

April 2, 2015

The Honorable Karen DeSalvo, M.D., M.P.H., M.Sc.
Office of the National Coordinator for Health Information Technology
Department of Health and Human Services
200 Independence Ave., SW
Washington, DC 20201

ELECTRONICALLY SUBMITTED TO: www.healthit.gov/interoperability

RE: Comments on "Connecting Health and Care for the Nation A Shared Nationwide Interoperability Roadmap DRAFT Version 1.0"

Dear Dr. DeSalvo:

IMS Health applauds your outreach for comment and input on "Connecting Health and Care for the Nation, A Shared Nationwide Interoperability Roadmap, DRAFT Version 1.0". This outreach provides an opportunity for private industry, government agencies, thought leaders, experts and law-makers to help identify key issues, policy work and legislative changes that can lead to innovative and effective data interoperability in our health care system. Your focus and policy work on health care data initiates a vital discussion that is fundamental to transforming health care to an evidence-guided, information-based system, which is the very focus of IMS Health's business.

As a global leader in information solutions, IMS Health is an international expert in health information stewardship — including privacy and data protection. We firmly believe that:

- Data accuracy, validity and interoperability are essential for data to be useful, trusted and lead to health care improvement;
- Health information used wisely and responsibly advances health care globally and offers real value for patients, payers and providers of health care, and;
- Data must be securely stored and patient privacy must be preserved and protected.

Since our founding more than 60 years ago, IMS Health has pioneered practices to de-identify individual patients' sensitive data, while serving a broad array of health stakeholders, including the FDA and other agencies of the U.S. Department of Health and Human Services. IMS Health relies on a combination of resources, policies and practices to ensure the leadership and expertise necessary to manage information in a manner that balances vital societal values, including improved health care and patient privacy.

To develop and advance important resources and practices for data security and privacy, IMS Health works collaboratively with businesses, information security, and technology experts to develop trust and security frameworks that promote excellent data stewardship. In particular, IMS Health works with HITRUST as well as with NIST in development of collaborative expert technical standard frameworks for data interoperability and data security. Both organizations (one private and one public) offer excellent examples for the

self-regulatory, open standard governance models goals of the current Health Interoperability Roadmap. We urge ONC to highlight and cite both HITRUST and NIST for leading the way with public-private sector collaborative security and cyber-security frameworks. Our comments focus, in particular, on the important role of HITRUST and suggest HITRUST as an important example to note for both a governance model and for its work on health information privacy and security.

As you proceed with your consideration of data and information policy, we would like to emphasize the need to identify as examples the excellent collaborative, technical work to create frameworks. HITRUST offers one important example of industry bringing together its experts to create a collaborative framework that is widely and broadly available, in this case for health data security and for information sharing on cyber-threats. We offer the following specific comments:

- Secure Network Infrastructure (page 57): We believe that these activities and goals should incorporate the HITRUST Common Security Framework (CSF) and HITRUST Cyber-threat Exchange (CTX) **as one example** of industry self-regulatory standard setting that is widely available to assist HIPAA covered entities. The HITRUST CSF incorporates relevant federal and state regulation, and International and US standards such as NIST, ISO, PCI while adding the health care industry context and specifications. As is the case with the HITRUST CSF providing a healthcare industry implementation of the NIST Cyber Security Framework, which is fully incorporated into the HITRUST CSF.
- Consistent Representation of Authorization to Access Data or Services (page 73): We support conduct of listening sessions and stakeholder input processes. Authorization, consent and access to data is complex both with regards to standards as well as for patient understanding and expectations for data and for health system performance.

Health care information must be handled with the utmost care. Balancing patient privacy, data interoperability, data accuracy, proprietary concerns and demand for transparency for data-driven health care analytics is a delicate, resource-intensive task. Yet it is a task that is at the heart of good data stewardship and that is required of entities engaged in the trusted exchange of health information. In the long run, proper data practices and excellent stewardship will lead to strong and long-standing data practices that will support and enhance patient care in this nation.

Respectfully submitted,



Kimberly S. Gray, Esq., CIPP/US
Chief Privacy Officer, Global
IMS Health
Direct: 484.567.6045
Email: kgray@us.imshealth.com