LAW360

Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

HHS Data-Scrubbing Guidance Backs Strict Privacy Definitions

By **Allison Grande**

Law360, New York (November 29, 2012, 10:27 PM ET) -- The U.S. Department of Health and Human Services recently affirmed the validity of the current methods for scrubbing patient records of identifying data under existing medical privacy law, a move that forces health care companies to thoroughly strip records of even seemingly innocuous forms of personal information, attorneys say.

In order to comply with a 2009 congressional mandate, HHS' Office of Civil Rights on Monday published long-awaited guidance on how health insurers, clearinghouses and medical providers can satisfy the two methods for data de-identification contained within the privacy rule of the Health Insurance Portability and Accountability Act, which was established in 2000. Companies benefit from the de-identification process because the use and disclosure of this type of data is exempt from HIPAA regulations and can be used for medical research and other general purposes.

While the guidance makes no substantial changes to the established de-identification methods, it does provide covered entities with useful details concerning some of the technical aspects of these methodologies, clarifying the agency's expectations at a time when electronic information technology is becoming more widespread and presenting tantalizing opportunities for research, according to attorneys.

"It's a confirmation of the methods that companies have been using for the past 10 years, with a deeper dive into them," Hunton & Williams LLP global privacy and data security practice head Lisa Sotto told Law360 on Thursday. "Companies will be able to gain certainty from this that the HHS will continue to interpret de-identification provisions conservatively, as evidenced by, for example, its articulation that the last four digits of a Social Security number [can be] considered protected health information."

The HHS guidance also singles out other types of borderline personal information, such as a person's occupation, a patient code derived from a secure hash function without a secret key, and test dates, as information that could prevent data from being considered de-identified, attorneys noted.

"There has been some debate about whether certain information derived from patient identifiers would still be considered to be protected health information," Holland & Knight LLP data privacy and security team co-chair Shannon Hartsfield Salimone said. "The guidance makes it clear that a data set containing a partial Social Security number, or the patient's initials, [or dates related to a specific patient's care] would still be protected health information unless an expert determines that the information has been sufficiently de-identified."

Congress required HHS to issue this guidance as part of 2009's Health Information Technology for Economic and Clinical Health Act, a directive that HHS was reluctant to fulfill based on its belief that the health care industry was fairly clear on its obligations.

“Covered entities have been operating under these de-identification standards for almost 10 years, and it has not been [HHS'] experience in administering the privacy rule that the standards have been the subject of significant or frequent compliance issues by covered entities,” HHS said.

While the agency's final guidance didn't break any new ground, attorneys welcomed it as a more flushed-out explanation of how to apply the two de-identification standards: a “safe harbor” method that requires companies to remove 18 specific data elements in order to strip data of its protected status, and a “statistical expert” standard, under which information can be considered de-identified if an expert determines that it is virtually useless for identifying an individual.

“HIPAA contains and recognizes some fairly obscure identifiers and data points that would not typically lead to the identification of an individual,” Mintz Levin Cohn Ferris Glovsky & Popeo PC member Dianne Bourque said. “Often, we find that organizations are using a data set that they believe to be de-identified, but there are actually identifiers in it, so it's helpful to reiterate what HHS considers personal data" that needs to be scrubbed.

Clarifying the types of data that need to be removed from data sets can also help companies maximize the value of the information that they hold as the value of and ability to use this data for research and public health purposes increases, Foley Hoag LLP security and privacy practice co-chair Colin Zick added.

“The guidance answers discrete questions that people have come across in operational circumstances, like can you list parts of a ZIP code,” he said. “The answers to these questions could help companies get more use of the de-identified data. For example, if they realize that they can use part of a ZIP code, they might be able to further narrow down their data set instead of completely eliminating that factor.”

But despite the solid positions taken by HHS in its guidance, attorneys pointed out that the regulator also built a bit of flexibility into its guidelines, as evidenced by its admission that “both methods, even when properly applied, yield de-identified data that retains some risk of identification” and that “although the risk is small, it is not zero,” meaning that there is some possibility that the data could be linked back to the corresponding patient.

“HHS recognizes that it is not a static process, and they sort of built in some flexibility there,” Wiley Rein LLP partner Kirk Nahra said. “They didn't say that there's a 100 percent chance it won't be identified; they said it's a low risk.”

Sotto pointed out that this view echoes general guidance issued by the U.K.'s privacy regulator last week, which provided companies with its first substantive piece of guidance on how to make user data anonymous without running up against the country's strict privacy rules.

“It's so interesting to see this HHS guidance after the issuance of the anonymization code in the U.K. because it's acknowledging that there is no way to guarantee anonymization, and that, although companies need to use this data, it needs to be done in a way that is less risky,” she said.

Companies may also find find more leeway in the expert-analysis approach to identification, which doesn't provide as much certainty as removing the 18 specific data elements under the safe-harbor method, but could benefit companies by allowing them to take a more holistic view of their data set, attorneys noted.

As the demand for general sets of health care data continues to rise, Bourque noted that it is important for not only HIPAA-covered entities, but also those outside of the statute's reach that might be handling this data, to take notice of the new guidance.

“All of these organizations are seeing the potential benefit of health care data, but they're not all familiar with HIPAA,” she said. “So it would be helpful for organizations that don't live with HIPAA every day to familiarize themselves with the guidance so that when they are building strategic plans to evaluate and use the data, they are taking the proper steps to ensure that their data will be considered de-identified.”

And while the methods for de-identification didn't change in the latest guidance, that doesn't mean that HHS won't consider updating the standards as technology continues to evolve, attorneys noted.

“HHS clearly seems to be satisfied with the identifiers they are using now and it doesn't appear that the circumstances have changed enough [since the issuance of the HIPAA privacy rule in 2000] to prompt a major change,” Bourque said. “But 20 years ago, a URL might not have been considered an identifier, and in 20 years, we may not need something like ZIP codes. So over time, it may evolve to the point that we are going to need new identifiers or we'll need to get rid of some old ones.”

--Additional reporting by Jeff Overley and Jeremy Barker.