

April 2, 2015

Karen DeSalvo, MD, MPH, MSc
National Coordinator
Office of the National Coordinator for Health IT
Department of Health and Human Services
200 Independence Ave, SW
Washington, DC 20201

Dear Dr. DeSalvo,

On behalf of the Healthcare Information and Management Systems Society ([HIMSS](http://www.himss.org)), we are pleased to provide written comments to the Office of the National Coordinator for Health Information Technology (ONC) in response to the Interoperability Roadmap document, [Connecting Health and Care for the Nation A Shared Nationwide Interoperability Roadmap DRAFT Version 1.0](#). HIMSS appreciates the opportunity to leverage our members' expertise in commenting on the Interoperability Roadmap. We look forward to continuing our dialogue with ONC as progress is made toward finalizing this document and the path forward to achieve interoperability and health information exchange in support of a broad scale Learning Health System.

HIMSS is a cause-based, global enterprise producing health information technology (IT) thought leadership, education, events, market research and media services around the world. Founded in 1961, HIMSS encompasses more than 58,000 individuals, of which more than two-thirds work in healthcare provider, governmental and not-for-profit organizations across the globe, plus over 640 corporations and 400 not-for-profit partner organizations, that share this cause.

HIMSS is committed to supporting and educating all stakeholders to achieve interoperability leading to information exchange that improves the quality and cost effectiveness of healthcare delivery. We will continue to leverage our resources and our diverse membership to ensure all individuals and communities have access to the tools necessary to share health information in a secure and appropriate manner. HIMSS intends to use our experiences as conveners to bring the broader community together to identify and execute on and achieve the tenets of the Interoperability Roadmap.

The Interoperability Roadmap lays out a plan that builds on an approach that HIMSS actively supports: standards that enable the foundation for interoperability today, and processes to test and certify that health IT systems implement those standards consistently and according to constrained implementation guidance.

In general, HIMSS supports the tenets of the Interoperability Roadmap. The key takeaways from our comments focus on six ideas:

- **The plan put forth by ONC to advance interoperability requires well-coordinated governance processes that include involvement from federal partners, the private sector,**

payers, and the patient community, with robust incentives for each domain to buy-in to the process

Over the past several weeks, HIMSS has been working closely with healthcare community colleagues to respond to ONC's call to action for health IT stakeholders to come together to establish a coordinated governance process for nationwide interoperability. The group includes a broad representation of organizations, including HIMSS, Carequality, CHIME, DirectTrust, Electronic Health Record Association, HealtheWay, and IHE USA.

As a member of the group, HIMSS shares ONC's observations that healthcare transformation to a Learning Health System in the U.S. requires interoperable healthcare information exchange that supports a sophisticated level of care coordination. In order to achieve the Learning Health System in the future, organizations must develop a trust among stakeholder groups, and a collaborative spirit between the stakeholders and the federal government without a top-down process dominated by the federal government and also without prescriptive requirements. Instead, ONC and other federal agencies should be active partners with the private sector in governance across the various domains, such as standards development, testing, and other areas.

Multiple organizations, along with existing and potentially new governance processes, are essential to orchestrate all the components together to arrive at the necessary interoperability capabilities that must be shared. No single network, organization, or process will be able to provide and manage the interoperability life cycle.

We, therefore, do not foresee a unitary and monolithic governance process, rather a set of processes that requires some coordination, but largely can operate independently as long as the overall scope, focus, and direction is well understood and shared. We urge ONC to work with stakeholders to establish such a lean coordination framework with a focused approach to support a small set of high-value, impactful use cases that can substantially benefit from improved interoperability. At the same time, prioritization should in no way hinder private sector and market efforts to develop and implement standards and technologies for other use cases or needs.

As we review the draft Interoperability Roadmap, HIMSS would like to emphasize all the notable private sector efforts underway in enabling interoperability. We see all of this great work already proceeding as a resource to be leveraged by the governance processes going forward, and as a reflection of the different domains currently active within interoperability governance.

We pledge our support to advancing interoperability that engages the patient through coordinated, collaborative, and complementary actions by public and private sector efforts. This coordinated approach takes advantage of the efforts already underway will provide the level of sophistication needed to meet the data sharing and health information exchange requirements of a Learning Health System.

We strongly value the ability to share data across the care continuum. Working together with ONC and other federal partners, we can make great strides toward achieving interoperability.

- **HIMSS is supportive of the implementation timelines for the privacy and security provisions**

noted in the Interoperability Roadmap and encourages the governance processes to reevaluate other aggressive timelines for critical actions put forth for the three, six, and ten-year timeframes

HIMSS is supportive of the implementation timelines noted for the Interoperability Roadmap's Building Block #3 on privacy and security. Our organization and other stakeholders have submitted previous public comments asking for more aggressive implementation timelines in areas such as cybersecurity. HIMSS asks that the governance processes give special consideration to the privacy and security piece of the Interoperability Roadmap and look for opportunities to speed up implementation.

Moreover, HIMSS supports the idea of new governance processes empowering a coordinated multi-stakeholder process to determine what critical actions are best-suited for the three, six, and 10-year timeframes. As these new processes are composed of public and private stakeholders across all the relevant interoperability domains, they are better-positioned to help define the timelines and the path forward.

- **HIMSS applauds ONC for its person-centric vision in the Interoperability Roadmap that enables interoperability and empowers patients to demand that their providers and relevant health IT systems be interoperable**

The individual's ability to access and share their electronic health data contributes to establishing an interoperable Learning Health System. It has been reported that two-thirds of patients already demand access to their health data. The next step is to continue ensuring patients and their healthcare representatives are able to understand and share the data, once accessed, and to encourage patient engagement in their health and health care, as well as in developing their own care plans and care coordination processes.

HIMSS recommends that ONC measure interoperability success not by demand of access to personal health information via electronic health records (EHRs), and other supporting health information technologies, but by how the health data is used. Ultimately, our vision is that our health system will evolve to a Learning Health System including a Collaborative Care Model where patients and their families are truly part of their own care team.

- **HIMSS does not support the idea that individual consent should be required for use and disclosure of information if individual consent is not required under applicable law**

The Interoperability Roadmap introduces the concepts of "basic choice" and "granular choice," which HIMSS feels can only serve to inject confusion among healthcare stakeholders in terms of what they are required to do (or not do).

HIMSS does not see the benefit of, nor is in favor of, the introduction of the concepts of "basic" and "granular" choice, particularly in view of these concepts being contradictory and inconsistent with applicable law (for example, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and state law). HIMSS supports that interoperability efforts should focus on facilitating exchange of data when the law expressly authorizes use or disclosure of the protected health

information (PHI). For example, covered entities may use or disclose PHI for treatment, payment, and health care operations without the patient's authorization in accordance with 45 CFR § 164.506.

- **Regarding security, HIMSS observes that healthcare, as a critical US infrastructure, needs support at many levels to keep data secure and to be positioned to address cyber threats**

HIMSS has included recommendations that would facilitate awareness and information sharing, provide guidance on minimum standards for implementation of security controls, specific guidance on the implementation of encryption and support an industry-wide migration to multi-factor authentication and digital identity.

HIMSS has included information on our substantial work in two areas: patient data/record matching (HIMSS Innovator-in-Residence) and digital identity (HIMSS Identity Management Task Force), which we are supportive of being leveraged by ONC for the Interoperability Roadmap.

- **HIMSS is committed to being a thought leader on interoperability and spurring the community and stakeholder groups forward**

HIMSS commits to continuing our role as a thought leader on advancing the principles described in our public comments. HIMSS pledges to conduct sector-wide events to convene meetings that promote the coordinated approach to interoperability and achieving a Learning Health System. We will use our network to disseminate information across our various communication vehicles, including social media. Overall, HIMSS will work with other stakeholders to gain their buy-in for inclusion in the new governance processes.

Through our sponsorship of a multitude of interoperability and health information exchange efforts, HIMSS is uniquely qualified to be a leader that helps enable an overall successful nationwide interoperability plan.

We have prepared the following thorough comments according to the five Building Blocks identified in the Interoperability Roadmap:

Building Block #1: Rules of Engagement and Governance

ONC has outlined its approach in the Interoperability Roadmap toward rules of engagement and governance in three distinct parts: ONC will define the common rules of the road for trust and interoperability; public and private sector stakeholders will come together to establish coordinated governance processes; and, federal agencies that pay for and provide healthcare services will align their policies for interoperability with the nationwide governance framework.

HIMSS supports the idea that multiple organizations, and existing and potentially new governance processes, are essential to orchestrate all the components that must be shared as part of a consistent set of basic interoperability capabilities. No single network, organization, or process will be able to provide and manage the interoperability life cycle.

One area where the governance processes could focus first is on the interoperability of common

clinical data sets for treatment purposes. In addition, the framework that is created through these governance processes must recognize that the goal is not to set a single way to achieve interoperability capabilities, but establish the floor of interoperability capabilities that health IT must be able to support.

- **HIMSS supports public-private interoperability governance processes that provide market mechanisms to ensure better coordination of health-related interoperability and standards development efforts**

Any new governance processes need to be focused in an action-oriented manner on getting the desired health system outcome of widespread interoperability and not simply talking about how to get there. HIMSS foresees the governance processes encompassing a set of procedures that requires some coordination but largely can operate independently as long as the overall scope, focus, and direction is defined, understood, and shared. We urge ONC to work with stakeholders to establish such a coordination framework with a focused approach to support a small set of high-value use cases that can substantially benefit from improved interoperability.

There are several considerations that need to be included in the development of interoperability governance processes. These include:

- Clarity and consistency throughout the process with stated goals and objectives.
- A unified direction and defined priorities.
- The ability to balance existing health information exchange efforts and innovative emerging capabilities.
- The harmonization of like work, that allow for minimum duplication.
- Inter-network interoperability.
- A clear, objective, and fair process that balances stakeholder representation.
- Offering incentives for adoption.

The interoperability initiative domains that need to be represented in developing the governance processes should include:

- Networks (e.g., DirectTrust, Commonwell, eHealth Exchange, State/Regional Health Information Organizations (HIOs), Surescripts)
- Testing Bodies/Certifiers/Accreditors
- Standards Development and Profiling Organizations
- Technology Developers and Vendors
- Consortia/Trade Groups
- Public-Private Collaboratives
- Professional Associations and Societies (e.g., American Medical Association, American Nurses Association, American Academy of Family Physicians, American College of Physicians)

Given the substantial work and investment in this area over the last several years, HIMSS does not support a “rip and replace” approach toward advancing widespread interoperability. The new governance processes should work within current infrastructure and systems. There would be far too many patient safety risks if the community started over on interoperability with completely new processes.

- **HIMSS suggests that any new interoperability governance processes assess the use of available policy levers**

There are a number of significant policy levers and instruments that can be used to help interoperability succeed. To advance interoperability and health information exchange, the approach needs to be an effort across the public and private sectors, including federal, state-based, and private payer-focused levers. In addition, patient engagement is a critical component, so that patients can be empowered to demand that their providers and all relevant health IT systems be interoperable.

Moreover, new incentives for health information exchange could directly impact supporting new and current health reform payment models. The provision of additional reimbursement incentives to those payment models that demonstrate robust use of interoperable systems should be examined.

- **The Centers for Medicare & Medicaid Services (CMS) should be engaged and involved in developing and sustaining interoperability**

A major part of the entire movement toward interoperability is involvement and buy-in from CMS. In order to make any substantial progress and lasting change to enable interoperability, there needs to be alignment between paying for health care services (particularly, Medicare and Medicaid) and facilitating health information exchange. If there is a Medicare interoperability requirement, other payment systems, including private payers, would follow suit.

- **HIMSS suggests leveraging an end-to-end process to more rapidly advance interoperability**

The current slower than optimal progress towards interoperability is in part a result of the marketplace's inability to reach agreement on the standards and implementation guidance that should be used to make systems interoperable, and the subsequent provider demand for those systems. If ONC would build on the Interoperability Roadmap to outline the national priority use cases and then recommend, through the Standards Advisory, a set of standards, implementation guides for constrained specifications that will make those use cases interoperable, then providers and vendors will understand what is expected.

Subsequently, vendors will implement those standards/guides and specifications in their health IT products and purchasers and providers will seek their use in upgrades and new products. Through an interoperability testing and certification process, such as the one under development by HIMSS, IWG, ICSA Labs, and IHE USA, vendors can test and certify that their products are interoperable according to the specifications for specific use cases, and providers can require those certified products in their purchases. This end-to-end process will create clarity in the marketplace and increase the 'pull' for interoperability from providers that is missing today. Further incentives to accelerate this process could come from ONC in the form of recognition for the organizations that comply.

Building Block #2: Supportive Business, Clinical, Cultural, and Regulatory Environments

HIMSS supports ONC's approach in the Interoperability Roadmap of looking at public and private policy levers beyond Meaningful Use to foster interoperability and health information exchange. We

remain committed to Meaningful Use and the Medicare and Medicaid EHR Incentive Program as an enabler of healthcare transformation as well as a means for moving forward on the path to interoperability that leads to health information exchange, but encourage ONC to pursue other avenues that also promote the exchange of health information.

There are several policy levers to promote interoperability available as a result of Affordable Care Act (ACA) delivery and payment system reform programs as well as Medicare and Medicaid payment policy changes. Private sector policy levers are also an important piece of the overall environment pushing for interoperability. The most effective solutions for accelerating interoperability and health information exchange will pull available levers, as well as employ payment and delivery system reforms that create real market incentives and business cases for interoperability.

In order to support and recognize the achievements of projects, healthcare delivery organizations, and individuals that enhance health IT, HIMSS recommends that notable advancements are rewarded to ensure that ONC can capitalize on both public and private sector policy levers.

HIMSS emphasizes the following points for Building Block #2:

- **HIMSS encourages ONC to pursue the natural lifecycle paradigm for promoting interoperability**

The Interoperability Roadmap describes how HHS will pursue interoperability policies that go beyond Meaningful Use and the provisions of the *Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH)*. HHS is planning to pursue a natural lifecycle of policies to drive interoperability beginning with the alignment of programs and incentives, followed by payment adjustments, and then conditions of participation in Medicare and Medicaid programs. HIMSS supports this direction and the promotion of interoperability as a core element of delivery system reform for providers across the country. Genuine healthcare transformation requires a stable and interoperable IT environment.

HIMSS is encouraged by the recent announcement from CMS that set goals for the percentage of Medicare payments tied to quality or value through alternative payment models, such as ACOs, as well as the shifting of traditional Medicare payments to quality or value-based payments. We support the development and use of IT that will provide health information required by emerging care delivery and business models. Moreover, HIMSS was pleased that the Interoperability Roadmap incorporated these goals into the three and six-year timeline as a critical action for Building Block #2.

While many of these new delivery models are still progressing, they encourage the coordination of mobile health, telehealth, and other novel care models to improve patient outcomes. These evolving service models play a key role in IT's evolution as well by helping to encourage the adoption of interoperability standards and enhance design and usability of health IT tools in order to meet provider, patient, and caregiver workflow needs. HIMSS supports increasing opportunities for the expansion of these innovative care delivery models that can enhance the impact of the technology that underlies and enables these reforms.

- **HIMSS recommends that ONC facilitate voluntary interoperability conformance assessment**

and seals of approval for healthcare delivery organizations and payers that patients and consumers can trust

Voluntary seals of approval can be administered to healthcare delivery organizations and payers by accredited, private sector conformance assessment and testing organizations for their proven ability to execute specific workflows in accordance with the following information:

- Accuracy as a foundation for patient safety.
- Testing in accordance with security and privacy standards configured by preferences.
- Provision of core facts like medication lists but also includes appropriate narrative to provide caregiver and patient with a coherent and complete “Health Story” with access to supporting detail.

Moreover, it is important that these organizations are using appropriately certified products integrated in appropriately engineered workflows, under rigorous change management standards, that address the people, process, and technology factors that, taken together, are necessary for success. All institutions should be able to qualify using their technology on-hand. In order to measure progress across the ecosystem, every participant should be encouraged to assess their current interoperability status, set goals in accordance to their resources to move in sequence with the Interoperability Roadmap, and implement an ongoing plan management process.

- **HIMSS recommends that the Interoperability Roadmap promote engaging patients to better empower them and improve their health outcomes**

The ability of patients to access electronic data is contributing to establishing an interoperable health IT ecosystem. It has been reported that two-thirds of patients already demand access to their health data. The next step is to ensure that patients are able to understand and share the health data, once accessed, and to encourage patient engagement in their own health and health care.

HIMSS recommends ONC measure interoperability success not by demand of access to EHRs, but by how the data is used. Furthermore, patients will need to be able to share data generated by themselves and others to their providers, family members, and other caregivers. Any View, Download, and Transmit (VDT) activity initiated or accessed by the patient, including patient-specific educational materials, must be understandable to the patient and their caregivers. This will help to maximize the many roles that providers and other caregivers play in the patient’s care.

HIMSS applauds ONC for its “person-centric” vision in the Interoperability Roadmap. An important element for enabling interoperability is empowering patients to demand that their providers and relevant health IT systems are interoperable.

The Interoperability Roadmap also emphasizes the importance of patient generated health data (PGHD). It is essential that PGHD must be able to be accommodated within EHRs and other health information technologies with attribution to the patient in order to be available to all providers and patients any time and any place where care is needed.

An important challenge that we still need to address is the fact that providers do not have control over patient behavior once the patient leaves the care setting, yet they are being held accountable for their

improved outcomes in these new models. We request your assistance in raising public awareness on the patient’s role in their health and healthcare. The collection and tracking of PGHD is becoming increasingly important in cultivating this clinician-patient relationship outside of the facility or office. We need to continue to develop standards and encourage the testing of emerging standards and tools such as application programming interfaces (APIs) and Fast Healthcare Interoperability Resources (FHIR) to support this effort.

In an effort to ensure that data most important to the patient is collected, a common clinical data set based on a common taxonomy must be developed and utilized in order to optimize interoperability. HIMSS recommends that ONC provide guidance or leverage the new governance processes in developing a common clinical data set by sponsoring an public-private collaborative to establish consumer/patient taxonomy for the gap items listed in the table below.

Although structured data is important, HIMSS would like to emphasize the significant contribution that the narrative story of the patient and thoughts of the clinician contribute to patient care. While we applaud “Notes/Narrative” making it into the “Common Clinical Data Set,” that is not sufficient unto itself; notes and narrative are important but need context. The patient’s story brings the structured data, notes, and narrative together into something succinct and coherent that can also summarize/reference the goals for care, and direction, caregiver/support team, including the patient’s own goals for self-care. This patient story may also vary by context, with a simple referral differing from a transition of care or discharge summary where the story is amended accordingly.

Interoperability Roadmap Recommended Common Clinical Data Set		Patient Data Gaps
<ul style="list-style-type: none"> ○ Patient name ○ Sex ○ Date of birth ○ Race ○ Ethnicity ○ Preferred language ○ Smoking status ○ Problems ○ Medications ○ Medication allergies 	<ul style="list-style-type: none"> ○ Laboratory test(s) ○ Laboratory value(s)/result(s) ○ Vital signs ○ Care plan field(s), including goals and instructions ○ Procedures ○ Care team members ○ Immunizations ○ Unique device identifier(s) for a patient’s implantable device(s) ○ Notes/narrative 	<ul style="list-style-type: none"> ○ Goals for Care ○ Direction <ul style="list-style-type: none"> – Advance directives – Value-based direction ○ Caregiver/support team

- **HIMSS encourages ONC to enable patients to contribute to their own EHRs and care processes**

While HIMSS agrees that it is a critical first step, the demand for and ability to access and contribute to EHRs is only the beginning of developing an interoperable, person-centered ecosystem. As providers and patients share information across the care continuum, ease of use for providers, patients, and caregivers is paramount to success. This approach should allow for individual configurations in order to promote innovation and maximize individuality. Therefore, continued efforts to support usability and ease of use should be encouraged in the Interoperability Roadmap (tied in with the appropriate clinical decision support) to include individual configuration on interface preferences for all health IT stakeholders.

Additionally, if individuals are regularly accessing and contributing to their electronic health information, the information must be accessible in the file format of the patient's choice and patient-specific education materials must be understandable and written in patient-appropriate language. A patient's ability to electronically use VDT should include both document and query exchanges as well as the ability to view the data in a health IT computable format of their choice, including as a Portable Document Format (PDF) or industry norms like Apple, Windows, and Consumer Information Technology (CIT).

HIMSS has previously recommended that established vocabulary, data type, authentication methods, and information model standards for patient health records aligned with EHRs must be understandable by patients, family members, and other caregivers. Realizing that the patient will ultimately become their own data exchange of information and will hold the most comprehensive data about themselves, it is also imperative that the patient is incorporated into the structure of all contracts and interoperability agreements in an effort to avoid duplication and include the patient in all data exchange activity.

In addition, health and digital literacy are intimately tied together. Goals for digital health literacy as in the current patient-specific educational materials in the Meaningful Use Program should include both plain language and multiple languages.

HIMSS recommends that ONC emphasize the importance of developing patient-specific education materials that are in line with a patient's health literacy base and also available in multiple languages beginning with English and Spanish and moving towards supporting the top five national languages.

The cost of healthcare plays a major role in the patient/provider decision making process and access to cost information at the point of decision making must be included in interoperable systems to improve transparency of value and engagement of patients, families, and caregivers. HIMSS suggests ONC look towards how pharmacy benefit management has been accomplished in order to share cost information that is patient-specific, accurate, and in real-time. Ideally, this information should be available at the point of care and integrated into clinical decision support and shared decision making with patients and their families.

- **Health IT needs to be carefully and precisely woven into individual and provider workflows with a focus on shared decision-making in order to move towards a more interoperable system**

HIMSS recognizes the importance of a successful workflow, specifically when providers are heavily engaged in their clinical environments. In regards to evaluating workflow, the levels of interoperability, as defined in the [HIMSS Interoperability Definition](#), could be used to define levels of interoperability achievement in specific workflows. For any vendor or healthcare delivery organization, the applicable workflows could be evaluated based on their ability to execute data flow and end-to-end exchange.

As we continue to engage patients, caregivers, and providers in using health information technologies we need to also engage the patients in the creation and testing of patient workflows. A true end-to-end

exchange will now require the inclusion of the patient.

Building Block #3: Privacy and Security Protections for Health Information

HIMSS's comments in this area are substantial and, therefore, we have provided detailed comments in the attached Appendix A. Below are summarized comments for this area.

- **Under the privacy provisions, HIMSS does not support the idea that individual consent should be required for use and disclosure of information if this concept is not required under applicable law**

The Interoperability Roadmap introduces the concepts of “basic choice” and “granular choice,” which HIMSS feels can only serve to inject confusion among healthcare stakeholders in terms of what they are required to do (or not do).

HIMSS does not see the benefit of, nor is in favor of, the introduction of the concepts of “basic” and “granular” choice, particularly in view of these concepts being contradictory and inconsistent with applicable law (for example, HIPAA and state law).

HIMSS supports the idea that interoperability efforts should focus on facilitating exchange of data when the law expressly authorizes use or disclosure of protected health information. For example, covered entities may use or disclose protected health information for treatment, payment, and health care operations without the patient's authorization in accordance with 45 CFR § 164.506. Given this context, HIMSS makes the following observations:

- Even if what is proposed is not a new law or regulation, the proposal of introducing the concepts of “basic” and “granular” choice may be considered an interpretive rule or, in effect, *a substantive rule*.
- HIPAA should not be essentially rewritten, through a reinterpretation, including in the context of what is perceived to be fair with respect to consumer expectations.
- HIPAA should not be essentially rewritten, through a reinterpretation, with respect to erroneously stating that individuals have the right to individual access and individual choice under the Nationwide Privacy and Security Framework, based on the Federal Trade Commission's Fair Information Practice Principles (FIPPs).
- HIMSS recognizes that the adoption and implementation, too, of new technical standards that are meant to facilitate or implement the new construct of basic choice and granular choice may also serve to:
 - Inject confusion among healthcare stakeholders in terms of what they are required to do (or not do), and,
 - Unnecessarily take time away from healthcare stakeholders in rendering care delivery and/or coordination of care to patients (i.e., having to essentially deal with technology as opposed to paying attention to the individual patient).

- Finally, some state laws governing protected health information provide that an individual's super-protected health information may be used or disclosed irrespective of patient consent in certain circumstances and/or under certain conditions (for example, Pennsylvania).
- HIMSS is supportive of the fact that the private sector can and should work to develop consistent means to represent consent, but, in the context of applicable law, including HIPAA and other applicable state and federal laws and regulations and judge-made common law, as appropriate.
- **Regarding the security provisions of the Interoperability Roadmap, HIMSS observes that healthcare, as a critical US infrastructure sector, needs support at many levels to keep data secure and address cyber threats**

HIMSS has included recommendations that would facilitate awareness and information sharing, provide guidance on minimum standards for implementation of security controls, specific guidance on the implementation of encryption and support a sector-wide migration to the multi-factor authentication and digital identity.

In addition, HIMSS has included information on our substantial work in two areas: patient data/record matching (HIMSS Innovator-in-Residence) and digital identity (HIMSS Identity Management Task Force), which we are supportive of being leveraged by ONC for the Interoperability Roadmap.

Please see Appendix A for detailed comments and inputs in this area.

Building Block #4: Certification and Testing to Support Adoption and Optimization of Health IT Products and Services

HIMSS agrees with ONC's approach that certification should be used to test that health IT systems and devices conform to standards, and also to certify that the technology has the ability to interoperate with other data sources so that users can exchange and use information from other systems. Our vision of an interoperable health IT ecosystem makes the right data available to the right people at the right time across products and organizations in a way that can be relied upon and meaningfully used by recipients.

Figuring out how to consistently represent data has been a complex undertaking that requires various information systems and technologies produced independently by a multitude of manufacturers to employ standards and specifications by which they document healthcare details and uniformly exchange them. Ensuring that those standards are adequately incorporated into health IT products to accomplish their objectives is the make-or-break step in the quest for interoperability.

For Building Block #4, we emphasize the following points:

- **HIMSS supports the idea of a well-coordinated, diverse, and complementary set of certification and testing programs that are administered by a variety of different entities, both inside and outside of government**

To achieve a Learning Health System, there needs to be better alignment and expansion of current efforts around certification and testing. Alignment must occur through well-coordinated governance processes. Such an effort will afford industry the opportunity to gain health IT stakeholder and public confidence in connected IT systems and data through enablement and accelerated deployment of interoperable solutions with high quality, validity, and sustainable delivery. There are several examples of private sector efforts that should be noted and reinforced through the Interoperability Roadmap, such as [IHE](#).

In our experience as sponsors of IHE and IHE USA, we have seen the private sector advance in the area of interoperability certification. As such, broader alignment and consolidation of current efforts could more rapidly ensure consistent adoption of standards and policies for health IT applications used across settings of care and spur an interoperable healthcare delivery system.

The IHE USA certification program is voluntary and based on vendor demand. Vendors can choose which certification offerings apply to them based on their market participation. This program avoids prescribing detailed functional requirements, or evaluating usability, which are considered questions best left to market preference.

Since 1998, IHE has achieved consensus on a common framework for going about the business of applying health IT standards to the real world. Its principal contribution to interoperability has been to narrow down (constrain) how pivotal information of a health IT system is conceived and packaged when processing that information and using it for clinical care. IHE calls the solutions to a particular use case an “Integration Profile” and the specifications are described in a “[Technical Framework](#).”

This process—developing Integration Profiles for clinical and IT functions, providing the specifications to implement them, and operating from clinical scenarios to ground them in the way health professionals conduct their business—has gotten the health sector closer to pragmatic interoperability.

To further validate interoperability in products, IHE USA conducts a testing process for health IT developers to help them implement IHE profiles. The testing process culminates in annual events called [Connectathons](#) and in vendor self-attestation of the conformance of their products with IHE profiles. This same process is also conducted annually by IHE Europe, IHE Japan, and IHE Korea. These testing events have more than a decade of success, demonstrating that hundreds of vendors are committed to advancing interoperability. Use case-based demonstrations, or vignettes featuring cross-vendor, standards-based information exchange, are also made public through the [HIMSS Interoperability Showcase](#)TM.

There is nothing in the Connectathon or demonstration process, however, that guarantees that a specific product version available in the market fully complies with those profiles. Certification cements this link between tested and marketed versions and helps vendors distinguish their products among buyers seeking compliance with IHE profiles in their health IT purchases. Thus, in the last two years, IHE has expanded its conformance testing services to include a product certification program.

To support the testing and certification process, IHE uses a testing platform and an extensive suite of testing tools in collaboration with an international team of developers, including the interoperability

testing laboratory at the National Institute for Standards and Technology (NIST), other research organizations and commercial developers. Tool development is costly and resource-intensive and today's efforts represent an exemplary model of collaboration, shared investment and use across the public and private sector that could be further extended and leveraged by the broader health IT ecosystem. ONC and other federal agencies should play an ongoing role in supporting and extending this robust set of interoperability testing tools. Ensuring their financial sustainability and making them available for use prior to system deployment is essential for consistent adoption of standards in health IT applications.

In the coming weeks, HIMSS is launching a voluntary interoperability testing and certification program, building upon the work of the EHR|HIE Interoperability Workgroup and IHE USA. This program will test and certify interoperability between vendors' products (EHRs), health information services providers (HISPs), and health information exchanges (HIEs). ICSA Labs serves as the testing and certification body for this new program as well as IHE USA's certification program. Both programs are designed to be complementary with ONC's certification program in the USA as well as conformity assessment programs in other countries. HIMSS welcomes the inclusion of such voluntary testing and certification programs in the Interoperability Roadmap.

- **HIMSS is pleased that the Interoperability Roadmap calls for establishing innovative certification and testing programs for new technologies as well as new settings of care**

HIMSS supports the need for certification and testing programs for provider and non-provider systems such as network technologies and resources, payer systems, population health resources and systems employed for patient engagement as all of these different technologies become part of a Learning Health System. Certification in support of a Learning Health System must be specific and focused on the areas that have the greatest impact on interoperability.

Overall, to achieve the greatest success, broad alignment and consolidation of current industry efforts will more rapidly ensure consistent adoption of standards and policies for health IT applications used across settings of care. Moreover, ONC should continue to work with established standards bodies (including IHE, Health Level-7 (HL7), Digital Imaging and Communications in Medicine (DICOM) and others) to develop, harmonize and disseminate comprehensive standards that provide the foundation for interoperability certification criteria.

In addition to advancing and aligning programs that test and certify that health IT systems conform to standards and interoperate with other data sources, it is essential that healthcare providers and users have the information and tools necessary to be smart purchasers of certified products. Widespread education and related service offerings that are an accessible part of the health IT ecosystem, and articulate the benefits of using certified products will increase their understanding of how to demand interoperability in the system procurement and upgrade process, furthering the adoption of interoperable products in the marketplace.

It is also important to note that ONC has the opportunity to leverage complementary voluntary testing programs by organizations for their ability to extend testing to emerging capabilities and specialty areas of healthcare.

To date, the certification criteria adopted by HHS has been correlated with support for Meaningful Use objectives and measures specified under the Medicare and Medicaid EHR Incentive Programs. During the last several years, many additional conformance testing and certification programs have been developed, which are often specific to a use case and set of standards, including: Surescripts certification for ePrescribing, IHE USA Certification, Electronic Healthcare Network Accreditation Commission (EHNAC) and DirectTrust programs for Direct services and many others. These programs are candidates to be leveraged by ONC as complementary to the certification efforts in the Interoperability Roadmap.

Building Block #5: Core Technical Standards and Functions

HIMSS supports the ideas advanced in the Interoperability Roadmap about how foundational the consistent implementation, use of standards, and broad access to technology services are to a Learning Health System.

The national interoperability governance processes have a prominent place in developing core technical standards and functions. HIMSS supports interoperability governance processes that are coordinated across the public and private sectors, and where stakeholders are empowered to come together to implement and enable interoperability efforts.

In this model, detailed standards development and generation of other deliverables is left to organizations, vendors, and others outside the federal governance process. HIMSS and our healthcare community colleagues can offer important expertise and resources to ensure all stakeholders' perspectives are included as Interoperability Roadmap milestones are developed.

For core technical standards, HIMSS encourages ONC to focus on being the convener and a facilitator that drives:

- *Consensus* with key stakeholder groups representing the breadth of the health IT ecosystem on core standards and technology, as well as expected timeframes.
- *Harmonization* of redundant and duplicative standards, and other guidance to healthcare delivery organizations, vendors, and developers to decrease confusion.
- *Delivery* of proven detailed and domain specific (local) standards, best practices, and implementation guides by teams led by stakeholder consortia including standards development organizations (SDOs), professional organizations, technology consortia, and advocacy organizations as appropriate, comprehensively covering the domains making up the full health IT ecosystem, using core standards and technology building blocks where possible.
- *Inclusion* with roles for all stakeholders.

“Through coordinated governance,” is an often-used phrase in this section of the Interoperability Roadmap. Given the frequency of its use, HIMSS encourages ONC to let the coordinated governance processes answer many of the specifics surrounding technical standards and functions that are required to enable interoperability. Since the governance processes should include all the relevant interoperability stakeholder organizations, using those processes to finalize many of these questions is the best way to proceed.

For Building Block #5, HIMSS emphasizes the following points:

- **HIMSS supports the development of the Interoperability Standards Advisory and the process outlined in the Interoperability Roadmap for publishing an annual update of the best available standards and implementation guides**

The Standards Advisory is a sound model to use for enabling priority functions in a Learning Health System. The most appealing part of the model is its flexibility in providing a list of the best available standards—there are no mandates for technology developers to use particular standards, only publication of the best available standards and facilitation of competition between standards for selection. Technology vendors, certification programs, and governing bodies can choose to use or not to use the standards on the list. HIMSS is diligently working to prepare its public comments on the Advisory document, and will have substantive comments to deliver in early May 2015.

Although the Interoperability Standards Advisory is a good model, HIMSS would like to note that there are several private sector processes already underway to publicize and highlight best available standards. ONC should strive to ensure that those processes that are working are not interrupted, but should be capitalized upon in the development of the Interoperability Standards Advisory.

As noted in the Interoperability Roadmap, SDOs such as IHE and HL7 are collaborating on several projects, but generally where applicable standards are not widely implemented, and may require additional curation, refinement, or harmonization.

Since the governance processes for the Interoperability Roadmap emphasizes and empowers private sector stakeholder groups to come together (with ONC and other federal agencies) to implement and enable interoperability efforts, ONC should try to find a way to capture what is already working in standards development and fill the gaps with this new effort. Moreover, the Interoperability Standards Advisory should provide commentary on the maturity and readiness for use and status of the standards and implementation specifications that it highlights.

- **HIMSS encourages ONC to use the new interoperability governance processes to finalize the Priority Interoperability Use Cases**

The list of proposed use cases presented in the Interoperability Roadmap is a good start for this effort. HIMSS recommends several ideas on how to review and evaluate the use cases in the draft document. However, we suggest that ONC use the coordinated governance processes to refine and prioritize the list and then arrange it for development of technical standards, policies and implementation specifications.

HIMSS notes several principles for ONC and the governance activity to consider as this process moves forward:

- Ensure use cases are included that focus on standards related to quality measurement and quality improvement.
- Move beyond the flow of data for care and health processes in the use cases to include the flow of data for public health, quality, billing, and other components. These other domains need to be considered when discussing use cases to ensure that the data is interoperable.
- Add a person-centric theme to the use cases so that they are not solely focused on health

system or population health-related improvements.

- Ensure that the use cases demonstrate the flow of patient data, as this should allow for more rapid patient-centered improvements to be implemented.
- Design the use cases to advance a more collaborative care framework between providers and patients and not be focused on use cases for transactional purposes as a way to measure interoperability.
- Incorporate data provenance into the use cases so that healthcare providers may make determinations about the trustworthiness of the data being exchanged.
- Involve clinical decision support in use cases.
- Strive to ensure that the semantic (meaning) is preserved from the initiation of the data to the receipt of the data.

- **HIMSS supports creating standards for integrating PGHD into the clinical workflow of all members of the collaborative care team**

PGHD is emerging as a potentially valuable data source in our value-based healthcare system as our society continues down the path toward an electronically-connected world. HIMSS recognizes the information attained from patient-generated systems such as mobile devices/sensors, patient portals, and personal health devices can be critical to showing the more holistic view of a particular patient and the patient population. However, we want to ensure the new data stream is integrated seamlessly into the EHR and workflow of the physician and others in the collaborative care team (e.g. nurse, pharmacist) so it can be consumed by the clinician and acted upon during patient encounters. Creating use and technical standards to support this data evolution will be helpful for evaluating and acting on PGHD before or during a patient visit, and in other care settings like retail pharmacy, home, and virtual visits.

- **HIMSS supports the development of an individual data matching strategy as part of the development of the Interoperability Roadmap**

One of the largest impediments to interoperability and threats to patient safety is the lack of an informed nationwide individual data matching strategy.

HIMSS continues to work with the HHS Chief Technology Officer on a Nationwide Consistent Patient Data Matching Strategy. We also recognize the work of the ONC Patient Matching Project and recommend investigating the near-term practical and long-term innovative/new technology proposals made by the various stakeholders on patient data matching. Moreover, the HIMSS “Innovator in Residence” at HHS should continue to be leveraged to develop a plan to blend near-term practical implementation work with a look at innovation/new technology to find a longer-term solution.

An informed nationwide patient data matching strategy will enhance, not compromise, the privacy and security of patient health information and will help enhance patient safety. Technological advances now allow for much more sophisticated solutions to patient identity and privacy controls, including patient consent, voluntary patient identifiers, metadata identification tagging, access credentialing, and sophisticated algorithms.

The Interoperability Roadmap includes an initial list of data elements that should be included in

exchange transactions in a standardized, consistently formatted manner. HIMSS supports this approach and recommends that a voluntary unique patient identifier be added to the initial list. We look at the lack of an identifier as a privacy issue. The only way that we can truly manage privacy and security is to have a way to identify what data goes with which patient.

HIMSS appreciates the opportunity to submit comments on the Interoperability Roadmap. We hope that our comments help ONC recognize the importance of each stakeholder's role in advancing interoperability and health information exchange, and ensuring that each domain is invested in overcoming the inherent challenges, while further enhancing health IT's pivotal role in enabling healthcare transformation.

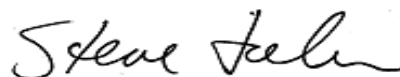
We look forward to the opportunity to meet with you and your team to discuss these issues in more depth. Please feel free to contact [Jeff Coughlin](#), Senior Director of Federal & State Affairs, at 703.562.8824, or [Eli Fleet](#), Director of Federal Affairs, at 703.562.8834, with questions or for more information.

Thank you for your consideration.

Sincerely,



Paul Kleeberg, MD, FAAFP, FHIMSS
Chief Medical Informatics Officer
Stratis Health
HIMSS Board Chair



H. Stephen Lieber, CAE
President & CEO

Appendix A – Input on Privacy and Security Provisions of the Interoperability Roadmap

Previous HIMSS comments – ONC Draft Vision Document, dated September 30, 2014

HIMSS provided [comments to ONC’s Draft Interoperability Vision Document](#), which are incorporated by reference herein. In particular, we draw your attention to the comments on Building Block #3 – Privacy and Security, located at lines 488-600.

Our mention of these comments here is meant to reiterate that a list of critical actions can be impactful only when developed and executed in the context of desired end-states for the industry and the health of our population. Our summary recommendation in this regard is:

Create an imperative for 3, 6, and 10 year (2015-17, 2018-20, 2012-24) desired privacy and security end-states by defining critical actions, by requisite stakeholder or actor, and include relevant levers, incentives, support, resources, standards, methods, requirements, and/or assessment methods (for example, HIPAA audits and/or any necessary regulation or regulatory/statutory changes).

Our comments on Building Block #3 were structured as a list of potential examples, milestones/end-states, actions and levers for the three, six, and 10-year goals. HIMSS feels that these recommendations are relevant for the Draft v 1.0 document as well. HIMSS encourages ONC to construct the Interoperability Roadmap for privacy and security in a fashion that includes:

- Defined end-states.
- Related critical actions.
- Include critical actions required of *any/all* actors/stakeholders, not just ONC/Office for Civil Rights (OCR).

General Comments on Privacy and Security Aspects of the Interoperability Roadmap

- **Ubiquitous, secure network infrastructure and information systems must be a goal for healthcare**

HIMSS has observed that the health sector has become acutely aware of cyber-attacks, insider threats, and other malicious activity. However, traditionally, healthcare’s focus regarding security has been on HIPAA compliance. Compliance, though, does not necessarily mean that information will be kept safe and secure.

Privacy and security protections for health information are quintessential, especially in light of recent breaches which have been in the news over the past few years. Malicious cyber attackers have shown their sophistication in attacking information systems of all kinds, including in healthcare. The healthcare industry is maturing in terms of its capabilities and know-how relevant to these protections. In the digital age, health information cannot be kept private, unless it is also kept secure.

Recommendation for the Interoperability Roadmap: See comments on Vision document for Building Block #3.

- **Holistic risk management must be adopted and implemented by the healthcare industry;**

HIPAA compliance is not enough in the face of sophisticated cyber-attacks and other serious threats

The healthcare industry needs to implement a holistic risk management approach to keeping health information private and secure. This approach should include management of insider threats as well as external threats (such as from hackers or malicious software). Unlike other industries, entities in the healthcare industry generally do not have robust insider threat management programs.

In addition, the capabilities and know-how to prevent and defend cyber-attacks vary greatly from organization to organization. Moreover, in the day and age of the highly trained and sophisticated nation state actors, the vast capabilities, resources, and know-how of even the largest organizations and entities, whether in the private or public sector, may not necessarily be advanced enough to effectively and efficiently contend with cyber-attacks from nation state actors. As a result, compliance with HIPAA (including the HIPAA Privacy and Security Rules) does not necessarily equate to an organization's information being secure.

The industry needs to go beyond HIPAA compliance and adopt and implement holistic risk management in order to keep information both private and secure. While risk management is done at some level by all entities across the healthcare industry, risk management, as it relates to information and IT infrastructure, needs to be added to that equation.

Overall, the HIPAA Security Rule and the requirement for risk analysis and management must be used as a foundation from which to build a robust, mature information security program. Complying with the HIPAA Security Rule is a way to achieve good security hygiene, but is not a complete solution especially in the day and age of the malicious insider threat actor, phishing and spear phishing campaigns, and the sophisticated and/or determined cyber attacker. Moreover, there are variations in the healthcare sector on how risks are assessed, the frequency of risk assessments; and, whether and how risks are managed, especially relevant to the cyber realm.

The United States, in particular, is one of the most advanced nations as far as high technology and its utilization of Internet and networked technologies to connect its information systems. As with everything else, there are trusted and vetted actors and there are those that are not. Before we can build a ubiquitous, secure network infrastructure, we need to make sure that each of the component parts (each node) of the network infrastructure is trusted and vetted. This includes trusted and vetted technologies (including hardware and software infrastructure) and people (the owners, operators, and users of the interoperable network). We also need to agree on what best practices we will apply to achieve an ubiquitous, secure network infrastructure.

Accordingly, the healthcare industry needs the following to raise its profile with regard to having a ubiquitous, secure network infrastructure and information systems for all stakeholders (i.e., covered entities, business associates, and others who may create, receive, transmit, or maintain healthcare information—regardless of size, geographic location, demographics, etc.):

Recommendations for the Interoperability Roadmap: ONC and industry stakeholder groups should promulgate:

- Guidance on what a thorough, holistic risk management program looks like (including plans,

policies, procedures, application security testing, penetration testing, networking monitoring and detection, incident response, continuity, disaster recovery, resilience, etc.).

- A central portal that aggregates cyber threat indicator and vulnerability information, across critical infrastructure sectors, accessible to and actionable by stakeholders in the healthcare industry.
 - Cyber threat indicator and vulnerability information shared in real-time between entities in the healthcare industry and to and from state and federal government.
 - Guidance on how to consume and use the threat and vulnerability information within the healthcare organization, including trusted and vetted technologies, people, and know-how.
- **There is wide variance in the healthcare industry in terms of what cybersecurity best practices mean; however there is a need for a universal security framework, a minimum set of control standards, metrics for measuring the strength of security controls and guidance on implementing the framework**

With respect to our current state of cybersecurity, there is a wide variance with respect to what “best practices” actually mean. Overall, trust is integral in building a secure health IT ecosystem. The National Strategy for Trusted Identities in Cyberspace (NSTIC) Trustmark, Payment Card Industry (PCI), and International Organization for Standardization (ISO) should be considered as possible universal frameworks for establishing electronic trust among healthcare organizations across the Internet. Additionally, existing security control frameworks, including the NIST Cybersecurity Framework, should be considered for alignment and guidance when gaps occur.

In addition, the healthcare industry needs a minimum set of standards and metrics for measuring the strength of security protections. A number of minimum standard sets exist and can be drawn from. These include, but may not be limited to: OCR’s minimum standards for control areas, the CAB-forum Baseline Requirements, and the questions asked by cybersecurity insurance companies and IT auditors in the financial sector.

Last but not least, the healthcare industry would benefit from implementation guidance in terms of adopting and implementing the framework as well as the minimum set of standards and metrics for measuring the strength of security protections.

Recommendation for the Interoperability Roadmap: HIMSS echoes the recommendations of the Health IT Standards Committee (HITSC) Transport and Security Standards (TSS) Workgroup (WG):

- **ONC should partner with NIST, OCR, other federal agencies, and industry stakeholders in several ways to address a uniform approach to enforcing cybersecurity in healthcare:**
 - Work to advance a consistent trust framework across the health IT ecosystem.
 - Endorse a set of appropriate baseline security controls that are uniformly applied to all health IT technologies that enter the ecosystem. (Perhaps consider specific use cases.)
 - Work with industry to accommodate a diversity of emerging health IT technologies across infrastructures within the health IT ecosystem. Health IT infrastructures must be flexible, in that they should permit any certified health IT solution to operate within the ecosystem.
 - Provide guidance on proper governance in cybersecurity, which is essential for building trust and security throughout the ecosystem. Finally, ONC should bring together federal, state, and industry stakeholders to address the goal of reducing variations in cybersecurity

enforcement.

- **The healthcare industry must be cognizant of vulnerabilities impacting other sectors upon which it depends**

We in the healthcare industry do not exist in a vacuum. Instead, as an industry, we have multiple dependencies upon other industries. Hence, we have many more points of vulnerability as a result of our dependencies. For example, the healthcare industry is highly dependent upon other critical infrastructure sectors such as energy, chemical, information technology, and emergency services, to name a few.

An attack on another sector may have a significantly adverse impact and effect on the healthcare sector. This is why information sharing of threat and vulnerability information across sectors, along with standard ways to implement the information for our cyber defenses, is essential, across allied and aligned critical infrastructure sectors and within our own healthcare industry. Ultimately, the information shared across sectors on threat and vulnerability information will be used by entities across the healthcare industry to manage network as well as enterprise security.

Recommendations for the Interoperability Roadmap: Promulgate the following:

- Develop a central portal that aggregates cyber threat indicator and vulnerability information, across critical infrastructure sectors, accessible to and actionable by stakeholders in the healthcare industry.
 - Share cyber threat indicator and vulnerability information in real-time between entities in the healthcare industry and to and from state and federal government.
 - Provide guidance on how to consume and use the threat and vulnerability information within the healthcare organization, including trusted and vetted technologies, people, and know-how.
- **Encryption is not a silver bullet, but it can be a useful safeguard when the right technology and know-how are used appropriately to keep information both private and secure**

There is no single solution for keeping information private and secure. Encryption is not a silver bullet. But, when encryption is used appropriately, it can make information more difficult to steal or otherwise misappropriate. The appropriate use of encryption includes, the use of an “algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key[.]”

The encryption algorithm must not have been compromised and there must be good key lifecycle management and key escrow recovery as well (e.g., the key must not be hardcoded in source code or otherwise easily accessible by an unauthorized user). The healthcare industry needs practical guidance on how to appropriately use encryption, not only in the context of having an exemption to breach notification available in case of breach, but also in the context of keeping information private and secure, whether at rest or in transit.

Above all, the healthcare industry needs to understand that encryption in and of itself is not a safe harbor provision under the Breach Notification Rule (i.e., an exemption for having to notify in case of breach)—appropriate use of encryption (and the right kind of encryption) is required.

Recommendation for the Interoperability Roadmap: Specifically, ONC should work with OCR, other federal partners, and industry stakeholders to address the following issues related to technology and standards for encryption:

- Explanatory guidance that encryption in and of itself is not a safe harbor provision under the Breach Notification Rule (i.e., an exemption for having to notify in case of breach)—appropriate use of encryption (and the right kind of encryption) is required.
 - Practical guidance on encryption key lifecycle management policy and procedures.
 - Practice guidance for encryption key escrow recovery policies and procedures.
 - Practical guidance on key oversight and authorization, addressing the people or entities that maintain access to the encryption keys.
 - Practical guidance on encryption requirements for protected health information stored or accessed via devices and software.
- **A cybersecurity program for the healthcare industry must necessarily include trusted and vetted technologies, people, and know-how; best practices must be shared across industry.**

A healthcare organization can have the best cybersecurity policies in the world, but its cybersecurity program can be very weak without trusted and vetted technologies, people, and know-how. Contracts may set forth, even in very granular detail, cybersecurity best practices. But, contracts and other written documents will not save the day in the face of a cyber-attack.

Instead, in the face of a determined and/or skilled adversary, that is where a healthcare organization's cybersecurity program is put to the real test—prompt and accurate detection of the incident and the know-how required to contain and eradicate the incident as swiftly as possible before harm is done to the information or information systems. The healthcare industry needs to exchange with other trusted and vetted organizations information on all of these things—trusted and vetted technologies, people, and know-how—in order to really understand what the best practices are for a strong cybersecurity program (i.e., detection, incident response, continuity, disaster recovery, and organizational resilience for both insider threats and external threats).

The network infrastructure will not be secure and ubiquitous unless such information is readily exchanged so that each healthcare organization can have a strong cybersecurity program. We cannot expect the whole to be both functional and secure unless the component parts (individual nodes) are as well. The healthcare industry cannot rely on HIPAA compliance for assurance that its information will be kept private and secure in the face of numerous and sometimes sophisticated insider and external threats.

Recommendation for the Interoperability Roadmap: Create mechanisms and incentives for sharing and exchange of information on trusted and vetted technologies, people, and know-how.

- **HIMSS suggests critical actions for ubiquitous, secure network infrastructure and information systems (Table 5)**

E1. Cybersecurity

HIMSS previously submitted [comments](#) in connection with the Security Risk Assessment tool. In

addition, HIMSS is happy to be an education and outreach facilitator as ONC updates this tool.

HIMSS suggests that the coordination of ONC with Assistant Secretary for Preparedness and Response (ASPR) include initiatives relevant to the multi-dependency of healthcare with respect to other critical infrastructure sectors (which includes the energy, chemical, information technology, and emergency services sectors).

HIMSS also respectfully requests that ONC refers to the [HIMSS Response on Emergency Preparedness Requirements for Medicare and Medicaid Participating Providers](#), in which HIMSS states that the cyber-attack is one type of manmade disaster for which healthcare providers need to be prepared. For example, a healthcare provider may be the victim of ransomware, but may remedy the situation by invoking its backup and disaster recovery plan (which may include restoring from a cloud backup). HIMSS also respectfully suggests that ONC and ASPR may provide guidance to healthcare providers, other covered entities, and business associates with respect to a robust, mature backup and disaster recovery plan and associated best practices.

In addition, HIMSS respectfully requests clarification on whether the term Information Sharing and Analysis Center (ISAC) includes an Information Sharing and Analysis Organization (ISAO) (as referenced in the Executive Order -- Promoting Private Sector Cybersecurity Information Sharing). If these terms are different, HIMSS respectfully requests clarification on HHS initiatives and activities with ISACs and ISAOs. On a related note, HIMSS asks whether and how the healthcare industry is to connect with the US Department of Homeland Security's National Cybersecurity and Communications Integration Center, with respect to this bidirectional sharing of information (this could be an example of the "central portal" referenced above).

HIMSS assumes that ONC intends to publish a NIST Cybersecurity Framework (Framework) and HIPAA Security Rule cross-walk in light of Version 1.0 of the Framework. To that end, HIMSS would like to highlight our statement in response to NIST's Request for Information (RFI) on user experience with regard to the Framework, as quoted in the [Framework's December 5, 2014 status update](#): "We have observed that the health sector has become acutely aware of cyber-attacks, insider threats, and other malicious activity."

However, traditionally, healthcare's focus has been on HIPAA compliance. Compliance, though, does not necessarily mean that information will be kept safe and secure. Accordingly, healthcare providers, other covered entities, and the business associates that do work on behalf of these covered entities, all need practical and detailed guidance on making the transition from 'compliance only' to being secure (in the same sense that other critical infrastructure sectors, such as the chemical, electrical, and financial sectors have adopted and embraced security)[.]"

Please see comments above with regard to the need for the healthcare industry to adopt a universal security framework and a standard way to implement the framework.

E2. Encryption

HIMSS observes that many healthcare providers, other covered entities, and business associates do encrypt data in transit, but many do not for data at rest. Accordingly, HIMSS respectfully requests guidance for the healthcare industry with regard to "at rest" standards for data encryption and other

technical assistance. Moreover, HIMSS respectfully requests timely, accurate, updated guidance which informs and educates the healthcare industry on “lessons learned” from compromises of encrypted information at rest.

HIMSS respectfully requests timely, accurate, updated guidance that informs and educates the healthcare industry on “lessons learned” from compromises of encrypted information in transit (e.g., rogue virtual private networks). Please see the aforementioned text on “Moving Forward and Critical Actions.” Secure electronic communications, including e-mail, messaging, and videoconferencing, should be encrypted, but in an appropriate manner.

HIMSS respectfully requests guidance for the healthcare industry on which secure algorithms to use, good key management, and guidance on due diligence to select an approved encryption product/service for encrypting data at rest and in transit.

HIMSS observes that cybersecurity insurance is not affordable for all types of healthcare providers, other covered entities, and business associates. It can be a very expensive proposition which is out of reach for many. Entities in the private sector should be sufficiently incentivized due to the significant economic impact which a major breach may have on the organization, with respect to fines and penalties, remediation costs, and potential lawsuits, as well as the adverse effect on goodwill.

HIMSS respectfully suggests that ONC may help raise the level of awareness and understanding of the adverse effects of data leakage, cyber-attacks, and negligent and malicious insiders, through its education and outreach initiatives, including through the use of associations as conduits to their respective members in the industry.

- **HIMSS recommends that the security aspects of RESTful services need to be addressed in a standardized manner**

In order to ensure that information in transit using Representational State Transfer (RESTful) services is both private and secure, the security of the application programming interface (API) needs to be addressed and criteria must be designated for secure APIs for information sharing between parties using RESTful APIs. As a result, HIMSS has the following recommendations:

- The security vulnerabilities and overall risks associated with Health IT RESTful APIs need to be addressed (e.g., secure by design, application security testing, communication of security vulnerability information and risks to stakeholders as well as available patches and updates, etc.).
- Some recommended topics to consider for certification of client and browser software across multiple platforms for implementing a secure API for the purpose of information sharing between parties using RESTful APIs include the following:
 - Application security testing of the software (e.g., threat modeling, source code review, static or dynamic binary analysis, etc.).
 - Determine whether a secure coding standard has been used to develop the software.
 - Use OAuth 2.0 and OpenID Connect standards with transport layer security (TLS) encryption to secure HIT RESTful APIs.
 - Use the OAuth 2.0 implementation model most appropriate for the architecture and risk profile of the application.

- Utilize OpenID Connect to enable single sign-on across multiple applications, which increases the importance of a strong initial login – assure that the method used to initially authenticate the user is sufficiently strong for the application use case.
 - Strengthen client and browser software authentication by using standardized signed web tokens instead of passwords transmitted over the network (please note: a web token signature is a verified and secure means of representing claims to be transferred between two parties).
 - Use TLS encryption with server side authentication to assure clients that they are communicating with the correct server and to protect data transmitted across the established link.
 - Minimize the risk of data exposure through redirect manipulation by using declared redirect Unique Resource Identifiers (URIs) during client registration.
 - Establish and enhance HIT RESTful API security vulnerability testing to minimize evolving cybersecurity risks.
 - Ensure appropriate awareness and mitigation of Cross-Site API vulnerabilities.
 - Ensure vendors provide to customers current information regarding HIT technology compatibility and interoperability with browsers and client software/platforms, and potential impacts on security.
 - Vendors should incorporate threat monitoring and risk mitigation into the HIT vendor’s product management lifecycle.
 - ONC should also track the efforts of the OpenID Foundation Health Relationship Trust (HEART) Working Group and the Argonaut Project, both of which are addressing privacy and security for RESTful HIT APIs.
- **Verifiable identity and authentication may be achieved by using multi-factor authentication; HIMSS supports the efforts and initiatives of NSTIC in further developing multi-factor authentication for use by the healthcare industry**

Multi-factor authentication provides greater assurances that an individual or entity that is attempting to access a system is who he or she claims to be, but it is not a silver bullet. First, multi-factor authentication has significant costs in implementation and maintenance. Second, there is a lot of variation by vendors in terms of how the multi-factor authentication technology is implemented. Third, multi-factor authentication can be hacked or otherwise compromised, using tactics, techniques, and procedures including phishing, malware, skimming, and other means.

Accordingly, HIMSS observes that verifiable identity and authentication may be achieved using multi-factor authentication but this method is not fool-proof – instead, multi-factor authentication needs to mature as a technology and also become more resilient to attacks and other compromises. HIMSS supports the efforts and initiatives of the National Strategy for Trusted Identities in Cyberspace (NSTIC) in an effort to help utilize secure, efficient, easy-to-use and interoperable identity credentials while mitigating cybersecurity issues using multi-factor authentication and solid identity proofing processes and [Executive Order 13681, Improving the Security of Consumer Financial Transactions](#) (which also supports NSTIC efforts and initiatives).

Related the NSTIC initiative, last year HIMSS formed an Identity Management Task Force (IDM TF). The charge of the IDM TF is to work with the NSTIC Health Committee to address the specific requirements of the healthcare sector, and to socialize this work within the HIMSS community of stakeholders.

The HIMSS IDM TF has published a [white paper](#) that addresses the following task:

Develop and publish guidance for specific levels of identity assurance to meet healthcare requirements (NIST Special Publication 800-63-2).

This task also relates to the CMS Meaningful Use Stage 2 requirements. For example, this is the most common way for an eligible provider or hospital to meet a core requirement for Meaningful Use Stage 2: *“Provide patients the ability to view online, download, and transmit information about a hospital admission.”*

The white paper documents the following recommended requirements for security in the specific use case of a patient accessing their own PHI:

All mechanisms or processes that provide electronic access by patients to their own protected health information (PHI, as defined by HIPAA) must be capable of employing user identity proofing and authentication at a high level of confidence, greater than or equal to National Institute of Standards and Technology (NIST) Level Of Assurance (LOA) 3 or equivalent (as determined by a documented HIPAA risk analysis).

Before a patient is given the ability to view online, download, or transmit PHI, they must be informed about potential risks to their privacy in doing so, including differences based on any security choices they may have.

With rare and well defined exception, all patients must meet such a high confidence identity proofing standard before being allowed electronic access to PHI. (Guidance must be promulgated as to how a clinical encounter that results in a patient being ‘known to the practice’ can be conducted and documented to meet such a standard or equivalent, as well as how to enable the exception of authentication for a patient who is anonymous or cannot be proofed at the necessary level of confidence.)

All patients must pass such a high confidence identity authentication standard (e.g., two factor authentication) before being given electronic access to PHI, unless they request access through a mechanism or process that bypasses such high confidence identity authentication (as allowed by HIPAA) after being informed about potential additional risks. Guidance must be promulgated as to the limitations and ramifications for the high confidence authentication for a patient who is ‘known to the practice’ but has not been proofed at that level.

Next Steps of the HIMSS IDM TF include:

- Develop guidance on how a clinical environment can conduct and document identity proofing at a high level of confidence, greater than or equal to National Institute of Standards and Technology (NIST) Level Of Assurance (LOA) 3 or equivalent (as determined by a documented HIPAA risk analysis).
- Develop guidance on how to do and documented a HIPAA risk analysis to support #1.

- Develop guidance on how to enable authentication at a high level of confidence for a patient who is anonymous or cannot be proofed at the necessary level of confidence, including the limitations and ramifications of doing so.
- Develop guidance on how to designate a proxy or delegate and give the delegate access to the patient's PHI with the same level of confidence.

Recommendation for the Interoperability Roadmap: ONC and the healthcare industry should promulgate and leverage the work of the NSTIC and the HIMSS IDM TF.

- **HIMSS does not support the idea that individual consent should be required for use and disclosure of information if individual consent is not required under applicable law.**

“A covered entity may, without the individual's authorization: Use or disclose protected health information for its own treatment, payment, and health care operations activities” under the HIPAA Privacy Rule and as set forth on the HHS website. This fundamental principle of the HIPAA Privacy Rule is acknowledged in some places of the draft Interoperability Roadmap document. However, other places of the draft Roadmap document clearly state contradictions.

For example, page 55 of the draft Interoperability Roadmap document states the following:
 “Participation in and use of a Learning Health System will be highly dependent upon reliable mechanisms to ensure that... (4) users have access only to data they are authorized to access, *where authorization is determined by individual's choice, or if no choices are recorded, what the statutes, regulations and consensus rules say a user may access, use, disclose and receive*” (emphasis added).

As set forth in the HIPAA Privacy Rule and the aforementioned, quoted text from the HHS website on the treatment, payment, and healthcare operations (TPO) exclusion, *no individual authorization is required whatsoever*. Accordingly, a covered entity may have access to TPO information, irrespective of the individual's choice and irrespective of whether or not choices of the individual have been recorded.

Individual consent should not be required for use and disclosure of information if individual consent is not required under applicable law (such as, but not limited to, the TPO exclusion under HIPAA and the minimum necessary standard under HIPAA (which is governed by providers, not patients)). If anything, the fact that individual consent is not required under applicable law should be made clear to all covered entities in any forthcoming technical or other educational guidance or other information. By the same token, when an individual authorization is required under HIPAA, this requirement should also be made clear to all covered entities in any forthcoming technical or other educational guidance or other information.

Introducing the concepts of “basic choice” and “granular choice” only serve to inject confusion among healthcare stakeholders in terms of what they are required to do (or not do). Healthcare stakeholders already have many applicable laws and regulations to comply with. Even if what is proposed is not a new law or regulation, the proposal may be an interpretive rule or, in effect, a substantive rule.

HIMSS does not see the benefit of and is not in favor of the introduction of the concepts of “basic” vs.

granular choice, particularly in view of these concepts being inconsistent with applicable law (namely HIPAA). HIPAA should not be essentially rewritten, through a reinterpretation, including in the context of what is perceived to be fair with respect to consumer expectations.

Moreover, HIPAA should not be essentially rewritten, through a reinterpretation, with respect to erroneously stating that individuals have the right to individual access and individual choice under the Nationwide Privacy and Security Framework (based on the FIPPs). HIMSS suggests that the adoption and implementation, too, of new technical standards that are meant to facilitate or implement the new construct of basic choice and granular choice may also serve to: (i) inject confusion among healthcare stakeholders in terms of what they are required to do (or not do) and (ii) unnecessarily take time away from healthcare stakeholders in rendering care delivery and/or coordination of care to patients (i.e., having to essentially deal with technology as opposed to paying attention to the individual patient).

Finally, some state laws governing protected health information provide that an individual's super protected health information may be used or disclosed irrespective of patient consent in certain circumstances and/or under certain conditions (for example, Pennsylvania).

HIMSS supports the idea that consent mechanisms are needed to be consistent with applicable law, including HIPAA and other applicable state and federal laws and regulations and judge made common law, as appropriate.

Recommendations for the Interoperability Roadmap: ONC should reconsider its approach to these consent mechanisms in the Interoperability Roadmap, to be entirely consistent with applicable law.

- **Harmonizing state laws will help move interoperability forward, but individual state autonomy and policy should be respected.**

HIMSS support the objective of undertaking activities that could potentially facilitate harmonization of the complex maze of federal and state laws that apply to privacy. However, without reviewing a draft or proposed law or regulation, HIMSS has no specific position on what the harmonization outcome would be. The draft Interoperability Roadmap document does state that substantive individual rights should not be eroded in the harmonization process, and yet it also states that such laws should be aligned with HIPAA.

In terms of what is contemplated by harmonization of state privacy laws with HIPAA, we respectfully request clarification on this point. We support a balanced approach to harmonizing state privacy laws and yet respecting state autonomy and individual state policy. But, we do not necessarily support adopting an a priori position requiring all healthcare stakeholders to abide by the most stringent state law relevant to healthcare privacy.

- **Accurate individual data matching is quintessential to patient safety and zero identity matching errors is the goal for the healthcare industry**

Accurate individual data matching is very much needed in the healthcare industry. Incorrect matches are a major source of healthcare errors and misidentification errors represent the most serious type of

error. Also, to be clear, it can be difficult to match patients within a given health system and complexity is increased when matching is done across different health systems when health information is being exchanged. Such matching errors often require significant amounts of time and effort to rectify by the health information management personnel of a healthcare organization. Healthcare organizations may not necessarily have the resources to devote to rectifying all of these errors.

At the present time, however, HHS is prohibited under [Public Law 105-277](#) Section 516 from spending any funds to “promulgate or adopt any final standard...providing for, or providing for the assignment of, a unique health identifier for an individual...until legislation is enacted specifically approving the standard.”

Notwithstanding this prohibition, if a unique health identifier were to be adopted and implemented (i.e., facilitated by the federal government or by the private sector) in a standardized way across all healthcare stakeholders, the healthcare industry generally agrees on what metrics should be measured to determine the accuracy of patient matching. Identity matching errors are among the most serious category of errors and lead to poor medical outcomes, unnecessary complications, increased medical care expense, and even death.

HIMSS has a resource on [Key Performance Indicators \(KPIs\) for Patient Identity Management](#) which helps healthcare stakeholders understand the effectiveness of its patient identity management and governance program by using certain essential key performance metrics for patient identity management. Again, to reiterate, the goal is to have zero identity matching errors.

HIMSS IIR Project

HIMSS (working with HHS – CTO/ONC) has an Innovator-in-Residence who is working on the challenge of measuring patient data matching algorithm performance, *developing a test sandbox that will facilitate clarify as to algorithm accuracy, generate synthetic test data and allow healthcare organizations to access comparative information on open source matching algorithm products.*

Recommendation for the Interoperability Roadmap: ONC should be aware of and incorporate this information into the Interoperability Roadmap actions.

- **Accurate individual data matching may be facilitated by ensuring high quality and integrity of the information through data provenance.**

Through data provenance, one can make the determination about whether data is trustworthy. Data provenance may be viewed in terms of source provenance and provenance of the intermediaries. Source provenance relates to who the author or originator of the data was or from where the data originated. With respect to health information which is exchanged, only source provenance matters so long as the information was not changed or otherwise modified from the original data.

However, if the data is changed or modified in some way, then intermediary provenance then comes into play – particularly, who viewed the data, how was the data used, how the data was conveyed, and whether or not the data was conveyed without modification along the way.

Based on the recommendations of the HITSC Data Provenance Task Force (chaired by Lisa Gallagher of HIMSS), the Interoperability Roadmap should incorporate the following required action steps for ONC (through the Standards & Interoperability (S&I) Data Provenance Project):

- Begin focus from the perspective of an EHR, including provenance for information created in an EHR (source provenance) and when it is exchanged between two parties.
- Clearly differentiate between communication/information interchange requirements and system requirements.
 - Start with the assumption that the source provenance is good, complete, and trusted at the point for information interchange.
 - i. With regard to any and all communication and/or information interchange requirements, converting between different transport protocols should be lossless so as to retain integrity in terms of provenance of the payload/content.
 - ii. Then, as to system requirements for provenance (which includes source provenance), look at the provenance of the data at the time of import, creation, maintenance, and export.
- Consider the definition of “change” to the data (e.g., amend, update, append, etc.) and the implications for provenance. If the content changes, the change should be considered a provenance event.
- Consider the implications of security aspects (e.g., traceability, audit, etc.) and the impact on the trust decision.
- If applicable, capture policy considerations. Defining levels of trust is a policy issue. For clinical care, if trending the data, one may need to know the degree to which the information may be trusted.