April 1, 2015

Karen B. DeSalvo, MD, MPH, MSc
National Coordinator for Health Information Technology
HHS/Office of the National Coordinator for Health IT
200 Independence Avenue S.W.; Suite 729-D
Washington, D.C. 20201

**RE: Connecting Health and Care for the Nation: A Shared Nationwide Interoperability Roadmap**

*[Comments submitted electronically via http://www.healthit.gov]*

Dear Dr. DeSalvo,

TASCET appreciates the opportunity to comment on *Connecting Health and Care for the Nation: A Shared Nationwide Interoperability Roadmap*. TASCET is a digital enterprise risk company providing software for the unique identification of individuals. We focus on the technology and processes needed to ensure individuals are not attributed to multiple identities, whether as a result of human error or an attempt at identity fraud.

I and my colleagues have served on numerous industry and government working groups and project teams tackling the challenges of identity and privacy, including the American National Standards Institute (ANSI) Identity Theft Prevention and Identity Management Standards Panel and the Financial Services Technology Consortium/BITS Identification Project. We have prepared numerous briefing documents for government and industry outlining the flaws in existing credentialing and identity verification programs. I presently serve on the board of the Center for Information Management and Identity Protection.

As such, my comments address those sections of the Roadmap that relate to patient and provider identification, patient matching and the privacy and security of health information.

**Regarding Section F: Verifiable Identity and Authentication of all Participants (page 58)**

1. The third paragraph of “Background and Current State” (page 58-59) implies that documents including driver’s licenses, passports, utility bills, financial records or the patient’s health plan card are acceptable forms of ‘identification’ for establishing that a person is who they say they are (identity proofing).

   Nothing could be further from the truth.

   Documents and information do not identify. Bank records, utility bills and health plan cards are easily forged, stolen, purchased and shared. Valid driver’s licenses and passports are fraudulently obtained on a daily basis by individuals presenting falsified and stolen birth certificates; and through weak document issuance processes, internal fraud, and the ability to spoof electronic verification systems.

   The crux of the problem is that the credentials suggested for identity proofing were never intended to identify individuals. They are records that verify the privilege to drive or travel internationally and, according to the 9/11 Commission, do not contain the characteristics needed to identify individuals.[i] The documents may be valid, but it is not possible to confirm that the presenter is the individual who owns that identity.

Just last year – in July 2014 – the Government Accountability Office (GAO) testified on Capitol Hill that its investigation of the Patient Protection and Affordable Care Act (PPACA) enrollment revealed that there were virtually no obstacles to the use of counterfeit identification documents for enrollment.[ii]

Relying on documents for identity will threaten the integrity of health system databases and undermine the nationwide exchange of EHRs.

2. The fifth paragraph (page 59) refers to OMB M-04-04 as an e-authentication requirement for federal agencies, with NIST 800-63-2 providing technical guidance for levels of assurance (LOA) for identity proofing. The Roadmap indicates that at the time of its printing, the health care industry had not standardized its LOA requirements for identity proofing.

   Nor should it.

   NIST 800-63 guidance was written for the remote authentication of a closed group of users (employees, contractors and private individuals) interacting with government IT systems over open networks. In no way does this application describe the broad group of users (patients, providers, organizational representatives and other authorized individuals) or the variety of devices used to access diverse health systems, networks and protected health information.

   NIST's four levels of identity assurance date back to 2003, and were based on the technology and practices available at that time. NIST 800-63 was also written before massive data breaches made the information to be used for identity proofing readily available for use in identity fraud.

   Today the four levels are described as "out of touch" and criticized for their inability to scale to industries outside of government.[iii] NIST and industry groups agree that the current model for determining identity and authentication assurance needs to be revisited.

   ONC should be extremely cautious in referencing recommendations that are intended for accessing federally controlled systems in a Roadmap for an industry made up of such varied and independent organizations. Any solution referenced by ONC must be hardware and EHR vendor agnostic and must not result in more 'silos' of information that enable fraud and inaccuracies.

3. Paragraph six notes the lack of consistent identity proofing and authentication across organizations. The Roadmap also suggests that in a learning health system, providers and hospitals should exchange only with others who are 'appropriately identity proofed and authenticated'. Paragraph seven focuses on HITPC's recommendation for multi-factor authentication.

   Establishing requirements for identity proofing and authentication is vital to successful exchange and patient safety and privacy. However, the recommendations within the Roadmap are flawed. The identity proofing process described is incorrectly based on the presentation and verification of documents and information and will lead to risks in patient safety and privacy, the contamination of health system databases, and fraud.

   NIST defines identity as "the set of physical characteristics by which an individual is uniquely recognizable," and identification as "the process of discovering the true identity of a person from the entire collection of similar persons."[iv] Individuals are not uniquely recognizable by documents that can be fraudulently obtained and easily shared, stolen and forged. Nor are they 'identified' by information that is readily available as a result of data breaches, the data mining practices of data brokers, and the posting of personal information on social networking sites.

   Any discussion of identity proofing (identification) must center on the use of physical characteristics, not on information and documents.

4. Paragraph eight references the work done as part of the National Strategy for Trusted Identities in Cyberspace (NSTIC) initiative. NSTIC is evaluating the re-use of third party credentials for authentication that have been issued to individuals based on the verification of information. Information-based verification tools match the biographics presented by an individual against the biographics stored by data brokers including Lexis Nexis and Kroll and credit bureaus such as Experian. Regardless of what is verified, e.g. name, address, phone number, previous addresses or Social Security number, biographic information is not linked to an individual and is therefore easily presented by someone other than the rightful owner. The outcome is verified information, not verified identities.

   Bank accounts are taken over every second of every day because the financial industry relies on these same verification practices. Financial institutions have tens of millions of synthetic identities in their databases. Identity fraud and the losses to investigation and remediation mount in the billions. Just as is being seen in healthcare, recent shortcomings by banks to protect consumer information and the integrity of databases are leading to more regulatory oversight and higher penalties.

   There may have been a time when relying on information and documents for identity processes was acceptable. But in today’s digital environment, in which identity fraud is rampant and data breaches are epidemic, that time is gone. Relying on information and documents now is both illogical and highly risky. ONC should not reconcile its recommendations for provider authentication with approaches being encouraged by NSTIC.

5. Finally, the paragraphs entitled “Moving Forward” suggests that mobile devices may one day be used to identity proof and authenticate a patient at the point of care. Mobile devices are already used to authenticate individuals in numerous ways, but it is important to note within the Roadmap that authentication can never be a starting place for securing access to patient information. There must be an initial identity proofing process utilizing the characteristics required for identification. This step must ensure that an individual is not attributed to more than one identity. Mobile devices may be linked to an individual after the person is uniquely identified in order to facilitate authentication, but these devices cannot be used to identify (or identity proof) an individual.

**Regarding Section M: Accurate Individual Data Matching (page 90)**

The Roadmap recognizes that there is a significant near-term need to focus on patient identity matching, including improving patient matching processes and standardizing data elements.

Patient matching within and across health systems and exchange networks will only be corrected by implementing a standard patient identification process that does not rely on the use of information and documents that are easily shared, stolen, purchased and forged. Patient matching also cannot be based solely on data elements that can be incorrectly entered or fraudulently presented, including those listed on page 93, i.e. name, date of birth, address, phone number, etc. The reliance on biographic data elements has already resulted in tremendous inaccuracies within patient matching. Simply standardizing their order will not make them any less vulnerable to errors, inconsistencies and fraud.

Instead, the category of data elements must be broadened to include physical characteristics such as face and finger, which cannot be used by others, to uniquely identify individuals and enable the safe, accurate and consistent matching of patients to their records.

**Final Comments**

Any efforts to standardize patient identification and patient matching processes must also protect the privacy of patients and protected health information. It may seem that this point can be left unsaid, yet the processes for identity proofing and authentication referenced within the Roadmap are based on the capture, storage, analysis and sale of vast amounts of personal information. These approaches do not protect privacy. Instead, they have led to a burgeoning industry of data brokers and created a privacy-security paradox, in which one must be sacrificed to get the other.

Data breaches have become epidemic because the information stored within patient and customer databases is the key to opening bank accounts, obtaining false credentials and receiving medical care. The recent Anthem data breach resulted in the loss of Social Security numbers for 79 million individuals. By now these numbers have been sold, resold and will be used to create synthetic identities (the use of valid Social Security numbers with false name and address) that will soon weave their way into our nation’s medical information systems, threaten patient safety, and undermine the goal of interoperability.

Medical records are highly valuable in criminal exchanges because the information is not only highly confidential, but is used in in-depth medical and insurance fraud. Criminals can impersonate patients to obtain prescriptions for controlled substances and use the data for financial fraud. Health information is also combined with other data to create complete ‘packages’ of identity information that sell for $1,000 or more. If the processes used to identify and authenticate patients continue to be based on this information, breaches will become even more commonplace, placing patients, providers and health organizations at significant risk.

The foundation for successful interoperability of electronic health records is the accurate, secure and confidential identification of patients and healthcare professionals. Broken identity processes threaten the goals of interoperability and, by enabling errors and fraud, will contaminate the nationwide EHR system.

Thank you for the opportunity to comment. I would be happy to discuss this in more detail and work with ONC and other industry stakeholders on these issues. My staff and I are interested in participating on committees and working groups, and our technology and software is available for demonstration projects of any scale and scope.

Please contact me or Kari Douglas at any time. My email is laubol@tascet.com; Kari’s email is kdouglas@tascet.com. We can both be reached at 608.442.8888.

Sincerely,

Larry Aubol

Larry Aubol, CEO

[i] 9/11 Commission. “The 9/11 Commission Report, Final Report of the National Commission on Terrorist Attacks Upon the United States.”
[ii] Government Accountability Office. “Patient Protection and Affordable Care Act, Preliminary Results of Undercover Testing of Enrollment Controls for Health Care Coverage and Consumer Subsidies Provided Under the Act.” GAO-14-705T. July 2014.
[iii] Martin, Zack. “End of life for fed’s four levels of assurance?” Secure ID News, January 5, 2015.
[iv] National Institute of Standards and Technology, “Federal Information Processing Standard Publication 201” (FIPS-201).