State of West Virginia
Office of the Attorney General

Patrick Morrisey
Attorney General

(304) 558-2021
Fax (304) 558-0140

August 14, 2013

Via Certified Mail & Email

The Honorable Kathleen Sebelius
U.S. Department of Health and Human Services
200 Independence Avenue, S.W.
Washington, D.C. 20201
Kathleen.Sebelius@hhs.gov

Re: A communication from the States of West Virginia, Alabama, Florida, Georgia, Kansas, Louisiana, Michigan, Montana, Nebraska, North Dakota, Oklahoma, South Carolina, and Texas regarding data privacy risks posed by programs assisting consumers with enrollment in health insurance through the new exchanges

Dear Secretary Sebelius:

As the chief legal officers of our states, we are concerned that the U.S. Department of Health and Human Services ("HHS") has failed to adequately protect the privacy of those who will use the assistance programs connected with the new health insurance exchanges. The Patient Protection and Affordable Care Act provides funding for groups to assist consumers in understanding their health insurance options on the new exchanges. When the exchanges begin enrollment, various "navigator," assister, application counselor, and other consumer outreach programs will begin inputting consumers' private data into insurance applications to help consumers enroll in health insurance plans. We take very seriously the privacy of our states' consumers and believe that your agency's current guidance regarding these groups suffers numerous deficiencies.

A Risk of Inadequate Training

Personnel in many of the new programs will have significant access to consumers' personal information, yet HHS's relevant guidance lacks clarity regarding privacy protection. In the July 17, 2013 Final Rule relating to the Standards for Navigators and Non-Navigator Assistance Personnel, HHS stated that personnel will "receive training on the privacy and security standards applicable" to their work. It promises that the training will be "extensive." But the Rule did not set forth any of the applicable standards beyond citing 45 C.F.R. § 155.260, which merely sets forth broad principles for data protection: "individual access," "correction," "openness and transparency," "individual choice," "collection use and disclosure limitations," "data quality and integrity," "safeguards," and "accountability." As to what these principles mean in practice, the Rule provides platitudes with little concrete guidance, requiring: "reasonable operational, administrative, technical, and physical safeguards to ensure [data] confidentiality, integrity, and availability and to prevent unauthorized or inappropriate access, use, or disclosure"; protections "against any reasonably anticipated threats or hazards to the confidentiality, integrity, and availability of such information"; and "openness and transparency about policies, procedures, and technologies that directly affect individuals and/or their personally identifiable information." The Rule does not even require uniform criminal background or fingerprint checks before hiring personnel; indeed, it does not state that *any* prior criminal acts are *per se* disqualifying.

Likewise, in the related June 19, 2013 Proposed Rule on Program Integrity, HHS proposed monitoring grantees for adherence to applicable privacy and security requirements, but did not articulate what those requirements would be. For example, while HHS proposed adopting abstract regulations forbidding unauthorized security "breaches" and "incidents," the proposed regulations did not identify what exactly would constitute such events. Moreover, although HHS proposed requiring grantees and exchanges to have accountability standards and procedures in the event of a breach of private information, the agency suggested nothing specific beyond a requirement that HHS be notified of such breaches.

The short time remaining before exchange enrollment begins will only exacerbate these unclear standards. Enrollment is currently set to begin October 1, 2013, and yet many programs have not received their grants and thus have not started preparations. HHS is scheduled to finish awarding grants to applicants no later than August 15, which will leave participating programs only thirty-two business days to screen, hire, and train thousands of new personnel nationwide. In that window, inexperienced new grantees will have to read these "principles" and guess what they should do, and HHS will not have sufficient time to consult with or audit each program prior to enrollment. Consumer privacy will be catch-as-catch-can in each program. As it now stands, it is inevitable that HHS's vague "standards" will result in improperly screened or

inadequately trained personnel. These individuals will be more prone to misappropriate—accidentally or intentionally—the private data of consumers.

To make matters worse, HHS recently announced that it may cut back on its previously announced and already scant training requirements due to time constraints. As reported in the Wall Street Journal on August 5, 2013: "With time running short before enrollment kicks off Oct. 1, the Obama Administration last week cut back on training requirements for these 'navigators.' Officials were concerned there might not be enough time to do more-extensive training before the health-insurance exchanges open." Previously, the Rule stated that navigators would need up to 30 hours of online training before they start, but, as reported in the same article, HHS has since said in an interview with an official spokesperson that an initial "20 hours would be sufficient." Setting aside the absurdity of simply changing the rules to paper over the Administration's abject failure at implementing the statute, *reduced* training requirements are only going to lead to more problems.

This is exactly the wrong response. HHS must take action to ensure that thorough and specific safeguards are put in place to protect the confidentiality of consumers' data before enrollment begins. Rigorous programmatic safeguards are needed to prevent security breaches by new personnel, as well as to ensure clear lines of accountability for any harm caused by confidentiality breaches. As of right now, your agency has no realistic plan to prevent identity theft or to provide recourse to consumers when it inevitably occurs.

Less Consumer Protection Than In Other Contexts

The risk of inadequate training is only one problem. The proposed consumer safeguards are also woefully substandard. When compared to other privacy protections at the state and federal levels, the vague requirements in your agency's guidance come up well short.

For example, the guidelines appear to provide significantly less protection to consumers with respect to navigators than the states have provided with respect to insurance agents and brokers. For decades, health insurance agents and brokers have been subject to strict state-level exam-based licensing laws and annual continuing education requirements, as well as significant federal and state privacy, security, and market conduct requirements. Furthermore, licensed agents and brokers are personally liable if they fail to comply with these laws and requirements, and are obligated to maintain professional liability insurance to protect consumers. Your guidance does not include comparably rigorous training or educational requirements for navigators. Nor does your guidance impose specific liability for disclosing the many forms of private information that will be given to counselors. Existing laws criminally prohibit sharing certain forms of consumer information, such as tax returns, but those laws do not cover all the information consumers will provide to these HHS-sponsored programs.

What is more, your agency's guidance could be construed to limit state efforts to impose such licensing requirements on the numerous non-profit groups expected to do most of the work of assisting consumers. The Rule provides that state licensure or certification rules must not prevent the application of ACA navigator requirements, and the regulations require at least one navigator entity *not* to be a licensed agent or broker. 45 C.F.R. § 155.210(c)(1); *id.* § 155.210(c)(2) (directing the Exchange to select at least two different types of entities as navigators, one of which must be a community and consumer-focused non-profit group). In practice, non-profit groups are anticipated to take a much greater role, and may be the main source for enrollment assistance. Yet your agency's requirements might bar states from imposing any comparable certification and licensing requirements, such as surety bonds and acts and omissions insurance, on non-profit navigator groups who are not licensed agents or brokers. 78 Fed. Reg. 42831 (stating that the "requirement by a state or an Exchange that Navigators be agents and brokers or obtain errors and omissions coverage would prevent the application of the requirement at § 155.210(c)(2) that at least two types of entities must serve as Navigators, because it would mean that only agents or brokers could be Navigators").

Your guidelines are also less demanding than many federal privacy requirements, such as those applicable to federal census workers and those that the Department of Treasury would like to apply to professional tax preparers. Census Bureau employees take an oath for life to protect identifiable information and information about businesses gathered by the agency. By law, the Census Bureau cannot share respondents' answers with the IRS, FBI, CIA, or any other government agency. The penalty for unlawful disclosure is a fine of up to $250,000 or imprisonment of up to 5 years, or both. Separately, since 2009, the Department of Treasury has aggressively pursued reforms to ensure comprehensive oversight of tax professionals including registration of individual preparers, background checks, certification, competency examinations, and continuing education requirements. Your agency's guidance regarding navigators and other assisters is not remotely comparable.

Finally, the lack of standardized background checks in the Rule pales in comparison to what is usually required for employees in programs receiving federal healthcare funds, particularly with respect to high-risk employees with direct access to consumers. For example, the Centers for Medicare & Medicaid Services has worked with twenty-four states to design comprehensive national background check programs for employees in long-term care facilities with direct patient access. Likewise, in other rules promulgated by your agency, heightened screening, fingerprinting, and background check requirements apply to high-risk providers seeking to participate in Medicare, Medicaid, and the Children's Health Insurance Program. *See* 76 Fed. Reg. 5862.

Further Work Is Required

It is not enough simply to adopt vague policies against fraud. HHS will be giving its stamp of approval to every counselor who interacts with a consumer. This position of trust will allow counselors to gain access to a wide variety of personal information from unsuspecting consumers. Unscrupulous counselors, who are not properly screened out or supervised, will have easy means to commit identity theft on consumers seeking enrollment assistance. According to the Bureau of Justice Statistics, more than five percent of adults already fall victim to identity theft each year, and that is before they hand over all their individual data to a minimally screened and virtually unaccountable "counselor." HHS needs on-the-ground plans to secure consumer information, to follow up on complaints, and to work with law enforcement officials to prosecute bad counselors. Without more protections, this is a privacy disaster waiting to happen.

In the questions below, we have identified a number of areas that we believe are critical to ensuring effective safeguards for the protection of consumers' private data through the navigator, assister, application counselor, or other consumer outreach programs. We ask that you please provide answers to the following questions in writing. Our hope is to work with you to better assess the state of health insurance consumers' data protection and to evaluate the role, if any, for state regulatory action.

1. **Screening Personnel.** Beyond the general grant screening process, does the process for hiring personnel include any screening for staff that may pose risks to consumer data privacy? For example:
    a. Will HHS or others require that all navigators or similar personnel have an educational degree or have any past experience or expertise in the health insurance field or data privacy?
    b. Will HHS or others require uniform criminal background checks or credit reports?
    c. Will certain individuals, such as those who have committed identity theft, be prohibited from becoming a navigator or other program personnel?
2. **Guidance to Program Personnel.** What forms of guidance will HHS provide to program personnel about consumer data privacy protections?
    a. For example, will navigators that receive taxpayer return information be advised of their potential criminal liability, under section 7213(a) of the Internal Revenue Code, for unauthorized disclosure of such information?
    b. Please identify the specific existing laws and standards that HHS believes govern the use of consumers' information and which HHS will expect navigator, assister, application counselor, or other consumer outreach programs to follow.

3. **Monitoring Program Personnel.** How will HHS or others oversee the activities of navigators and non-navigator assistance personnel and ensure that employees do not retain personal information?
4. **Notice to Consumers.** Will consumer outreach programs inform consumers of their data privacy rights and the programs' liability before they decide to receive assistance?
5. **Liability.** Where does liability rest when a consumer outreach program causes harm to a consumer, either purposefully or unintentionally, through the misuse of personal information?
    a. Specifically, does liability rest with the individual who had direct consumer contact, the entity that received funds for consumer outreach, or the exchanges?
    b. Does HHS plan to require that entities that receive federal or exchange-generated funds for consumer outreach activities carry any sort of professional liability insurance?
6. **Fraud Prevention and Remedies.** Does HHS have any plans to provide assistance and relief to defrauded consumers?
    a. Will programs be required to aid consumers who believe information provided to a program has been misused?
    b. How does HHS plan to prevent potential fraud by entities and individuals that may disingenuously represent themselves as navigators or other assisters to unsuspecting consumers?
7. **Penalties.** HHS has promised to take "appropriate action if complaints of fraud and abuse arise."
    a. Beyond civil monetary penalties, what other "appropriate action" will your agency take?
    b. Beyond the False Claims Act, what other existing statutes providing for penalties will apply?
8. **Supplemental State Regulation.** How do you view the role of states with regard to supplementing federal data privacy requirements in all three types of exchanges? Many states have enacted or are considering legislation that further regulates navigators.
    a. Has HHS informed any state that a proposed or adopted state requirement is inconsistent with federal rules? If yes, please provide an exhaustive list of such requirements.
    b. To what extent will states be able to impose additional certification requirements and safeguards relating to a program's data privacy operations, at levels comparable to the licensing of agents and brokers, without being in conflict with the Act?
    c. What is your understanding of the minimum insurance and bonding requirements that states could impose on non-profit programs?

d. How does HHS plan to inform state regulators about which entities and individuals may be performing federally-funded, out-of-state consumer outreach activities in their states, so that they will be aware of who may be interacting with their constituents and may enforce state-based consumer protection requirements?

We appreciate your prompt attention to these critical questions and request a response by August 28, 2013.

Sincerely,

Patrick Morrisey
West Virginia Attorney General

James D. "Buddy" Caldwell
Louisiana Attorney General

Luther Strange
Alabama Attorney General

Bill Schuette
Michigan Attorney General

Pamela Jo Bondi
Florida Attorney General

Tim Fox
Montana Attorney General

Samuel S. Olens
Georgia Attorney General

Jon Bruning
Nebraska Attorney General

Derek Schmidt
Kansas Attorney General

Wayne Stenehjem
North Dakota Attorney General

E. Scott Pruitt
Oklahoma Attorney General

Greg Abbott
Texas Attorney General

Alan Wilson
South Carolina Attorney General