KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 Eye Street, NW
Suite 1100
Washington, DC 20006

October 28, 2011

The Honorable Kathleen Sebelius
Secretary of Health and Human Services
Attention: CMS–9989–P
U.S. Department of Health and Human Services
200 Independence Avenue, SW
Washington, D.C. 20201

Re: RIN 0938–AQ67 (Patient Protection and Affordable Care Act; Establishment of Exchanges and Qualified Health Plans)

Dear Secretary Sebelius:

The Center for Democracy and Technology (CDT), through its Health Privacy Project, promotes comprehensive, workable privacy and security policies to protect health data as it is exchanged using information technology. CDT is frequently relied on for sound policy advice regarding the challenges to health privacy and security presented by health information technology (health IT) initiatives. We have testified before Congress four times on the privacy and security issues raised by health IT, and we chair the privacy and security working group of the federal Health IT Policy Committee (called the "Tiger Team").

CDT submits these comments in response to the Centers for Medicare and Medicaid Services July 15, 2011 Notice of Proposed Rulemaking (NPRM) on the *Patient Protection and Affordable Care Act; Establishment of Exchanges and Qualified Health Plans.*[1] We commend your efforts to develop comprehensive regulations, guidance and grant programs to provide an initial foundation for health insurance exchanges. However, we have identified a number of areas where HHS should make improvements when drafting the final rule.

I. Introduction

We are enthusiastic about the potential of insurance exchanges for connecting consumers to affordable health care coverage, for bringing fresh competition to the insurance marketplace, for expanding and improving enforcement of consumer protections, and for driving system reforms in addition to quality improvement. If built right, exchanges can offer individuals new tools and information related to cost, quality, network adequacy, comprehensiveness of benefits, reliability and responsiveness that will make a difference in their ability to secure adequate and affordable coverage for themselves and their families. However, much of the data that these exchanges will

[1] 76 Fed. Reg. 41866-41927 (July 15, 2011).

collect is sensitive (and some of it highly sensitive). If this data is not protected by adequate privacy rules and security safeguards, individuals will not have sufficient trust in the exchange to take advantage of its benefits.

We offer the following recommendations, discussed in more detail below, regarding the implementation of these exchanges and specifically ask that you:

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

- Adopt language in the final regulation that incorporates the strict statutory limitations on the ability of exchanges to collect, use and disclose personally identifiable information, including social security numbers in particular. We further recommend that you ensure that exchanges do not collect data on individuals who are merely exploring the exchange website for information, rather than applying for coverage.

- Retain the requirement in the final rule 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 privacy rules set by HHS or states governing exchanges.

- Require exchanges to follow the "individual rights" provisions of the HIPAA Privacy Rule or to incorporate these provisions into their policies and 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 take action against contractors that violate them. We urge you to apply these requirements to the Navigator program as well.

- 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.

II. Adoption of Policies Consistent with Fair Information Practices

CDT has repeatedly called for a comprehensive framework of privacy and security protections for health data that address the full complement of fair information practices (FIPs).[2] FIPs, which provided the foundation for the HIPAA Privacy and Security Rules, are fundamental to privacy law both domestically and internationally. The Office of the National Coordinator for Health Information Technology (ONC) also adopted FIPs

[2] *See, e.g.*, McGraw D., Dempsey JX, Harris L, Goldman, J. "Privacy as Enabler, not an impediment: Building trust into health information exchange." Health Affairs 2009; 28(2): 416-27.

through the Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information.[3]

FIPs provide the roadmap for establishing comprehensive and sound policies to govern the collection, use and disclosure of personal information. Ensuring that consumers' personal information is kept private and secure is an important element of fostering the public's trust of these new insurance exchanges, and the proposed rule includes a number of important provisions in this area.

We strongly support the rule's proposed requirement that insurance exchanges follow the full complement of FIPs and urge that you retain this requirement in the final rule. Further, the final regulation should make clear that exchange policies must address each and every component of the FIPs. For purposes of consistency, we suggest that HHS adopt the model of FIPs endorsed by the HHS Office of the National Coordinator for Health IT (and referenced in footnote 6 of the preamble to the proposed rule).[4] In addition, it is critical that exchange privacy policies be developed with public input. Consequently, we urge HHS in the final rule to include a requirement that exchanges engage participants, including consumers, in developing its privacy policies and allow for a period of public comment prior to submission to the HHS Secretary.

As noted in more detail below, although FIPs should be the foundation for comprehensive privacy policies governing exchanges, exchanges also should be subject to clear limits regarding their ability to collect, use, disclose and retain personal information about an applicant for insurance.

Recommendations: *Require exchanges to follow the full complement of fair information practices. Ensure that exchange privacy policies are subject to public notice and comment prior to submission to the HHS Secretary. An exchange's specific policies should be part of a state-operated exchange's written Exchange Plan or a similar comparable document that is available to the public.*

III. Exchanges Should be Subject to Limits in Their Ability to Collect, Use, Disclose and Retain Personal Information

Although FIPs are certainly fundamental and following them should be required, they are insufficient on their own to ensure individual trust in the operations of an exchange. In order for individuals to feel comfortable using an exchange, they must be able to trust that any information they provide to the exchange will be kept confidential; that it will be accessed, used and disclosed only for exchange-related purposes; and that it will be retained only for so long as is reasonably needed for exchange-related purposes.

---

[3] Dept. of Health and Human Services, Office of the National Coordinator, Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information, Dec. 15, 2008, pg. 7, http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_10731_848088_0_0_18/NationwidePS_Framework-5.pdf.

[4] *Id.* at 41880.

As a result, we recommend that you adopt language in the final regulation that incorporates the strict limitations in the statute (discussed below) on the ability of exchanges to collect, use and disclose personally identifiable information. We urge you to restrict the collection, use and disclosure of social security numbers in particular for any purpose unrelated to eligibility determination and ensure that exchanges do not collect data on individuals who are merely exploring the exchange website for information, rather than applying for coverage.

A. Limitations on Data Collection, Use and Disclosure

Section 1411(g)(1) of the Patient Protection and Affordable Care Act of 2010 (the "Affordable Care Act" or ACA) places strong limits on the data that can be collected about a person seeking insurance coverage through an exchange. Specifically, data collection is limited "to the information *strictly necessary* to authenticate identity, determine eligibility, and determine the amount of the credit or reduction" (emphasis added).[5] Section 1411(g)(2) states that exchanges can use such information only "for the purpose of, and to the extent necessary in, ensuring the efficient operation of the exchange."[6] Such language is an example of how to implement the collection and use limitations of the FIPs.

The proposed regulatory language, however, does not follow the strict limitations set by the statute. For example, proposed Section 155.260(b) would allow personally identifiable information to be collected, used or disclosed by the exchange if it is permitted "by other applicable law."[7] Since such other laws may permit the exchange to collect, use and disclose personally identifiable information for purposes not necessary for the operation of the exchange, this provision in the proposed rule fails to implement the statute and the clear intent of Congress. The final rule should appropriately reflect the strict statutory limitations on the ability of exchanges to collect, use and disclose personally identifiable information.

B. Limitations on Collection, Use and Disclosure of Social Security Numbers

Section 1411(g) of the ACA also limits the collection, use and disclosure of social security numbers. These numbers can only be required from applicants seeking benefits (as noted in §435.907(e)(1)) and of the primary taxpayers that have SSNs (pursuant to §155.305 (f)(6))[8]. The use of these numbers should be restricted to activity related to determination of eligibility for health insurance affordability programs and cannot be disclosed to any third parties for purposes unrelated to eligibility determination.

C. Anonymous Site Exploration

We also believe that many potential applicants for insurance through an exchange will want to explore the exchange website and investigate available information and coverage options before formally submitting an application for insurance. We urge HHS

[5] P.L. 111-148, §1411(g)(1).
[6] *Id.*, at §1411(g)(2).
[7] Proposed § 155.206(b), 76 Fed. Reg. at 41916 (July 15, 2011).
[8] P.L 111-148, §§ 435.907(e)(1) and 155.305(f)(6).

in the final rule to ensure that exchanges provide individuals the option of exploring the site anonymously (including the ability to peruse the site without their on-line activity being cached) until the individual has affirmatively indicated an interest in applying for insurance through an exchange.

Recommendations: *Adopt language in the final regulation that incorporates the strict limitations in the statute on the ability of exchanges to collect, use and disclose personally identifiable information. Restrict the collection, use and disclosure of social security numbers for any purpose unrelated to eligibility determination. Ensure exchanges do not collect data on individuals who are merely exploring the exchange website for information and not applying for coverage.*

IV. Application of HIPAA Security Rule and Potential Application of HIPAA Privacy Rule

We applaud HHS for proposing that exchanges be required to comply with key provisions of the HIPAA Security Rule, and we urge HHS to retain this provision in the final rule. It is critical to building public trust that exchanges be held accountable for implementing reasonable security measures to protect the information they are collecting from individuals.

In the preamble to the proposed rule, HHS notes that, in some cases, an exchange might be covered by the HIPAA Privacy Rule, either as a covered entity or a business associate.[9] For those entities not covered by HIPAA, we agree with HHS that it would be unwise to apply the entirety of the HIPAA Privacy Rule (although we do note below some provisions of the Privacy Rule that HHS should consider including in the final exchange rule).

The HIPAA Privacy Rule was created to support the routine flows of patient health information among health care providers, health plans and healthcare clearinghouses for treatment, payment and operations functions. The Rule was not specifically designed to accommodate the privacy challenges raised by exchanges and would likely permit overbroad collection, use and disclosure of data than was intended by Congress in setting clear statutory limits on exchanges in Section 1411(g). Consequently, even those exchanges that are covered by the Privacy Rule should be subject to any additional specific rules set by HHS or states with regard to exchanges, and the final rule should be clear on this point.

A. Individual Rights

Although we agree that HHS should not apply the Privacy Rule in its entirety to exchanges, the "individual rights" provisions of the Privacy Rule provide individuals with some baseline rights with respect to personally identifiable information that should be applicable to exchanges. For example, the HIPAA Privacy Rule gives individuals the right:

[9] 76 Fed. Reg. at 41879 – 41880.

- To receive a notice of privacy practices;[10]
- To request an amendment to personal information;[11]
- To access a copy of personal information collected about them;[12] and
- To receive an accounting of disclosures of their personal information (currently being revised by the HHS Office of Civil Rights to potentially include a right to a report of who has had access to their personal information).[13]

These provisions implement several FIPs, and the final rule should require exchanges to follow them or incorporate them into their policies.

B. Marketing

In addition, the Privacy Rule prohibits the use of an individual's personally identifiable information for marketing purposes unless that particular marketing use has been expressly authorized by the individual.[14] Since exchanges are required to be financially self-sustainable by January 1, 2015, selling access rights for marketing purposes might be seen as a viable potential business model. However, surveys consistently show that individuals want to be asked before their personal information is used for marketing purposes.[15]

To ensure that individuals across the country can trust an exchange to keep their information confidential, the final rule should require exchanges to obtain specific authorization from individuals before they are permitted to use any personally identifiable information (including an IP address) for a marketing purpose. Requiring authorization or consent for marketing uses is also consistent with recent reports on privacy issued by the Federal Trade Commission and the Department of Commerce.[16]

Recommendations: *Make clear in the final rule that even those exchanges that are covered by the HIPAA Privacy Rule are subject to any specific privacy rules set by HHS or states governing exchanges. Require exchanges to follow the "individual rights" provisions of the HIPAA privacy rule or to incorporate these provisions into their policies. Require exchanges to obtain specific authorization from individuals prior to using any personally identifiable information (including an IP address) for a marketing purpose.*

---

[10] 45 C.F.R. §164.520.
[11] 45 C.F.R. §164.526.
[12] 45 C.F.R. §164.524.
[13] 45 C.F.R. §164.528.
[14] 45 C.F.R. §164.508((a)(3). (Currently being revised by HHS to incorporate changes required by Section 13406(a) of the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH).)
[15] *See, e.g.,* Study by Lake Research Partners and American Viewpoint, conducted by the Markle Foundation (November 2006), *available at*: http://www.markle.org/downloadable_assets/research_doc_120706.pdf.
[16] *See* "Protecting Consumer Privacy in an Era of Rapid Change," Federal Trade Commission preliminary staff report, December 2010, and "Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework," the Department of Commerce Internet Policy Task Force, December 2010.

V. Requirement to Bind Contractors

We support HHS' proposal to require exchanges to bind their contractors to the same or more stringent privacy and security standards than are applicable to the exchange. We recommend that you retain these requirements in the final rule and apply them to the Navigator program as well.

It is critical that these privacy and security standards for contractors include the limits set by Congress in Section 1411(g) of the ACA with respect to data collection, use and disclosure, the other express limits urged by these comments and adopted by HHS in the final rule, and any additional requirements set by states. It is understandable that exchanges will likely need to use contractors to assist them in performing certain functions, but the contract should not be permitted to become a vehicle for broader sharing of the personally identifiable information of insurance applicants.

In addition, the final rule should also require exchanges to take action against contractors that it knows (or reasonably should know) are in violation of privacy and security standards. Such action can start at requiring corrective action by the contractor but should ultimately result in contract termination if compliance failures are not corrected within a reasonable period of time. (The amount of time considered reasonable should be based on the potential of the violation to put an applicant's personal information at risk). Exchanges that fail to take such action against contractors should be held accountable under the penalty provisions discussed below.

Navigators, which will be funded through grant programs to be established by exchanges, should also be subject to the requirement to abide by the same or more stringent privacy and security standards than are applicable to the exchange. The details of Navigator privacy and security standards should be spelled out as part of the exchange's grant-making process or otherwise as part of state requirements for Navigators.

Recommendations: *Bind contractors to the express statutory data collection, use and disclosure limitations, and require exchanges to take action against contractors who are in violation of privacy and security standards. Require Navigators to abide by the same or more stringent privacy and security standards that are applicable to the exchange*

VI. Penalties for Improper Use and Disclosure of Information

We support the inclusion in the proposed rule of the statutory penalty for knowing and willful uses or disclosures of information in violation of Section 1411(g) of the ACA. We note that in HIPAA, knowing and willful violations of privacy and security regulations can be subject to criminal penalties, with civil penalties reserved for violations that are based on lack of knowledge of the law or negligence.[17]

[17] Sections 1176 and 1177 of the Social Security Act.

We believe that lesser violations of the proposed rule – such as those based on negligence – should be subject to penalties as well, and that harsher penalties should apply when violations are knowing and willful. We recommend that HHS 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. If HHS does not believe it has the legal authority to impose a more HIPAA-like penalty structure on exchanges, it should seek specific authority to do so from Congress.

Recommendation: *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.*

VII. Conclusion

We thank you very much for the opportunity to submit these comments and again applaud the effort that went into these proposed regulations. CDT remains committed to advancing policies that support the privacy and security of health information based on fair information practices and we look forward to the final rule.

Sincerely yours,

Deven McGraw
Director, Health Privacy Project
Center for Democracy & Technology