EPSTEIN BECKER GREEN

Health Law Advisor

Thought Leaders on Laws and Regulations Affecting Health Care and Life Sciences

Free the Data! ... Better Think Twice ... Legal Issues Regarding Data Sharing and Secondary Data Use

By Patricia Wagner & Alaap Shah on February 4, 2019

Data is king! A robust privacy, security and data governance approach to data management can position an organization to avoid pitfalls and maximize value from its data strategy. In fact, some of the largest market cap firms have successfully harnessed the power of data for quite some time. To illustrate this point, the Economist boldly published an article entitled "**The world's most valuable resource is no longer oil, but data**." This makes complete sense when research shows that **90% of all data today was created in the last**

two years, which translates to approximately 2.5 quintillion bytes of data per day.

This same trend has taken hold in the healthcare industry as it seeks to rapidly digitize and learn from data in order to bend the cost curve down, increase quality of outcomes, and improve overall population health. Specifically, there is certainly an ever-growing pool of health data being generated by providers, payors, life sciences companies, digital health companies, diagnostic companies, laboratories, and a cornucopia of other entities. Recent estimates indicate that volume of healthcare data is growing rapidly as evidenced by **153 exabytes produced in 2013 and an estimated that 2,314 exabytes will be produced in 2020**. This translates to an overall rate of increase at least 48 percent annually. But, to what end?

The rapid production and aggregation of data is being met with increasing demand to access and analyze this data for a variety of purposes. Life sciences companies want access to conduct pre-market analysis, clinical trials and post-market surveillance. Providers want access to conduct population health research. AdTech and marketing companies want it to . . . you guessed it . . . sell more things. These examples are just the tip of the proverbial iceberg when it comes to the secondary data analytics market.

Nevertheless, there are various issues that must be addressed before aggregating, sharing, and using such data.

First and foremost, identifiable health data is typically treated as a sensitive class of information warranting protection. As such, entities should consider whether their intended activities must comply with applicable privacy and security regulations. Depending on the data being collected, the use and disclosure of such data, and the jurisdictions within which data is stored and processed, entities may be subject a wide array of legal obligations, including one or more of the following:

- Health Insurance Portability and Accountability Act of 1996 ("HIPAA")
- the Common Rule
- the EU General Data Protection Regulation ("GDPR")
- 42 C.F.R. Part 2

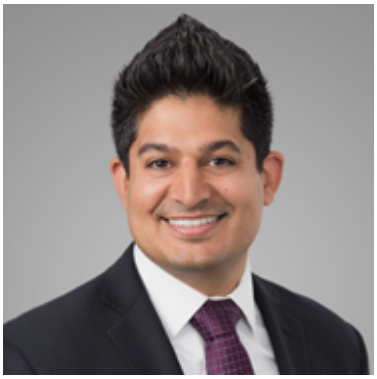
- State data protection and breach laws and regulations
- Food and Drug Administration ("FDA") regulations; or
- Federal Trade Commission ("FTC") regulation.

Second, entities must consider contractual obligations, including property rights governing data collection, aggregation, use, and disclosure. The contractual obligations that should be evaluated will depend largely on the nature of the data collected, contemplated uses and disclosures of such data and the applicable laws and regulations relative to such collection, use and disclosure. Accordingly, entities should also consider the impact of upstream agreements and downstream agreements on rights to collect, use or disclosure data through the chain of custody. Agreements that warrant considering may include:

- Master Services Agreements
- Data Use Agreements
- Business Associate Agreements
- Data Sharing Agreements
- Confidentiality/Non-disclosure Agreements
- Terms of Use/Privacy Policies (and other representations made to consumers).

Third, even if collection, aggregation and analysis is possible under law/regulation and contract, companies must still consider whether additional data governance principles should be implemented to guide responsible data stewardship. It is critical to remember that businesses that mishandle personal data can lose the trust of customers and suffer irreparable reputational harm. To mitigate against such issues, entities should consider developing data governance principles guided by **fair information practices** including: openness/transparency, collection limitation, data quality, purpose specification/use limitation, accountability, individual participation and data security.

Patricia M. Wagner



Alaap B. Shah

Health Law Advisor

EPSTEIN BECKER GREEN