written authorization of the covered entity in the parties' business associate agreement, or in an amendment thereto.

At this juncture, the importance of a well-crafted business associate agreement should be coming into clear focus. Business associate agreements are not generic, but must be tailored to each relationship, to the parties' anticipated use of the data at issue, and to ways by which both parties may wish to monetize the data in the future.

Transferring Value, Not Just Data

As never before, patient information represents a store of value that technology has the ability to unearth. However, entities should have a clear understanding of their rights to use that information, and of the risks of misuse. Further, they should also understand not only the value such rights contain, but the value that is potentially transferred to others as patient information they create is passed to others in our increasingly-integrated health care infrastructure.

JOEL K. GOLOSKIE
Of Counsel

Joel K. Goloskie is Of Counsel with Pannone Lopes Devereaux & West LLC and a member of the Health Care, Litigation, and Corporate & Business Teams. His experience ranges from compliance and HIPAA privacy matters to regulatory filings and approvals, contract drafting and management, and mergers and acquisitions. He has assisted health care clients as they dealt with compliance orders and deferred prosecution agreements, and has represented clients in both civil and criminal matters in federal court.

PLDW
PANNONE LOPES DEVEREAUX & WEST LLC
counselors at law

317 Iron Horse Way, Suite 301 Providence, RI 02908
tel 401 824 5100 • fax 401 824 5123