Toward a Privacy Healthy, Health Insurance Exchange

March 28, 2012

Further Reading

Strong privacy and security rules are crucial to the success of the new health insurance exchanges mandated by the Health Care Reform.1

These exchanges will require new and unique exchanges of data among state agencies, the federal government, private health plans, businesses, individuals and the exchange itself. This process will trigger the creation, collection, exchange, and disclosure of personally identifiable information. Exchanges will handle, at a minimum, basic demographic information, financial information, immigration information, incarceration information and Social Security Numbers.

If health insurance exchanges are built and implemented correctly, individuals will no longer need to decide whether to apply for public program or private insurance. Instead, individuals will have a single, online portal at which one application filed will be screened and result in the correct form of coverage and benefits depending on the applicant's circumstances. However, if adequate privacy rules and security safeguards do not protect the information collected by exchanges, individuals will not have sufficient trust in an exchange to take advantage of its benefits.

The Department of Health and Human Services (HHS) has finalized the basic requirements [1] for exchanges. CDT was pleased to see HHS extensively address privacy and security concerns, consistent with the comments and recommendations [2] CDT made in October.

According to the rule:

- Any personally identifiable information created or collected by a health insurance exchange to perform its core functions may not be used or disclosed, except to carry out those functions. Any individual who knowingly or willfully violates this limitation may be subject to a civil penalty of not more than $25,000 per person or entity, in addition to any other penalties that might apply.

- An exchange must establish and implement privacy and security standards for personally identifiable information that are consistent with the framework [3] of fair information practices adopted by the HHS Office of the National Coordinator. The policies and procedures must be in writing and available to the HHS Secretary on request, and identify any other applicable law governing the health insurance exchange's collection, use and disclosure of personally identifiable information.

- An exchange must establish and implement operational, technical, administrative, and physical safeguards that that comply with privacy policies and limits on the exchanges' collection, use and disclosure of personally identifiable information.

- Sharing of personally identifiable information between the exchange and agencies administering Medicaid or Medicare for purposes of eligibility determinations must meet the rule's privacy and security requirements as well as requirements in other parts of the Affordable Care Act and the Social Security Act. Agency-to-agency "data matching" programs must follow relevant federal rules, too.

- Except in circumstances where collection, use or disclosure of personally identifiable information is required by law, or for tax return information that is covered by Section 6103 of the Internal Revenue Code, exchanges are required to hold contractors – such as Navigators, agents and brokers – and others accessing personally identifiable information through an exchange to the privacy and security requirements. The health insurance exchange is also required to ensure its workforce

follows the rule's requirements.

California "Role Model"

Several states have taken steps to create exchanges. California is a national leader on insurance exchanges - in 2010 it became the first state to pass legislation establishing the core functions of the state insurance exchange, the Health Benefit Exchange or HBEX.

California is well positioned to continue leading the way by developing and implementing policies from the outset that protect the privacy, confidentiality and security of personal information and promote public trust in the state's exchange.

CDT has released a paper [4] summarizing the federal and state privacy laws that will apply to California's HBEX and calling on the state to work with consumers and other stakeholders to promptly develop specific privacy and security policies that will apply to the state's exchange.

1. 1. The Patient Protection and Affordable Care Act of 2010 called for the creation of health insurance "exchanges." Exchanges are new, web-based entities intended to create a more organized and competitive market for health insurance by offering a choice of plans, establishing common rules regarding the offering and pricing of insurance, providing information to help consumers better understand the options available to them, and helping individuals find and enroll in affordable health insurance coverage.

-
- health privacy project
- Health Privacy
- health insurance exchange

Copyright © 2013 by Center for Democracy & Technology
The content on this website that originates with 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/kate-black/2803toward-privacy-healthy-health-insurance-exchange

Links:
[1] http://www.gpo.gov/fdsys/pkg/FR-2012-03-27/html/2012-6125.htm
[2] https://www.cdt.org/blogs/deven-mcgraw/211how-build-trust-health-insurance-exchanges
[3] http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_10731_848088_0_0_18/NationwidePS_Framework-5.pdf
[4] https://www.cdt.org/files/pdfs/California-Insurance-Exchange-Privacy.pdf