ROBINSON & COLE LLP
ATTORNEYS AT LAW

Attorney Advertising

UPDATE
Health Law Pulse

DECEMBER 2012

HHS-OCR Releases Guidance Regarding Methods for De-identifying Protected Health Information Under HIPAA

The Department of Health and Human Services (HHS) Office of Civil Rights (OCR) recently released guidance (Guidance) on how to implement the de-identification requirements of the Health Insurance Portability and Accountability Act of 1996 Privacy Rule (Privacy Rule). The Health Information Technology for Economic and Clinical Health Act, enacted as part of the American Recovery and Reinvestment Act of 2009, requires HHS to issue this Guidance.

The Privacy Rule protects certain information regarding individuals. This protected health information (PHI) includes information held by a covered entity or a business associate that identifies an individual and relates to his or her physical or mental health, the provision of health care to him or her, or payment for such health care. Information can be classified as PHI if there is a reasonable basis to believe that it can be used to identify a particular individual. The Privacy Rule protects PHI by imposing limits on the ability of covered entities and their business associates to use and disclose PHI. Because health information can be useful for research, policy making, and other activities, even when it does not identify particular individuals, the Privacy Rule permits covered entities and their business associates to de-identify PHI. De-identification is a process in which sufficient individual identifiers are removed from information that would otherwise be classified as PHI so that there is no reasonable basis to believe that the remaining information can be used to identify the individual. Under the Privacy Rule, PHI can be de-identified using one of two methods: (1) by obtaining a written determination from a de-identification expert that there is a "very small" risk that the information, alone or in combination with other reasonably available information, could be used to identify an individual (the Expert Determination Method); *or* (2) by removing 18 specified identifiers from the PHI (Identifiers) and having no actual knowledge that the remaining information, alone or in combination with other information, could be used to identify an individual (the Safe Harbor Method). The Guidance, presented in question-and-answer format, elaborates on these two methods.

In discussing the Expert Determination Method, the Guidance includes the following:

- No specific credentials qualify an individual as an expert. In an enforcement situation,

OCR determines expert status by reviewing the expert's experience using PHI de-identification methodologies as well as his or her academic, professional, and other qualifications.

- The Privacy Rule does not require the use of any particular risk assessment or mitigation methods. Experts can apply generally accepted scientific or statistical principles when conducting the assessment. The Guidance provides an overview of various approaches to mitigation, including suppression (removing certain data elements prior to publication), generalization (creating abstract representations of specific data), and perturbation (replacing specific values with different values, such as replacing a patient's age with a random value within a five-year window of the actual age). No standard establishes what level of risk meets the Privacy Rule's "very small" risk of re-identification requirement. The expert's determination of risk level must take into account the particular data set and the context in which it will be used. OCR expects the risk mitigation process to be a collaboration between the expert and the covered entity through which the expert provides guidance to the covered entity on methods to reduce the risk of re-identification and assists the covered entity in implementing such guidance until the expert determines that the level of risk is "very small."
- While the Privacy Rule does not impose an expiration date on data sets containing de-identified information, some experts set expiration dates on the grounds that technology and other conditions may change over time. Information can still be deemed sufficiently de-identified after its expiration date. When a data set expires, the covered entity should have an expert reexamine the data set to determine whether additional de-identification procedures are required.

In discussing the Safe Harbor Method, the Guidance includes the following:

- The use of only partial Identifiers or derivatives of Identifiers does not satisfy the Safe Harbor Method. For example, a data set containing only the last four digits of a Social Security Number does not satisfy the Safe Harbor Method.
- Examples of dates that should be removed from health records under the Safe Harbor Method include any date more specific than the year of an event. For example, April 10, 2012, can only be reported as "2012." Dates associated with particular tests, such as lab tests, cannot be included because they relate to a specific individual.
- With respect to the Safe Harbor Method's requirement to remove "any other unique identifying number, characteristic or code," the Guidance states that this requirement obligates the covered entity to remove any other information not specifically listed as an Identifier but that could be used to identify an individual, such as a clinical trial record number or certain methods of listing an individual's occupation (for example, by stating that the individual is the "current President of State University").
- The Safe Harbor Method requires that a covered entity have no "actual knowledge" that information remaining after all Identifiers have been removed could be used, alone or in combination with other information, to identify an individual. The term "actual knowledge" means "clear and direct knowledge" that the information could be used for such purposes. Knowledge of specific studies about how data can be re-identified does not constitute actual knowledge under the Safe Harbor Method.
- Covered entities are not required to suppress the names of physicians or members of their workforce that appear in a data set unless those individuals are the subject of the health information or are the relatives, employers, or household members of individuals who are the subject of the health information; however, the covered entity should consider whether the inclusion of such names should be excluded to enable

the covered entity to meet the actual knowledge requirement.

The Guidance clarifies that neither the Expert Determination Method nor the Safe Harbor Method requires covered entities to enter into data use agreements in order to share de-identified data. The Guidance also includes tables and examples that illustrate its explanations of the Privacy Rule's de-identification requirements. While the Guidance does not have the force of law, such as a statute or regulation, it does provide useful insight to how the OCR may review matters involving de-identification of PHI.

If you have questions regarding the de-identification of protected health information, please contact a member of Robinson & Cole's Health Law Group.

Lisa M. Boyle	Theodore J. Tucci	Stephen W. Aronson
Michael J. Kolosky	Charles W. Normand	Pamela H. Del Negro
Teri E. Robins	Brian D. Nichols	Susan E. Roberts
Meaghan Mary Cooper	Eric R. Greenberg