PROJECT NIGHTINGALE AND THE TAKE-AWAY LESSON FOR PROVIDERS AND PAYORS

There has been much ado lately about a newly-revealed joint venture between Ascension Medical Group and Google. Ascension is the nation's largest non-profit health care system; Ascension Medical Group is the company's subsidiary physician group, with facilities in more than twenty states. Google is, well, Google.

The joint venture being undertaken by these industry behemoths is known as "Project Nightingale." Ascension and Google describe Nightingale as a treatment-focused initiative, designed to facilitate access and use of data in the medical records of Ascension's patients. It also involves migrating Ascension's data from proprietary storage to Google's cloud-based storage. The software tool developed from this initiative allegedly makes it easier for a doctor to access and use specific patient data such as recent test results, medications, and more.

Such "treatment" focused use of PHI is of a type generally permitted by Subpart E of HIPAA, which governs permissible uses and disclosures by covered entities and business associates. Further, there is a colorable argument that this tool could support quality improvement activities, which would also bring it under the aegis of HIPAA's carve-out for "health care operations." Thus, the development and use by a provider of a software tool that facilitates treatment and quality improvement would be a permissible use of a provider's protected health information ("PHI").

Such an initiative also seems to be squarely of the type that HIPAA would permit to be undertaken by a provider's "business associate." The two companies assert that they have signed a business associate agreement ("BAA"), and also assert that the terms of the agreement prohibit Google from using Ascension's PHI for any other purpose than for provisioning this tool for use by Ascension clinicians. Further, the BAA allegedly prohibits Google from combining Ascension's patient data with Google consumer data.

There have been reports that a whistleblower who claims first-hand knowledge has expressed concerns that patients' medical records are being shared without their consent. However, the development and use of a software tool designed to facilitate physicians' access to and use of patients' PHI is not something that HIPAA would require a provider to obtain patient consent to undertake. Similarly, outsourcing such an initiative to a business associate would also not require patient consent.

Nonetheless, Nightingale is now under scrutiny from the HHS Office of Civil Rights ("OCR"), the office charged with enforcing HIPAA. "OCR would like to learn more information about this mass collection of individuals' medical records with respect to the implications for patient privacy under HIPAA," Roger Severino, OCR's director, said in a statement recently.

It may well be that the companies' description of Nightingale does not adequately describe the true value-add of the initiative, either to Ascension or to Google. After all, Ascension utilizes industry-leader Cerner as its electronic medical records platform provider. If all that Ascension really sought was migration to a cloud-based platform, it seems that Cerner might have been happy to oblige. If Ascension was merely seeking improvements to its providers' ability to access data in its Cerner EMR system, why wouldn't it have just had Cerner make these improvements? Google isn't in the business of creating plug-and-play upgrades to EMR platforms. Maybe all that Ascension truly wants is for Google to patch gaps in Ascension's ability to call up data in its industry-leading EMR platform. Far more likely, however, is that the long-term goal of Nightingale is to enable Google to use its analytical powers to draw actionable insights from the data it is receiving.

One can hardly read a health care trade journal without coming across yet another study showing that the leading cause of today's unprecedented level of physician burnout is the EMR. Physicians are simply overwhelmed with data. The problem with today's industry-leading EMR systems is not that providers can't access enough data. Quite to the contrary. What they need are tools that will cull and present the most relevant and actionable data, in a self-generating way that will meet the time constraints of the physician's typical seven-minute patient encounter. This is the purview and the promise of Big Data.

Like all other massive data platforms, Google is increasingly in the business of drawing actionable insights from data. Big data, to be specific. Data of the magnitude held by the nation's largest non-profit healthcare system. Ascension and Google assert that Nightingale complies with HIPAA. While the parties claim that Google cannot use the PHI for any other purpose, or to combine it with other Google data, those things aren't necessary for this data to be of immense value to Google. A HIPAA-compliant BAA could allow Google to create and use de-identified health information from the millions of records it is receiving from Ascension. Even as a stand-alone data lake, deidentified health information of that scale would hold tremendous analytic and predictive value. Further, the de-identified data Google could create would likely not be subject to the parties' prohibition against combining Ascension's PHI with other Google data.

So, why has Nightingale received such a storm of whistleblower complaints, public backlash, and regulatory scrutiny? Again, the companies assert that Google is not permitted to pool Ascension's patient data with any other data Google possesses, or even to make any other use of this data. It is not like some Ascension patient going about an unrelated Google search will suddenly find himself being subject to pop-up ads for incontinence supplies based on a recent entry in his Ascension EMR. (In truth, he likely gets these ads already, based upon his online searches and purchases.)

The simplest answer? The backlash is because it's Google.

For data platforms, a lack or loss of trust is one of the key determinants of failure.[1] Trust in Facebook fell fully 66% after the Cambridge Analytica scandal.[2] About 40 percent of digitally connected people worldwide said they had deleted at least one of their social media accounts in the past year because they didn't trust that the platform would properly handle personal information.[3] Google, too, continues to have issues of public trust.[4]

It may well be that trust in the large platforms like Google and Facebook is now so so badly broken that the public will lash out against providers and payors who share their medical records and claims data with these platforms. In a health care market like Boston, for example, where each competing health system is perceived as being world-class, a successful marketing campaign might turn on advertising built around the simple, differentiating message: "We don't share your data with Google or Facebook."

If Nightingale had been a joint project between Ascension and Cerner, not a single journalistic keystroke would have been expended on it. If Ascension had announced that it was engaging one of the large healthcare-specific data platforms like Inovalon, Optum, or Premier to help it develop algorithms to identify test-results with heightened probability of clinical relevance based upon each patient's overall medical history, any press coverage would likely have been limited to the healthcare and information management trade journals, and would likely have heralded this as yet another advance in the ability of data to enhance delivery and reduce cost. There would be no whistleblowers, no public backlash, no OCR investigation.

For health care providers and payors, this may be the only thing they need to know about Project Nightingale. If you would like further information, please contact PLDO Attorney Joel K. Goloskie at 401-824-5100 or email jgoloskie@pldolaw.com.

[1] David B. Yoffie, Annabelle Gawer, Michael A. Cusumano, Social Platforms - A Study of More Than 250 Platforms Reveals Why Most Fail, Harvard Business Review, May 29, 2019 (avail. at: https://hbr.org/2019/05/a-study-of-more-than-250-platforms-reveals-why-most-fail).

[2] Herb Weisbaum, Trust in Facebook has dropped by 66 percent since the Cambridge Analytica scandal, NBCNews.com, Apr. 18, 2018 (avail. at: https://www.nbcnews.com/business/consumer/trust-facebook-has-dropped-51-percent-cambridge-analytica-scandal-n867011).

[3] Kesley Sutton, Trust in Social Media Platforms Is Eroding—and Brands Have a Lot to Lose, AdWeek.com, June 18, 2018 (avail. at: https://www.adweek.com/digital/trust-in-social-media-platforms-is-eroding-and-brands-have-a-lot-to-lose/).

[4] Owen Williams, Google Promises 'reCAPTCHA' Isn't Exploiting Users. Should You Trust It?, One Zero, July 9, 2019 (avail. at: https://onezero.medium.com/google-promises-recaptcha-isn-t-exploiting-users-should-you-trust-it-ed99f1543f28); Matthew Green, Why I'm Worried About Google, Slate.com, Oct. 30, 2018 (avail. at: https://slate.com/technology/2018/10/google-is-losing-users-trust.html).

Joel K. Goloskie
Senior Counsel

PANNONE LOPES
DEVEREAUX & O'GARA LLC
counselors at law