The Interoperability Pledge

Intel Corporation shares the principle that to achieve open, connected care for our employees, our customers and our communities, we all have the responsibility to be pro-active. To further these goals, we commit to the following principles to advance interoperability among health information systems enabling free movement of data, which are foundational to the success of delivery system reform.

1. **Consumer access:** To help consumers easily and securely access their electronic health information, direct it to any desired location, learn how their information can be shared and used, and be assured that this information will be effectively and safely used to benefit their health and that of their community.

2. **No Blocking/Transparency**: To help providers share individuals' health information for care with other providers and their patients whenever permitted by law, and not block electronic health information (defined as knowingly and unreasonably interfering with information sharing).

3. **Standards**: Implement federally recognized, national interoperability standards, policies, guidance, and practices for electronic health information, and adopt best practices including those related to privacy and security.

To implement these commitments we are executing on several fronts:

1. **Intel's Open Architecture** – providing interoperable platforms for the capture, integration and analysis of healthcare data. Most recently Intel is engaged in three pilot programs with the Michael J. Fox Foundation and the Oregon Health State University to integrate patient generated health data from sensors with electronic health record information that will guide patient adherence and better inform both clinicians and patients of health status. For more information on the MJFF program, link to http://www.intel.com/content/dam/www/public/us/en/documents/white-papers/using-wearable-technology-mjff.pdf

2. **Intel's Connected Care Program (an Employer ACO)**–Clinicians for Intel employees as part of the Connected Care employee benefits program have point of care access to their patients' integrated data from hospitals and clinics. Intel chose the Sequoia Project to define the nationwide interoperability standards and implementation models for our programs in Oregon, New Mexico and Arizona covering 33,000 lives. Through contractual relationships with providers, we have guaranteed that records for our employees will not be blocked. For detailed information, please go to: http://www.premisehealth.com/wp-content/uploads/2015/06/Advancing-Interoperability-Healthcare-Paper.pdf

3. **Intel Healthcare Service Gateway (IHSG)** - Intel is working with ecosystem / service providers to implement EHR integration for structured and unstructured data through the IHSG. Specifically, IHSG is facilitating data exchange through the NYeC, the coordinator for the New York State Department of Health's Statewide Health Information Network of New York (SHIN-NY) http://www.nyehealth.org/wp-content/uploads/2015/07/sPRL-Technical-Webinar-Final.pdf

   IHSG has also been used with UMMC (University of Mississippi Medical Center) to integrate patient generated health data from diabetes patients living in rural areas to EHR systems.

4. **PCHA (originally Continua Health Alliance)** - as an original co-founder Intel has volunteered thousands of engineering and management hours to develop a reference implementation model and use cases for personal connected care device interoperability,. Additionally, the Continua design standards are part of the Intel roadmap for future product development. http://www.pchalliance.org/

5. **OpenICE** – Developed with support from ONC's SHARP grant program, ASTM F2761-09 (2013) or "OpenICE" is an FDA-recognized standard that provides a framework for the integration of devices, EHRs and other health IT systems and "apps" into the Medical Internet of Things (IoT). Intel, through collaboration with Partners Healthcare and as a founding member of the IEEE "ICE Alliance," is working to advance the interoperability of medical devices and health IT as part of broader systems in both clinical and non-clinical environments. https://www.us-ignite.org/globalcityteams/

6. **Best practices for Privacy and Security -** Intel offers *the open Security Connected platform from McAfee* as a unified, adaptive framework for encouraging McAfee and third-party products and services to learn from each other, share threat intelligence and context in real time, and act as a team to keep data and networks safe. This application offers interoperability between security products even from different security vendors.

   The benefits of open, connected care for our communities are clear. We believe that privacy and security can play a key role in enabling these benefits while reducing risks of security incidents such as breaches. Intel Security advocates a Protect, Detect and Correct approach to security. On the Protect front, key technical controls include Identity and Access Management, and encryption, both at rest and in transit, as well as at the link and message levels as appropriate. De-identification and tokenization can also play a key role in enabling information exchange and research while minimizing risks. Even with effective security, residual risk of security incidents such as breaches is never zero. This is especially true with "human factor" vulnerabilities emerging such as spear phishing, accidents or workarounds using BYOD devices. Therefore, Intel Security strongly advocates good Detect capabilities to rapidly detect security incidents so they may be quickly addressed to minimize impact. Once security incidents are detected, Intel Security recommends good Correct capabilities such as

Secure Remote Administration to enable organizations to take corrective action and remediate impacts from security incidents to ensure availability of PHI to support connected care. Security Connected http://www.mcafee.com/us/enterprise/security-connected/index.aspx

We are pleased to support Health IT systems nationwide to fulfill the promise of secure access to comprehensive patient records at the point of care in hospitals, clinics, labs and other clinical settings and commit to providing the tools that will facilitate interoperability at every access point.