Dr. Karen DeSalvo

National Coordinator for Health Information Technology  
Acting Assistant Secretary for Health  
U.S. Department of Health and Human Services  
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; DRAFT Version 1.0"**

Dear Dr. DeSalvo:

Imprivata is an international expert in healthcare IT security. Our authentication, access management, and secure communications solutions are used by more than 1,200 healthcare organizations and 3 million end-users globally. Imprivata’s products deliver fast, secure access to clinical applications and patient information, saving providers significant time to focus on the patient care, increasing their productivity and satisfaction, and helping healthcare organizations comply with privacy and security regulations.

Our flagship product, Imprivata OneSign®, offers single sign-on (SSO) and authentication management to eliminate manual login processes and deliver fast, secure access to EMRs, other clinical applications, and patient records at the point of care. According to HIMSS Analytics data, Imprivata has the highest SSO market share amongst U.S. hospitals, at 34 percent.

Imprivata Cortext® is our secure communications platform for healthcare, enabling more efficient, secure, and reliable communication between providers both inside and outside the hospital using smartphones, tablets, and desktops. Imprivata Cortext improves communication and care coordination by reducing the dependence on pagers and other outdated technologies.

Imprivata Confirm ID™ is our fast, secure EPCS solution, delivering a single, integrated platform for provider identity-proofing, supervised credential enrollment, and two-factor authentication. Imprivata Confirm ID supports multiple DEA-approved, two-factor authentication modalities and integrates with leading EHR and e-prescribing applications to give providers a fast, secure, and convenient prescribing experience across all systems.

We are committed to openness and interoperability as essential elements to realizing technology’s promise to improve healthcare efficiency, patient outcomes and the overall health of our population. Through access to Application Programming Interfaces (APIs), documentation, test and certification tools, the Imprivata Developer Program allows software and hardware solution providers to seamlessly integrate our authentication and secure communications capabilities within their applications and across a broad set of devices.

**General Comments to "Connecting Health and Care for the Nation, A Shared Nationwide Interoperability Roadmap; DRAFT Version 1.0"**

We applaud the ONC for developing the interoperability roadmap. Over the last few years, billions of dollars have been spent in the development of our electronic health records system. Until we have a guide in place, we will not be able to fully realize the potential of this revolution. We agree with the ONC that interoperability of healthcare IT systems and the secure, efficient sharing of electronic health information are important to improving patient care and reducing healthcare costs. The ONC’s “Roadmap” provides the vision and framework to realize this potential. We are grateful for the opportunity to provide insight and comment.

As a general matter, Imprivata strongly recommends that the ONC continues to consider the importance of security and data protection, as critical to the success of interoperability. The bi-directional flow of information between healthcare organizations and, in time, between patients and care providers relies on the integrity of health information. This can only be accomplished if the proper security policies, process, and technology measures are integrated at each step in the process – and if those security measures do not interrupt clinical workflows.

For interoperability to succeed on a broad scale, the entire healthcare community—including patients, care providers, hospital administration, policymakers, payers, and technology vendors—must be assured of the authenticity and validity of the information itself, as well as the identity of the individuals accessing and sharing the data.

**Specific Comments to "Connecting Health and Care for the Nation, A Shared Nationwide Interoperability Roadmap; DRAFT Version 1.0"**

1. **Proposed addition of EPCS (Electronic Prescription of Controlled Substances) as a “prioritized workflow".**

The current draft of the *Roadmap* presents a call to action (in Table row D.4):  "e-prescribing of controlled substances with concurrent availability of PDMP data”.  We applaud this goal as an essential part of increasing patient safety and public health.

We are, however, concerned that this call-to-action, as presently written, could inadvertently delay the broad adoption of EPCS by causing providers to wait until PDMP-based workflows are developed before adopting EPCS.

As is eloquently described in Appendix F of the *Roadmap*, the use of EPCS -- even in the absence of PDMP -- significantly reduces abuse, and acceptable workflows that enable its adoption today are available.  Further, the broad adoption of EPCS will result in more complete and reliable PDMP data.  On the other hand, we believe that the development of PDMP-based workflows that put the prescribing physician in an enforcement role will take longer.  Such workflows will need to go beyond the technical challenge. They will require the resolution of sociological and ethical issues in balancing patient-doctor trust with the wishes of law enforcement.

We therefore propose that the current call-to-action:

* E-prescribing of controlled substances with concurrent availability of PDMP data

be replaced with two calls to action along the following lines:

1. E-prescribing of controlled substances (EPCS) with integrated reporting to PDMP systems.
2. Availability of PDMP data when e-prescribing controlled substances.

We also propose that “EPCS” be added to the glossary.

2. **Section M (Accurate identity Matching):  Motivate use of authentication data in matching.**

We believe that the use of authentication data, including biometrics, has the potential to improve the accuracy of matching by several orders of magnitude.  We also believe that the availability of such data will increase as identity proofing of patients becomes more prevalent as proposed in section F of this Roadmap.  The roadmap appears to agree, as evidenced by critical action M2.3 ("ONC will coordinate with industry stakeholders to study voluntary collection of additional identity attributes …”), but there is no introductory text motivating that action.

In fact, the current draft seems to dismiss authentication as being distinct from identity matching (“*Identity matching should not be confused with authentication*”) and by implication, not relevant.  To dispel that implication and to be consistent with the critical actions suggested in table row M2, we propose that Section M, “Moving Forward and Critical Actions” be enhanced.  We propose inserting as the second paragraph the following text:

*We must use all means available to improve the accuracy of matching.  To that end, it may be fruitful to study the use of authentication data in the matching process.  As we move forward, patients will acquire “proven” identities that can be securely attached to biometric or other identifying data.  It is important to study the use of authentication data in the matching process as it could, when available, improve the matching accuracy by orders of magnitude.*

Again, we agree with the intent and mission of ONC’s “Roadmap”. As this proposal is fleshed out and implemented, Imprivata stands ready to help in any way toward our common mission of making health data safe, secure, and usable.

Sincerely,

Sean Kelly, MD, FACEP

Chief Medical Officer, Imprivata