How to Build Trust into Health Insurance Exchanges

November 2, 2011

Further Reading

Under the Patient Protection and Affordable Care Act [1] (PPACA), the legislation that enacted most of the recent federal health care reforms, states are directed to establish health insurance exchanges to assist individuals with finding affordable insurance coverage for themselves and their families. If built right, exchanges can offer a number of important benefits. However, much of the data that these exchanges will collect is sensitive (and some of it highly sensitive). If the information collected by exchanges is not protected by adequate privacy rules and security safeguards, individuals will not have sufficient trust in an exchange to take advantage of its benefits.

The Department of Health and Human Services (HHS) issued [2] a proposed rule setting out some basic requirements for exchanges. CDT was pleased to see HHS pay some attention to privacy and security concerns, but we also believe the rule could be improved in a number of ways. In comments submitted earlier this week [see *supporting documents box* on this page], CDT urged HHS to:

- Adopt policies governing the exchanges that follow the full complement of fair information practices;

- Specifically incorporate the strict statutory limitations in PPACA on the ability of exchanges to collect, use and disclose personally identifiable information, including social security numbers in particular;

- Prohibit the collection of data on individuals who are merely exploring the exchange website for information, rather than applying for coverage;

- Retain the requirement that exchanges comply with key provisions of the HIPAA Security Rule, and make clear that even those exchanges that are covered by the HIPAA Privacy Rule are subject to any specific, more stringent privacy rules set by HHS or states governing exchanges;

- Require exchanges to follow the “individual rights” provisions of the HIPAA Privacy Rule, such as the right to amend or dispute the accuracy of personal information;

- Require exchanges to obtain specific authorization from individuals prior to using any personally identifiable information (including an IP address) for a marketing purpose;

- Require exchanges to compel their contractors to abide by the same or more stringent privacy and security standards than are applicable to the exchange; and

- Establish a tiered penalty structure, so that civil penalties apply to relatively lesser violations of privacy and security requirements and criminal penalties apply when there is a knowing or willful violation.

Links:
[1] http://www.gpo.gov/fdsys/pkg/PLAW-111publ148/pdf/PLAW-111publ148.pdf
[2] http://www.gpo.gov/fdsys/pkg/FR-2011-07-15/html/2011-17610.htm