July 19, 2013

Marilyn Tavenner
Administrator
Centers for Medicare & Medicaid Services
Department of Health and Human Services
P.O. Box 8010
Baltimore, MD 21244

Re: CMS-9957-P

Dear Administrator Tavenner,

The Center for Democracy & Technology ("CDT") is a non-profit Internet and technology advocacy organization that promotes public policies that preserve privacy and enhance civil liberties in the digital age. As information technology is increasingly used to support the exchange of medical records and other health information, through its Health Privacy Project, champions comprehensive privacy and security policies to protect health data. CDT promotes its position through public policy advocacy, public education and litigation, as well as through the development of industry best practices and technology standards. Recognizing that a networked health care system can lead to improved health care quality, reduced costs and empowered consumers, CDT is using its experience to shape workable privacy solutions for a health care system characterized by electronic health information exchange.

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 the U.S. Congress six times since 2008 on the privacy and security issues raised by health IT, and we chair the privacy and security policy working group of the federal Health IT Policy Committee.

CDT submits these comments in response to the Department of Health & Human Services' (HHS) Centers for Medicare and Medicaid Services' (CMS) proposed rulemaking on *Patient Protection and Affordable Care Act; Program Integrity: Exchange, SHOP, Premium Stabilization Programs, and Marketing Standards*. Most of our comments are aimed at assuring that the infrastructure to support

implementation of the Affordable Care Act adequately protects the privacy and security of consumer's personal information, a topic that was recently highlighted in a joint hearing of the U.S. House of Representatives Committees on Oversight and Investigations and the Homeland Security on July 17, 2013.

Distributed Access Model (45 CFR 153, Subpart H)

We commend CMS for pursuing a distributed model for accessing claims data for risk adjustment purposes. In October of 2011, CDT recommended that CMS adopt a model that enables the agency to access claims data without physically collecting it. (https://www.cdt.org/files/pdfs/CDT_Comments_to_CMS-9975-P.pdf) Such a "distributed access" model allows CMS to perform risk adjustment on actual claims but without the privacy risk associated with collection or retention of the data.

We recognize that the distributed access model for risk adjustment depends on all plans providing CMS with the necessary access to claims data. Therefore, we agree with CMS' proposal to impose sanctions on those plans that do not provide the requisite data access and urge the agency to retain it in the final rule.

Agent and Broker Privacy and Security Training (45 CFR 155.220)

We applaud CMS' proposal to require that agents and brokers assisting individuals enrolling in the individual market of a Federally-Facilitated Exchange (FFE) receive privacy and security training. However, we recommend that the final rule require that this training occur on at least an annual basis and apply to both FFEs as well as State Exchanges. In addition, the final rule should require such recurring training to include any updates to exchange privacy and security regulations, both at the state and federal level. Also, such training should include any changes made to exchange policies and practices adopted to implement privacy and security regulations.

Standards for Agent and Broker Termination (45 CFR 155.220)

We agree with CMS that FFE agreements should be terminated between HHS and agents or brokers should the agent or broker be found to be in severe non-compliance with the standards of Section 155.220, including the privacy and security standards. We also appreciate that the requirement to abide by exchange privacy and security regulations survives the termination of any agreement between an agent or broker and a FFE. However, CMS should provide State Exchanges with similar authority to terminate agreements with their agents and brokers and hold State Exchanges accountable for proper

management of agents and brokers, including assuring compliance with Exchange privacy and security rules.

The Affordable Care Act makes clear that data collected by an exchange be used for exchange purposes only. Consequently, when an agreement between an Exchange and an agent or broker is terminated, such termination also ends an agent or broker's authority to access, use or disclose any data collected from applicants. Unfortunately, the proposed regulation does not include language requiring agents and brokers to securely destroy the data any applicant (or potential applicant data) that they collected prior to termination of the agreement. We urge CMS, in the final rule, to require agents or brokers whose agreements with any Exchange has been terminated (either voluntarily or for severe noncompliance) to destroy applicant data in a manner consistent with NIST destruction standards.

In addition, we recommend that CMS include language in Section 155.220(c)(3) that Web-based brokers are not allowed to collect any data that is not solely for exchange enrollment purposes and not allowed to use data collected for exchange enrollment for other purposes. As an example, a web-based broker may use a web browser cookie to collect information on an enrollee. While these kinds of tracking elements are valuable for recognizing an enrollee over time after a log-in step or if the enrollee must return to the application multiple times; there is a risk that this kind of tracking could be used by an issuer with multiple business lines to market other goods or services to the enrollee based on confidential and sensitive data that the enrollee provided as part of the exchange application. Usage of application and applicant data for third party marketing should be strictly prohibited.

Oversight and Monitoring of Privacy and Security Requirements (45 CFR 155.280)

We commend CMS for proposing that HHS will audit and oversee compliance of FFEs, their non-exchange entities and State Exchanges with privacy and security policies through periodic auditing and investigations when necessary. In addition, we recommend that HHS make either a de-identified or an aggregate report of the findings from these audits available to the public on an annual basis to provide transparency to the public about how well Exchanges are complying with federal requirements. In addition, we agree that State Exchanges should be responsible for monitoring privacy and security compliance of their non-Exchange entities. However, we request that State Exchanges be expressly required to conduct audits of their non-Exchange entities on a recurring basis.

Breaches and Incidents (45 CFR 155.280(c)(1))

We agree with CMS that using the definitions of "breach" and "incident" from HIPAA are not adequate in terms of the protections necessary for Exchanges.

We are very pleased to see that CMS has adopted the requirement that FFEs, non-Exchange entities associated with FFEs and State Exchanges will be required to report incidents and breaches to HHS. While we agree with CMS that prompt notification is good, we believe that a one hour time frame might be too quick in order to enable assessment of whether a suspicious event is truly a breach or incident.

We recommend that this language be modified to say that "…FFEs, non-Exchange entities associated with FFEs and State Exchanges must report all *suspected* privacy and security incidents or breaches to HHS within one hour." In addition, these entities should be required to provide continuing communication with HHS after understanding the full extent of a suspected breach or incident.

Another concern is that there is no timeframe for non-Exchange entities to report to State Exchanges any incidents or breaches. We recommend that CMS adopt a baseline standard and permit State Exchanges to either adopt this baseline standard or adopt more stringent standard.

In addition, we expect that the one-hour reporting requirement for State Exchanges is not triggered until the State Exchange has knowledge that such a breach or incident has or may have occurred. Consequently, the final rule should make clear that State Exchanges must require their non-exchange entities to report to the State Exchange all suspected privacy and security breaches or incidents within an hour. Failure to incorporate the state non-exchange entities into the reporting loop reduces the potential benefits of a prompt reporting requirement on State Exchanges.

Allowing Issuer Customer Service Representatives to Assist with Eligibility Applications (45 CFR 155.415 & 155.1230)

We are pleased to see that issuer customer services representatives who assist with eligibility applications will be required to comply with exchange privacy and security rules. Because these issuer representatives, in the course of assisting an applicant, will have access to information that is required by law to be used solely for Exchange purposes, we urge CMS to make clear in the final regulations that issuers who deploy representatives to assist with eligibility must adopt clear internal policies and technical safeguards to ensure compliance with exchange privacy and security rules. In addition, CMS should specify that a serious violation of privacy and security regulations by an issuer or their customer service

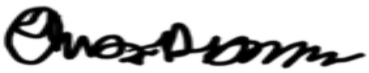
representative may be cause for de-certification of the plan in the Exchange, in a case where the plan knew or, or should have known of, the serious noncompliance by their representative.

Publicly Available Privacy and Security Rules

We note that Section 155.260(a)(3) requires that Exchanges develop privacy and security standards that are open and transparent. Accordingly, we recommend that CMS require that FFEs and State Exchanges make publicly available the privacy and security policies and procedures that they develop.

We thank CMS for the opportunity to submit comments. Please do not hesitate to contact us if we can be of any assistance.

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



Christopher Rasmussen
Policy Analyst, Health Privacy Project
Center for Democracy & Technology