KIRKLAND & ELLIS

KirklandPEN

HIPAA: Big Data, Big Issues

21 May 2019

Healthcare data has assumed an increasingly valuable role in healthcare targets, ranging from traditional providers to cutting-edge health IT platforms. Below are some important trends and developments related to healthcare data for a potential private equity investor considering a healthcare target.

De-identification

As the disruptive effects of artificial intelligence ("AI") continue to pervade the healthcare industry, it is becoming increasingly important to leverage patient-specific information. However, much of this information is considered "protected health information" (“PHI”) under the Health Insurance Portability and Accountability Act of 1996, commonly referred to as "HIPAA." HIPAA generally restricts the use and disclosure of this information, including to companies creating cutting-edge machine learning technologies.

Fortunately, de-identification, if performed correctly, can eliminate these requirements and allow data holders to license the de-identified data or use it for their own development. This process is easier said than done. Proper de-identification takes significant resources and expertise, and failures can result in reportable data breaches that are expensive to a firm’s bottom line and its reputation. The situation is even trickier for IT platforms and other companies that access or store PHI on behalf of healthcare providers and other so-called “covered entities.” HIPAA requires that these IT platforms — referred to in HIPAA as “business associates” — have the covered entities' written permission to de-identify. Failure to obtain such permission can effectively lock up a valuable data source. It is therefore important for private equity investors to conduct thorough due diligence on these matters when pursuing healthcare targets if there is a desire to monetize or otherwise use the target’s accumulated data.

Amazon Announces HIPAA Eligible Skills for Alexa

Last month, Amazon announced six new Alexa skills from various healthcare providers, including payors, pharmacy benefit managers and digital health companies. These Alexa skills are unique in that they are operating in what Amazon calls its new "HIPAA eligible" environment. While Amazon's cloud service subsidiary, Amazon Web Services, has been signing business associate agreements for years, Amazon itself has not. In practice, this means that Amazon has implemented a HIPAA compliance program that enables it to perform activities on behalf of providers and other HIPAA-regulated entities that require access to protected health information. For example, Livongo, a consumer digital health company, is releasing a skill that will allow individuals to ask Alexa for their blood sugar readings and trends, as well as for personalized health nudges.

Amazon's entry into this space is important for a number of reasons, not least of which is that it gives digital health companies and other healthcare providers a means of interacting with the millions of individuals that use Alexa. Amazon's deeper push into digital health is also intriguing in light of its recent acquisition of online pharmacy PillPack, and its announcement earlier this year that it will partner with J.P. Morgan and Berkshire Hathaway to create Haven, a joint venture aimed at improving healthcare for the companies' 1.2 million combined employees. The full extent to which Amazon's healthcare activities might have knock-on effects on potential healthcare targets remains to be seen.

Enforcement

The healthcare targets of PE investors continue to operate in a heavily regulated environment that is subject to significant enforcement, including increasingly in healthcare privacy. Healthcare providers are facing steep fines over their failure to comply with HIPAA. Earlier this month, a Tennessee-based diagnostic medical imaging services company paid $3,000,000 to settle a breach that exposed over 300,000 patients' protected health information. The provider was notified by the FBI and federal privacy regulators that one of its FTP servers storing protected health information was accessible by search engines. The investigation also found that the provider failed to:

(i) investigate the security incident until several months after noticing it;
(ii) conduct an accurate risk assessment; and

(iii) have business associate agreements in place with vendors, including IT support vendors and third-party data centers.

This enforcement action highlights the importance of conducting thorough healthcare regulatory due diligence on transactions involving healthcare targets to avoid facing potentially large settlement fines as well as costs related to breach mitigation and notification.

Authors

Dennis Williams

Partner / New York

Chad D. Ehrenkranz

Partner / New York

Jordan T. Cohen

Associate / New York

Phillip V. DeFedele

Associate / New York

Related Services

Practices

- Private Equity
- Transactional

Suggested Reading

- 20 May 2019 Press Release Kirkland Counsels Red Wolf Natural Resources on Acquisition of Oil & Gas Assets in the Anadarko Basin
- 20 May 2019 Video Public Takeovers

- 17 May 2019 Press Release Kirkland Represents Marlin Equity Partners in Strategic Minority Investment by Blackstone