wiley

NEWSLETTER

New Litigation Brings De-Identification of Health Care Information Back Into the Spotlight

August 2019

Privacy in Focus®

Significant advances in technology have resulted in the development of an increasing number of connected medical devices, software applications, and online health systems. However, these innovations have raised new and challenging questions about the protection of health information by, among others, health care providers, health plans, and technology companies handling health information.

Dinerstein v. Google

On June 26, 2019, a proposed class action – *Dinerstein v. Google, the University of Chicago Medical Center, and the University of Chicago*, Civil Action No. 1:19-CV-04311 – was filed in the U.S. District Court for the Northern District of Illinois. In the complaint, the plaintiff alleges that the University of Chicago Medical Center, in contravention of HIPAA, unlawfully shared the Electronic Health Record (EHR) of "nearly every patient from the University of Chicago Medical Center from 2009 to 2016." These records, according to the plaintiff, were shared without patient authorization to assist Google in designing its own proprietary and commercial EHR system.

The University has denied the claims through a spokesperson, as a responsive pleading has not yet been filed. According to the spokesperson: "The Medical Center entered into a research partnership with Google as part of the Medical Center's continuing efforts to improve the lives of its patients. That research partnership was appropriate and legal, and the claims asserted in this case are

Authors

Antonio J. Reynolds
Partner
202.719.4603
areynolds@wiley.law

Dorthula H. Powell-Woodson
Partner
202.719.7150
dpowell-woodson@wiley.law

Boyd Garriott
Associate
202.719.4487
bgarriott@wiley.law

Practice Areas

Health Care

Privacy, Cyber & Data Governance

baseless and a disservice to the Medical Center's fundamental mission of improving the lives of its patients."

De-Identification Requirements Under HIPAA

Under HIPAA, health care providers and other covered entities generally may not disclose EHRs to third parties for commercial purposes without written patient authorization. They may, however, use or disclose the information without authorization if the information is "de-identified." At the heart of the dispute between plaintiff and defendants is de-identification and what steps must be taken to reasonably de-identify health information that is furnished to third parties.

HIPAA's long-standing de-identification standard provides two methods of de-identification that are sufficient for compliance with the statute. U.S. Department of Health and Human Services (HHS) guidance calls them the "expert determination" method and the "safe harbor" method. *First*, the "expert determination" method provides that an expert statistician may certify that the risk of *re*-identification is "very small" for a given data set.

Second, the "safe harbor" method is applicable if a provider removes 18 enumerated identifiers, including "names," "email addresses," "Social Security numbers," and others. The wrinkle, however, is that removal of the 18 identifiers is insufficient if one has "actual knowledge that the information could be used alone or in conjunction with other information to identify an individual who is a subject of the information."

In addition to the two de-identification methods above, HIPAA rules also provide for the sharing of a "limited data set ... only for the purposes of research, public health, or health care operations." This rule allows for the sharing of health data with *some* direct identifiers – but still precludes sharing names, Social Security numbers, etc. – in tandem with a "data use agreement" that requires, among other things, specific and limited use of the data and "appropriate safeguards" to prevent use or disclosure of such data. Finally, this method requires the disclosing party to take "reasonable steps to cure" if it becomes aware that the recipient is in violation of the data use agreement.

Looking Forward

The exception to the safe harbor – where information could be used "in conjunction with other information" to re-identify an individual – presents a thorny issue in the world of big data. As the *Dinerstein* plaintiff put it: "Google has access to nearly unlimited information capable of re-identifying medical records." If that is true – and only time will tell if it is – the exception could swallow the rule, as there is an argument to be made that big technology companies have the capability to re-identify most "de-identified" data by using troves of complex consumer profiles in tandem with advanced machine learning.

These kinds of issues were probably not on HHS' radar when it promulgated its de-identification standard nearly a decade ago. But they are a reality now. As a result, the question increasingly becomes how a company will credibly maintain that it does not have "actual knowledge" that de-identified information it provides a tech company could be re-identified. Simply complying with the "safe harbor" might not be enough, and additional contractual commitments beyond HIPAA may become warranted.