Commercial Online Health Data Research

Continued from page 11

based on search history, who gets the information?" Santillana said. "The benefit could be great, but the implementation is not clear."

He emphasized that he supports industry-academic partnerships provided the goals are very clearly outlined.

"I'm a big supporter of innovation and a big supporter of partnering with industry with the understanding that the goal is to improve social good and patient-centered care," he said.

There are also questions about oversight of search-data–based research. In traditional biomedical studies, academic scientists and medical professionals at universities must get approval from institutional review boards (IRBs) (Vayena E, et al. *Am J Public Health* 2012; 102:2225–2230). Corporations may have less strict review processes, said Buchanan.

For population-level or aggregate data research, such as that done by Santillana's group, IRB approval is not required even at academic institutions.

Government oversight of such research is limited. The Department of Health and Human Services' Office of Human Research Protections (OHRP) has published non-binding recommendations about online health data research, which Buchanan co-authored. The recommendations call on researchers to be sensitive to the unique privacy and security concerns associated with online health data.

The US Department of Health and Human Services National Coordinator for Health Information Technology has issued recommendations for "Big Data" health research that call for more transparency about the computer algorithms used to collect and analyze health data online. The recommendations also call for policies to protect online health data that would fall outside of the Health Insurance Portability and Accountability Act (HIPAA).

The European Union (EU) has been ahead of the curve in regulating the use of search data (http://ec.europa.eu/justice/data-protection/) and ensuring that the public is informed, Santillana said. For example, on a recent trip to England he searched for information about fevers on Google and immediately received a notification that his information could be used for research purposes, and was given the option of saying yes or no to that use of his data.

"The EU based on their history has become very aware of the harmful potential of having a single entity control information that is sensitive," Santillana said.

While debate continues about the regulation and uses of personal data in the US, Santillana said, "People should be informed."

Buchanan agreed. "It comes back to our communal sense of data and social media literacy," she said. "All of us need to understand what is happening behind the scenes. We need to be aware of the trails of data we are creating and how they are being used."

Expanded Access To CMS Claims Data Offers Benefits and Risks for Patients

By Bridget M. Kuehn

A new rule from the Centers for Medicare & Medicaid Services (CMS) would extend access to CMS claims data to support quality improvement efforts. But the increased access to personally identifiable claims—including to for-profit companies—may pose privacy risks for patients.

The rule, released July 1, 2016, will allow organizations that the CMS has certified as "qualified entities" to share or resell CMS claims data analyses to clinicians, health care organizations, or other organizations, including for-profit ones, to be used for quality improvement efforts. The new rule also outlines privacy and security requirements for the organizations receiving patient-identifiable or de-identified data.

"Increasing access to analyses and data that include Medicare data will make it easier for stakeholders throughout the healthcare system to make smarter and more informed healthcare decisions," said CMS Chief Data Officer Niall Brennan in a press release.

For example, CMS noted that qualified entities could analyze the care received by chronically ill populations to boost quality and possibly drive down the cost of care for these individuals. This might be particularly useful in improving care for patients with chronic kidney disease (CKD) or end stage renal disease. Patients with CKD now make up about 10 percent of the Medicare population, but account for about 20% of Medicare costs, according to an analysis from the United States Renal Data System (http://bit.ly/29ODoit).

Extending data access

The Affordable Care Act of 2010 required CMS to make claims data more accessible to enable measurements of clinician and supplier performance. To qualify for the program, organizations must have experience with performance measurement, be able to handle and combine large datasets, allow clinicians to review and correct performance reports, and meet strict standards for data privacy and security (http://bit.ly/29ELnOK). Initially, CMS only allowed the data to be accessed by non-profit organizations and required public reporting of analyses. But the new rules will extend access to for-profit entities and allow resale of analyses.

To maintain patient privacy, the new rule requires organizations receiving the CMS claims data to use data privacy and security protections "at least as stringent" as that required of organizations covered by the Health Insurance Portability and Accountability Act (HIPAA).

Although CMS has placed some limits on the use of the claims data by for-profit organizations in the new rule, some privacy advocates are concerned identifiable health data might eventually wind up in the hands of companies selling the data for marketing purposes.

"The for-profit change opens the door to a lot of problems," said Pam Dixon, executive director of the World Privacy Forum, a public interest research group based in San Diego, CA.

Many of the for-profit companies that are sophisticated enough to analyze the information-rich CMS claims data also have data brokering divisions, explained Dixon. These data brokering endeavors infer health information about individuals using data sets, like magazine subscriptions, and combine that with other marketing data for resale. The data gathered about an individual through these enterprises is often riddled with errors. For now, CMS has been conservative, only approving a small number of highly vetted for-profits, Dixon said.

"I'm really concerned about who might be approved down the line," Dixon said. "Right now, it does not seem to be really problematic for for-profits [approved by CMS], but that doesn't mean there won't be [problems] in the future."

New protections in the rule, such as requiring qualified entities and those they share data with to meet HIPAA standards for privacy and security, are good steps, Dixon noted. But they are not foolproof. For example, HIPAA allows de-identified patient data to be shared. Studies have revealed, however, that it is very easy to re-identify individuals in such data sets (Sweeney L. *Journal of Law, Medicine & Ethics* 1997; 25:98–110). Large for-profits that broker data for marketing purposes in particular could easily re-identify individuals, Dixon noted.

"There is no such thing as anonymous claims data," Dixon said "Our ability to re-identify the data is too strong."

Another concern is that CMS sharing the data with outside organizations increases the risks of privacy breaches.

"If the data is ever breached and goes out in the wild, that is going to be a profound issue for every patient who has their personally identifiable claims data breached," Dixon said.

Finally, CMS will no longer require public reporting of all of the qualified entities' analyses based on the data, although other requirements still apply. This change may reduce transparency, which was part of the initial promise of the program, Dixon said.

"The purpose of this data is to be used for public benefit, not just for enhancing the profits of a for profit company," she said.