April 3, 2015

Karen DeSalvo, MD, MPH, MSc
National Coordinator for Health Information Technology
The Office of the National Coordinator for Health Information Technology
U.S. Department of Health and Human Services
200 Independence Avenue S.W.
Suite 729-D
Washington, D.C. 20201

Re: Intel's Comments on the Department of Health and Human Services ONC Draft Interoperability Roadmap

Dear Dr. DeSalvo:

Intel Corporation (Intel) appreciates the opportunity to comment regarding *Connecting Health Care for the Nation, A Shared Nationwide Interoperability Roadmap* (the Roadmap). We commend the Office of the National Coordinator for Health Information Technology (ONC) for developing a plan focused on ensuring interoperability between health care providers and stakeholders, and we look forward to working with ONC to achieve the goals that Congress and the Department of Health and Human Services (HHS) have established for our nation's health care system.

Moreover, we are pleased with the Roadmap's emphasis on testing and certification programs, shared governance of interoperability standards, and privacy and security protections. ONC's plan and recommendations are well structured and progressive.

Below is a summary of our comments:

1. **Timing:** Many have criticized the roadmap's timeframe as unhelpfully long. We have experienced firsthand the importance of data sharing, patient engagement, and the barriers today that prevent the execution of the goals for interoperability. We believe the timeframes in the Roadmap can be condensed into the 2015 to 2020 period without negative consequences. We encourage ONC to be more aggressive in pursuing interoperability more rapidly.

2. **Testing and Certification:** Certification programs should leverage proven test cases instead of relying on published Certification Test Cases by Agencies. We support the theory of testing early and testing often by incorporating better testing approaches into EHR vendor standard development lifecycles.

3. **Standardization of Data Elements:** Structured data and standardized vocabulary should be utilized to the fullest extent possible in order to move toward greater semantic operability and to enable more comprehensive patient records that support better analytics and clinical decision support.

4. **Shared Governance of Interoperability Standards:** Other than stating that standards development and adoption should not unfairly provide an advantage to one sector or one organization over others, the Roadmap fails to elaborate on how to achieve that goal.

5. **Patient Generated Health Data and Personalized Care:** Patient-generated data is essential for a fully comprehensive patient record, and should therefore be required for EHR integration. EHRs should be required to demonstrate compliance with open industry standards for interoperability for remote patient monitoring equipment and devices. Additionally, target goals should be established for remote patient monitoring for patients with one or more high-priority conditions.

6. **CDS Integration:** Intel supports additional requirements for CDS to be integrated into health records that are tied to consistent and streamlined quality metrics that can be reported electronically.

7. **Privacy and Security Protection:** Privacy and security should be addressed in a holistic approach, accounting for policy, risk assessment, procedure, training, and technology. This approach considers the privacy and security protection requirements of large scale networks consisting of a variety of different type of clients, network components, and servers. Since security is only as strong as the weakest link, it is crucial that the entirety of all network infrastructures are secured across different types of clients, network components, and servers. Only through effective end to end security can we ensure there are no weak links or vulnerabilities that could be exploited, for example, by cybercrime.

Intel and Health Care

Intel is a world leader in silicon innovation, but we, and our 500+ subsidiaries, are active health care arena participants, both directly and indirectly. Our technologies power the internet and the broadband-connected world, and our global institutions increasingly work to connect patients, families, providers, and health care researchers with one another. For over a decade, we have focused our research and development efforts specifically on health care in order to better understand how to connect all major health care players through a wide variety of health information technologies. Intel has studied over 1,000 patient homes and 250 hospitals and clinics in over 20 countries in order to develop products and solutions and help create a connected world for health care.

Intel technologists and architects have advised and led health IT and standards efforts to create what we call "solution blueprints" for health care entities in many parts of the world. Intel helped build the National Health Information Backbone (Spine) and N3 in the United Kingdom. Intel has worked with regional and national health exchange efforts such as Health Infoway in Canada and Regional Health Information Network (RHIN) in China. Intel was invited to serve as the non-voting technical advisor to the recently formed Open Data Center Alliance, a consortium of over 300 global organizations that have come together to help make the vision of cloud computing a reality for health care and other industries.

Intel also submits these comments from the perspective of an employer providing health care benefits to more than 100,000 employees worldwide, and 127,000 covered lives in the United States alone. In 2011, we spent $1 billion on employee and dependent benefits worldwide in order to fulfill our commitment to providing comprehensive, cost-effective coverage for those in our employ and their families. We were an early adopter of biometrics for wellness in 2006, and took the bold step of establishing an employer-based accountable care organization in New Mexico and medical health homes in Oregon in 2013. We founded Dossia with seven other Fortune 500 companies in 2006 in order to offer employees free personal health records populated with data from insurers and providers, as we know firsthand the importance of data sharing and the barriers that prevent interoperability.

Within the structure of the Roadmap, Intel looks to ONC to include the following:

I. Timing

We have experienced firsthand the importance of data sharing, patient engagement, and the barriers today that prevent the execution of the goals for interoperability. We are pleased to see the Roadmap's emphasis on interoperability. We believe ONC can and should standardize vocabulary and data elements and foster open standards under a workable architecture more rapidly than the timeline outlined in the Roadmap. We are concerned that a ten year plan for a learning health system is too prolonged and would leave US health care interoperability behind most other industries and countries.

II. Testing and Certification

Certification programs should leverage proven, real-world test cases, instead of relying on published Certification Test Cases by Agencies. We believe that a mature certification program will publish, in draft form, a series of test cases that industry will have an opportunity to vet or test out within their respective systems, allowing industry an opportunity to report back on the maturity (status) of support and identify any potential challenges which may exist within the use cases.

This proposed approach of introducing test cases early to industry and providing an opportunity for feedback will likely avoid potentially difficult situations. We are concerned that certification based test cases could be released that a limited (or a very few) set of EHR vendors may be able to meet, providing those few with a significant market advantage. Later, under increased public pressure, the certification body may try to relax some of the published testing requirements (potentially deemed too difficult), which could result in swings between too strict and too loose that would generate confusing market signals.

Organizations such as Gartner, AMA, and others have spoken to the lack of negative testing within health IT implementations as an industry-wide issue. Our concern is that ONC, in an effort to address "negative" or "exception" test cases, will introduce a sprinkling of negative test cases across the Certification Testing Program. We urge ONC to more clearly define the objective, rationale, and desirability of supporting "Negative" and "Exception" type testing.

Additionally, we support the theory of testing early and testing often by incorporating better testing approaches into EHR vendor standard development life cycles. In accordance with wide agreement that interoperability will be best reached via industry standards, individual organizations should not develop unique individual approaches to testing. Uniform, industry-wide standards are preferable. Where appropriate, EHR testing should use standards based on a shared services testing platform, leveraged by the community at large. The best methodology would be to implement a cloud based testing service to improve access and testing uniformity.

III. Standardization of Data Elements

Structured data and standardized vocabulary should be utilized to the fullest extent possible in order to move toward greater semantic and syntactic interoperability and to enable more comprehensive patient records that support better analytics and clinical decision support. Expanding structured data to fields such as family history would allow for a more comprehensive approach that includes the use of policy, risk assessments, procedure training, and technology. We believe this is where ONC should accelerate its timeframe significantly. We urge ONC to build into its Roadmap, strategic and tactical planning, and policy development the following:

- **Leverage existing standards work and iterate from existing baseline.** In accordance with ONC's desire to work and engage with industry, we encourage collaboration with established industry best practices and proven capabilities.

- **Require software vendors to certify consistent adoption.** We suggest requiring EHR vendors to produce a CCDA that has corresponding sections populated and encoded, and establish a robust certification process to demonstrate consistent adoption.

IV. Shared Governance of Interoperability Standards.

Other than stating that standards development and adoption should not unfairly provide an advantage to one sector or one organization over others, the Roadmap fails to adequately elaborate on the matter of reasonable and non-discriminatory access to standards.

While we appreciate ONC's focus on some of these goals in the Roadmap, we are concerned that the Agency has placed too much emphasis on strategies and not enough on the specifics of implementation. ONC should encourage development of the tools that will empower providers to be successful in delivering highly effective and efficient health care. Specifically, we believe the Roadmap focuses too much on broad concepts that are not actionable in the near-term.

For example, will there be consideration for any backward compatibility assurances? While we understand that there must be a balance between evolving with the industry, we urge ONC to consider that updates necessary for evolving technologies will not undermine standards of the system that will eventually be in place.

Further, will interoperability standards have certification programs associated with them to give an extra level of assurance? This will require examination of the list of interoperability standards themselves, with an understanding that the standards will have to be narrowly tailored or broadly

construed in certain instances.

V. Patient Generated Health Data and Personalized Care

Patient-generated data is essential for a fully comprehensive patient record, and should therefore be required for EHR integration. EHRs should be required to demonstrate compliance with open industry standards for interoperability for remote patient monitoring equipment and devices.

Additionally, target goals should be established for remote patient monitoring for patients with one or more high-priority conditions. The incorporation of patient-generated health data for EHR integration requires the addition of meta-data about data provenance (identifying which device was used, firmware level at capture, the device's certifications, modifications made to the data through the data flow, etc.).

EHRs should integrate with remote patient monitoring because clinical evidence demonstrates that it can improve care, particularly for the chronically ill, in ways that reduce hospitalization and complications while improving satisfaction. Additionally, EHRs should use open industry standards to ensure interoperability of patient generated health data.

The following highlight specific areas we believe ONC should focus its efforts on patient-centered health:

- **A Patient-Centered Learning Health System**. The Roadmap suggests that individuals should demand access to health information in a patient-centered learning health system (See Table 3). However, the Roadmap fails delineate any incentives for individuals to demand such access. We believe ONC should explore such incentives, and such incentives should be the focus of subsequent ONC-patient-industry discussions. In the short term, we suggest ONC adopt a consistent interoperable formant to ensure individuals will be able to demand access to health information through a single source.

- **Standardization.** Ultimately, a patient-centered learning health system should reduce the number of options for data formats in order to gain interoperability. ONC should develop a feedback mechanism that routes to the standards organizations. Such a mechanism is necessary in order effectively work towards reaching desired standards more effectively and efficiently.

- **Patient-Centered Learning Health System, Privacy and Security for Individuals**. Undoubtedly, individual trust in the privacy and information security of a learning health system is paramount to promoting information sharing. Following industry best practices along with device certification will ensure data is secure both when it is in transit and at rest.

VI. CDS Integration

Intel supports additional requirements for CDS to be integrated into health records that are tied to consistent and streamlined quality metrics within a defined scope. The following is a current

valid use case from Intel's award-winning Connected Care program. This case demonstrates the advantages of full CDS integration in the form of push/pull information exchange, illustrated by the eventual addition of Intel's Onsite Health For Life Center (HFLC) vendor and their Greenway EMR and local Connected Care Delivery System Partners (DSP) on Epic EMR via Healtheway, an information exchange platform. This business use case example highlights how information technology, through streamlined quality metrics, will provide optimal push/pull interoperability within systems and will allow for better information exchange within provider institutions, across different providers, and ultimately with patients.

Pull

- Onsite HFLC providers/staff will be able to manually pull a Connected Care DSP member's CCD from the Epic EMR through Epic Care Everywhere via the Healtheway platform.

    - *Sample Use Case*: Jennifer, an Intel employee, visits the Health for Life Center for an upper respiratory infection. The HFLC staff learns that Jennifer is a DSP Connected Care member during the intake process and informs the provider and staff member who will be seeing her. The HFLC provider or staff member uses the data exchange to pull Jennifer's CCD from DSP's Epic EMR system to better inform the interaction with Jennifer, address any issues or gaps in her care, and coordinate with her primary care provider as appropriate.

- DSP providers/staff will be able to manually pull a DSP Connected Care patient's CCD from HFLC Greenway EMR via Healtheway.

    - *Sample Use Case:* Jack, a DSP Connected Care member, visits a Connected Care primary care provider (Dr. Barich) for the first time to establish as a new patient. Jack tells Dr. Barich that he has been seeing a provider at Intel's Health for Life Center for his primary care in the past. A member of Dr. Barich's care team uses the data exchange to pull Jack's CCD from HFLC Greenway EMR system to view the health information captured on Jack during his previous HFLC visits, and attach it to his Epic record.

Push

- HFLC providers/staff will be able to manually push secure messages from the Greenway EMR via the Up Docs messaging platform to a DSP designated mailbox (DSP will monitor this mailbox for messages and triage them appropriately).

    - *Sample Use Case:* David, a 55 year old Intel employee, visits the Health for Life Center for a skin rash. The HFLC staff learns that David is a Connected Care member during the intake process and informs the provider and staff member who will be seeing him. The HFLC provider or staff member also learns he has a regular primary care physician (Dr. Barich) at the DSP local clinic. The HFLC provider or staff member uses the data exchange to pull David's CCD from DSP's

Epic EMR system. As part of the visit, David's weight and blood pressure are taken and both are on the high side. He also has a family history of heart disease. After the visit, the HFLC provider or staff member sends a secure message through the platform to Connected Care DSP about David's visit and that his weight and blood pressure results were high, recommending follow-up with his primary care physician. The DSP's care team member retrieves the message and pulls David's CCD from HFLC's Greenway EMR. The care team member attaches the CCD to his DSP Epic record, notifies Dr. Barich of David's recent visit to the HFLC and the HFLC provider/staff's message, and helps with scheduling appropriate follow-up for David.

- Connected Care DSP providers/staff will be able to manually push secure messages from the Epic EMR via SureScripts to HFLC providers/staff

    - *Sample Use Case:* Tracey, a DSP nurse case manager, is working with Denise, an Intel employee and Connected Care member. Denise has been struggling with persistent back pain and has visited the ER to seek pain relief several times. As part of Denise's care plan, her DSP primary care provider has recommended physical therapy; however, Denise did not show up for her scheduled physical therapy appointment at DSP's rehab center due to an issue with her work schedule. Tracey suggests to Denise that she could receive physical therapy at the HFLC which may be more convenient for her and Denise agrees to give it a try. Tracey sends a secure message through the platform to the HFLC team informing them of her recommendation and to enlist their help in coordinating Denise's care.

VII. Privacy and Security Protection

Privacy and security should be addressed holistically, accounting for policy, risk assessment, procedure, training, and technology. Many health care organizations still take a traditional "perimeter" approach to privacy and security, where there is over-reliance on perimeter controls such as firewalls in the logical sense and buildings in the physical sense. End user technologies enable anytime, anywhere access to Protected Health Information (PHI) inside this perimeter. Even though cloud technology moves PHI out of this perimeter and into the cloud provider's data center, Malware infections routinely occur inside security perimeters of health care organizations. With this in mind, Intel strongly recommends protecting health care data directly, wherever it is, at rest or in transit, and including the use of encryption on EHR clients, servers, databases and backup systems. Specifically, Intel urges ONC to consider the following:

1. Inclusion of biometric factors in valid factors for multi-factor authentication. Inclusion and clarification of PII/PHI disposal for circumstance either when a patient explicitly requests it, or in light of use outside of primary use and any applicable retention periods. See *Table 6: Critical Actions for Verifiable Identity and Authentication of All Participants*.

2. Consistent Representation of Authorization to Access Health Information

Inclusion of a "minimum necessary" requirement (cf. HIPAA Privacy Rule) that only provides authorized users access to minimal but sufficient data for specific purposes. This requirement can apply to the fields and types of records (variety and volume of data), as well as the time period of access to data.

More generally, Intel strongly advocates a holistic approach to privacy and security, including the use of policy, risk assessments, procedures, training, and technology. All usage modes and use cases touching the EHR should be covered in the risk analysis conducted by providers, including the creation/collection, processing, retention, disclosure/exchange, and disposal of PHI. Risks resulting from implementation vulnerabilities and operational aspects of the EHR also should be analyzed, including use cases for security key management. Highest priority risks identified should be mitigated through a combination of administrative, physical, and technical controls.

Our approach is based on the fact that cybercrime uses increasingly sophisticated techniques and malware to conduct attacks. Much of this malware seeks to compromise increasingly lower levels in the software stack, for example including the kernels of operating systems (rootkits), hypervisors, BIOS, or firmware. To provide effective security against such sophisticated attacks, it is important to use security safeguards that are hardened and capable of resisting such attempts to circumvent or disable them. This is particularly important in areas of the security network infrastructure that are at high risk of cybercriminal attacks, such as large databases storing PHI, or high bandwidth network connections exchanging PHI.

With health care worker end users having so many technical options for getting their job done, compounded by the rapid growth of "Bring Your Own Device" and social media, it is critically important these personnel have adequate training on risks associated with various options, and their responsibilities in protecting health information integrated into their clinical workflows.

The 2014 HIMSS/Intel Security Survey found that 46% of hospital and clinical professional staff report security workarounds happen every day. Multiple layers of log-ins and slow IT departments are the most common factors that cause workarounds. Personal smartphones and texting are the most often utilized workarounds to improve care, and co-worker collaboration is the most often cited purpose for workarounds risk not only the confidentiality of such information but also the integrity (completeness) of the patient record in the EHR since such out-of-band workflows generally don't update the patient records. As a result, Intel suggests requiring personnel training related to privacy and certification as a condition of certification.

Conclusion

Intel appreciates ONC's vision of an information-rich, person-centered, high performance health system where, "…every health care provider has access to longitudinal data on patients they treat to make evidence-based decisions, coordinate care and improve health outcomes." We encourage ONC to use its unique position and leverage to ensure that this vision is realized sooner rather than later. We look forward to continuing to work together on this very important issue in the future.

Sincerely,

Michael B. Jackson
General Manager, Consumer Health Care
Health and Life Sciences
INTEL CORPORATION