

Better Policies for De-Identified Health Data

by [Deven McGraw](#) [1]

August 21, 2012

The staggering amount of personal health data now being collected for treatment or billing purposes has a life beyond the doctor's clipboard. That data is collected, stripped of personally identifying information ("de-identified") and re-used in ways that are vital for medical breakthroughs, improving patient care, or predicting public health trends. And it's just as valuable when used for targeted marketing campaigns or eliminating inefficiencies in the healthcare industry.

[HIPAA](#) [2] restricts uses of identifiable health information for secondary purposes; but information that is de-identified per HIPAA standards is largely not subject to federal regulation. As a result, de-identified health data is in high demand.

The HIPAA de-identification standards were controversial when introduced in 2000. The reason: no record of personal information can be truly de-identified to the point where there is no risk of becoming identifiable. The Department of Health and Human Services acknowledged this risk when approving the standard, but at the time said it was comfortable with "a reasonable balance between the risk of identification and the usefulness of the information."

Time has not erased the initial concerns about the de-identification standards. Those concerns appear to be on the rise and fall into three categories: 1) sufficiency of the methods used for de-identification; 2) lack of accountability for unauthorized or inappropriate re-identification; and 3) disapproval of certain uses of de-identified data.

In 2009, CDT [began exploring concerns](#) [3] about HIPAA de-identification. In October 2011, we held a workshop for about 50 academic, industry and consumer stakeholders to discuss some policy ideas for addressing de-identified data concerns. A [paper](#) [4] based on the findings of that workshop will be published by the Journal of the American Medical Informatics Association. (An online version of the paper was published in June 26, 2012.)

The paper includes more details on the following policy options for addressing concerns about de-identified health data:

- Prohibiting by law or contract the unauthorized re-identification of de-identified data;
- Ensuring strong, dependable de-identification methods through consistent review of safe harbor methodology and objectively vetting statistical approaches;
- Requiring reasonable security safeguards for de-identified data (today no such safeguards are required); and
- Providing greater transparency to the public regarding uses of de-identified data.

CDT believes these policy ideas merit greater discussion. De-identification should remain an important tool for protecting privacy while preserving the availability of data for uses critical to advancing a more effective and efficient healthcare system.

- [hipaa](#)
- [de-identified](#)



Source URL: <https://cdt.org/blogs/deven-mcgraw/2108better-policies-de-identified-health-data>

Links:

[1] <https://cdt.org/personnel/deven-mcgraw>

[2] <http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html>

[3] https://www.cdt.org/files/pdfs/20090625_deidentify.pdf

[4] <https://www.cdt.org/files/pdfs/JAMA-de-identified-data-trust.pdf>