

# PROTECTING THE BENEFITS OF DE-IDENTIFIED HEALTH CARE INFORMATION

by  
Kirk J. Nahra

A Pennsylvania Federal District Court's recent decision in *Steinberg v. CVS Caremark Corp.*, 2:11-cv-02428 (E.D. PA Feb. 16, 2012), recognizes both the benefits of the uses and disclosures of de-identified health care information and the primacy of the HIPAA regulatory structure for defining the appropriate rules for this information. The court's decision therefore is an important step in the ongoing battle to reinforce the beneficial uses of this information, and the decision takes the courts out of disputes about this data that already are defined by the appropriate regulatory process.

## ***Background***

The Privacy Rule established pursuant to the Health Insurance Portability and Accountability Act ("HIPAA") created a series of obligations for health care providers and health insurers related to the uses and disclosure of individually identifiable health care information. These rules created particular situations where patient consent was presumed (in the areas of treatment, payment, and health care operations), as well as certain "public policy" areas where disclosure of patient information was permitted for other public goals (such as establishing rules for disclosure in connection with fraud investigations, litigation, certain public health activities, and otherwise).

The HIPAA rules also created a set of standards for establishing when health care information was no longer "individually identifiable" – or would be considered "de-identified." Where information met the regulatory requirements for de-identification, health care information was considered "de-identified" by law, and therefore was no longer subject to the HIPAA restrictions on the uses and disclosure of individually identifiable information. Because the "individual" component of this

---

**Kirk J. Nahra** is a partner with Wiley Rein LLP in Washington, D.C., where he specializes in healthcare, privacy, information security, and overall compliance litigation and counseling. He is chair of the firm's Privacy Practice and co-chair of its Health Care Practice. Mr. Nahra assists companies in a wide range of industries in analyzing and implementing the requirements of privacy and security laws across the country and internationally. A member of the Board of Directors of the International Association of Privacy Professionals, he is the editor of *Privacy Advisor*, the monthly IAPP newsletter.

information had been removed, this de-identified information then could be used and disclosed for a wide variety of purposes (including research and public health purposes as well as commercial purposes), without creating meaningful privacy risks for any individuals. De-identified information is used widely for these purposes, in the United States and across the world.

This HIPAA framework has existed since the HIPAA Privacy Rule went into effect in 2003. Pursuant to this framework, identifiable health care information is subject to HIPAA restrictions, and de-identified information can be used for additional purposes that otherwise could be impermissible, not subject to restriction under HIPAA. (There are, of course, also good privacy reasons to use de-identified information even for otherwise permitted purposes, whether pursuant to the idea of “minimum necessary” or simply as a means of avoiding or reducing the risk of a privacy or security breach, but this is more of an issue of data “minimization” than anything else).

The HIPAA Privacy Rule acknowledges and supports the benefits of these uses of de-identified information while, at the same time, recognizing that any material privacy interests have been eliminated through this de-identification process. The HIPAA rules make clear that the information we are talking about is “Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information.” See 45 C.F.R. § 164.514(a). HHS, in developing these standards, therefore, specifically wanted to ensure that “the Privacy Rule would not be a disincentive for covered entities to use or disclose de-identified information wherever possible.” 67 Fed. Reg. 14776, 14799 (Mar. 27, 2002).

## ***Litigation Background***

*Steinberg v. CVS Caremark* was filed on behalf of individual consumers and a union benefit fund. The allegations involve two potential classes, comprised of pharmacy patients and third party payors. It alleges sales of prescription information to data mining companies and to pharmaceutical manufacturers directly. This complaint asserts that the data being sold was derived from both consumers and third party payors, contrary to law and to the relevant privacy notices.

These activities allegedly occurred “despite Defendants’ public pronouncements as to the sanctity of both consumers’ privacy and the physician-patient relationship.” In addition to various general “public relations” statements about privacy identified in the complaint, the complaint also focuses on specific statements from the CVS Caremark Notice of Privacy Practices. It asserts that this notice “contains exactly zero information detailing the twin multi-million dollar sale programs.”

The core of the complaint is that CVS, “in direct contradiction to representations made by Defendants,” has profited from the sale and dissemination of “confidential prescription information” obtained from patients and third party payors. This allegedly constitutes unfair and deceptive practices and unjust enrichment.

In Count 1 (an alleged violation of Unfair Trade Practices), the Defendants allegedly omitted material facts from its disclosures whenever it sold a prescription, and intentionally failed to disclose to consumers that it would be engaged in the sale of prescription data. The Complaint asserts that Defendants have engaged in fraudulent or deceptive conduct which creates a likelihood of confusion or misunderstanding.

In Count 2 (for unjust enrichment on behalf of a third party payor class), the assertion is that CVS's receipt of funds through sale of prescription information is unjust in the circumstances, and therefore CVS was "unjustly enriched" to the detriment of the third party payor class. Similarly, in Count 3 (also an unjust enrichment count but this time on behalf of a patient class), the plaintiffs allege, with no additional detail, the restated allegations for the unjust enrichment claim involving the third party payor class.

### ***The Steinberg Decision***

The decision by Judge McLaughlin rejects the plaintiffs' theories in their entirety and dismisses the complaint, with prejudice, relying primarily on her conclusions that the defendants "have not disclosed legally protected information." In addition, as plaintiffs "clarified" at oral argument, the court concluded that defendants "neither sold information entitled to legal protection nor made any misrepresentations on which the plaintiffs justifiably relied regarding the way that consumer information would be handled. In addition, the information the defendants sold to third parties does not carry a compensable value to the plaintiffs or constitute an invasion of privacy." Accordingly, the court dismissed all claims. In addition, "[b]ecause the plaintiffs have not articulated a viable alternative theory of liability, the court's dismissal will be with prejudice."

In small part, the court's decision was based on continuing confusion from the plaintiffs about the basis for their claims. At oral argument, the plaintiffs (despite allegations to the contrary in the complaint) "conceded that the information sold by the defendants to third parties was de-identified within the meaning of HIPAA" (this concession was inconsistent with various assertions in the complaint).

Moreover, the court's decision reinforces the conclusion that the relevant HIPAA rules provide the appropriate yard stick for measuring the appropriateness of the plaintiffs' claims. For the unfair trade practices claim, the court concluded that both "disclosures" made by the defendants (certain communications about the patients made to their treating physicians and certain disclosures of de-identified information to third parties) were "permissible disclosures" under the HIPAA rules. Because these disclosures were permitted by the applicable rules, and the relevant privacy notices made clear that the defendants could make disclosures that were permitted by law, the court found no basis for plaintiffs to assert an unfair or deceptive trade practices claim.

Just as important, however, the court also rejected the plaintiffs' standing under this count, as the plaintiffs demonstrated no justifiable reliance on any statements by the defendants and suffered no financial loss. The court found that "plaintiff's claim that he suffered a loss as a result of the sale of his information is without factual support in the complaint." The complaint "contains no allegations that [plaintiff] would have sought to fill his prescriptions elsewhere had he known of the defendants' practices. Nor does [plaintiff] allege that the defendants' actions deprived him of the opportunity to sell his information to data aggregation firms directly." Therefore, the plaintiff "has not shown that he was harmed by the defendants' actions," and therefore lacked standing to pursue this claim.

The court also rejected the idea that any financial benefit to the defendants was somehow unjust in these circumstances, as the plaintiffs "have not shown that the information disclosures by the defendants caused them to suffer an ascertainable loss. For related reasons, they cannot show that they conferred a benefit on the defendants or that retention of any benefit would be unjust under the circumstances." The court added:

The relationship between the plaintiffs and defendants was one wherein the plaintiffs provided certain information in exchange for the provision of pharmacy services. Under the circumstances the plaintiffs could have no reasonable expectation of being compensated for the information related to that transaction, because that information carries with it no compensable value at the individual level. The plaintiff paid the defendants to fill prescriptions, and the defendants did so. Retention of any benefit accruing to the defendants from the de-identification, aggregation, or sale of patient information could not be considered unjust under the circumstances.

### *Implications*

Questions about the use and disclosure of de-identified information continue to be raised, both in litigation and through the regulatory process. The *Steinberg* decision addresses several of these key issues, and (presumably) creates significant precedent to shut down future claims involving this information. Specifically, the court's decision makes clear that:

- Disclosure of information that has been de-identified pursuant to HIPAA is permitted by law;
- Because this information has been “de-identified,” the individuals whose information was the original source of this de-identified data have no material privacy or monetary interest remaining in the data; and
- The courts should not intervene to address challenges to de-identification practices beyond the HIPAA standards, including the evaluation of whether information properly has been de-identified (as that is an issue for the regulatory and HIPAA enforcement process).

These findings should serve both to stem the tide of future litigation in this area and to protect the many benefits of the use and disclosure of de-identified healthcare information, both for public health and research purposes as well as various commercial purposes. These findings – which clearly are consistent with the approach taken in the HIPAA Privacy Rule – conclude that there is no material privacy interest when otherwise personal information has been de-identified. This approach represents a reasonable and appropriate balance between the Privacy Rule itself – which protects individual privacy interests – and the demonstrable benefits of the use and disclosure of de-identified data, both for clear “public benefit purposes” such as research and public health and for other commercial purposes.