

Decentralized Approach Needed to Protect Personal Health Data

November 21, 2012

There is a general trend among some businesses and government agencies to develop a new database for every analytic need, and too often these databases collect data centrally. This is particularly problematic when the database contains individual health information.

Although CDT supports cost-cutting and fraud detection goals of centralized health claims databases, individual privacy and data security are at risk when repositories and copies of identifiable personal information are created unnecessarily. When possible, government agencies and businesses should create databases using methods that minimize data transfer and maintain the relative anonymity of data subjects. This can be accomplished through a decentralized approach.

On September 21, 2012, the U.S. Office of Personnel Management (OPM) [submitted a request for comments](#) [1] on a draft of the application for the Multi-State Plan Program (MSP). The OPM, which runs the Federal Employees Health Benefits Program, is mandated by the Affordable Care Act (ACA) to contract with at least two health insurance issuers to offer individual and small group coverage through MSPs. In turn, health insurance issuers who wish to offer MSPs will complete an application, to be evaluated by OPM.

There are several important privacy features in this draft. CDT commends OPM for committing to evaluate applicants on their privacy and security compliance. We are also pleased that OPM will require applicants to describe their compliance with Fair Information Practice Principles. We urge OPM to retain these evaluation criteria in the final MSP application.

However, we have some [recommendations](#) [2] for improvement. In particular, we are concerned about the requirement for MSP applicants to transmit personal data to OPM, including enrollment, reconciliation, health claims/encounter data, and reports. We believe that OPM's plan to centrally collect copies of this data creates unnecessary privacy and security risks. Instead, we've recommended that OPM use a decentralized database approach for the health data it collects; this plan enables data analysis, but typically leaves data housed with its original source.

There are two general approaches to a decentralized system: the "distributed access" approach and the "distributed query" approach. We describe these systems in our comments. Each has its benefits, and the best fit for OPM will depend on OPM's particular analytic needs and resource constraints.

Our comments to OPM show why a decentralized approach will be useful to not only the MSP, but for future health claims databases, too. A decentralized approach utilizes the existing system, minimizes data transfer and costs, and reduces the risk of data breach. Variations of decentralized alternatives can achieve most database goals in a manner more protective of privacy and security in the long term. This level of protection also lines up with public expectations of privacy, and will lead to greater trust from consumers and health care providers.

~~The copyright © 2013 by the Center for Democracy & Technology. All rights reserved. CDT can be freely copied and used as long as you make no substantive changes and clearly give us credit. [Details](#).~~

Source URL:

<https://www.cdt.org/blogs/meredith-whipple/2111decentralized-approach-needed-protect-personal-health-data>



Links:

[1] https://www.fbo.gov/index?s=opportunity&mode=form&id=c9bfc9934ed823d4cae661b06d99d710&tab=core&_cview=0

[2] <https://www.cdt.org/comments/comments-opm-multi-state-plan-program-msp-draft>