The Office of the National Coordinator for Health Information Technology

Connecting Health and Care for the Nation

A Shared Nationwide Interoperability Roadmap

SUPPLEMENTAL MATERIALS

Version 1.0

Contents

Introduction

Connecting Health and Care for the Nation: A Shared Nationwide Interoperability Roadmap version 1.0 contains important detail on the drivers, policy and technical requirements and outcomes that are necessary to achieve nationwide interoperability to enable a learning health system. This document contains a significant amount of background information and additional detail that supports the Roadmap's milestones, calls to action, and commitments. The supplemental materials are organized into three main sections that mirror the Roadmap: drivers of interoperability, policy and technical requirements that enable interoperability and outcomes that will be possible when nationwide interoperability is achieved. Additionally, the resources below also provide the reader with background information on health information technology (health IT) interoperability.

- Historical background and current progress on interoperability:
  - ONC Report to Congress: Update on the Adoption of Health Information Technology and Related Efforts to Facilitate the Electronic use and Exchange of Health Information, October 2014.
  - ONC Data Briefs
  - ONC Interoperability Portfolio
- Background on ONC's 10 year vision and the five Building Blocks:
  - Connecting Health and Care for the Nation: A 10-Year Vision to Achieve an Interoperable Health IT Infrastructure, August 2014
- Additional information on ONC's Quality Improvement 10 year vision:
  - Health IT Enabled Quality Improvement: A Vision to Achieve Better Health and Health Care, November 2014
- Additional information on APIs and a national architecture for interoperability:
  - JASON Report: A Robust Health Data Infrastructure, April 2014
  - HIT Policy and HIT Standards Committees' JASON Task Force Final Report, October 2014
  - JASON Report: Data for Individual Health, November 2014
- Additional information on person-centered health care:
  - Person at the Center | HealthIT.gov
- Additional information on patient generated health data:
  - Patient-Generated Health Data | HealthIT.gov
- Additional information on governance:
  - Health Information Exchange | HealthIT.gov

Drivers

Appendix A: Supportive Payment and Regulatory Environment that Encourages Interoperability

Despite strong agreement on the need for interoperability and data liquidity to enable higher quality, more efficient and effective, person-centered care, the demand among providers, consumers and purchasers of health care has not yet translated into seamless interoperability across the health care system. Countervailing market forces and structural attributes of the health care system make it costly to move away from the status quo of fragmented care and silos of health information, inhibiting widespread adoption of interoperable systems. One key barrier to interoperability arises from the way in which health care in the United States (U.S.) has traditionally been reimbursed (typically "fee-for-service" payment models.) Economic gains from interoperability are realized in the form of greater efficiency in the delivery of health care—for instance, laboratory and imaging tests are often duplicated when an existing image that might preclude the need for a test is not available or not accessed, contributing to wasteful health care spending that could be allocated more efficiently. While the effective use of interoperable systems has the potential to address this waste by allowing providers to share test results, there are few incentives to adopt these systems under the fee-for-service system, which can actually incentivize providers to deliver a greater volume of services and disincentivize the reuse of prior lab tests.

In addition, many market participants, especially those in health care markets characterized by intense competition, may be wary of how increased interoperability will impact their business strategy and competitive position. Providers are concerned about increased liability risk when they exchange health information outside their walls. These providers may not view the benefits associated with interoperability as outweighing the costs of ensuring that they are exchanging information in a secure fashion that adequately protects individuals' information. Seamless interoperability could also enable individuals and their caregivers to more easily change care providers and transfer electronic health information among providers, thereby reducing providers' competitive advantages from exclusive access to an individual's health information.

These same forces may impact technology developers' behavior, reinforcing a status quo characterized by high costs to switch products and services, greater lock-in and reduced data portability. The lack of economic incentives for coordinated and efficient care across the continuum has fostered a health IT market where providers have demanded tools that meet their organization's internal care delivery needs but not tools that are person-centered in allowing interoperability across many different settings and providers of care. Moreover, providers interested in improving interoperability are in some cases limited by their technology developer agreements in demanding interoperability.

Experience from the Regional Extension Center (REC) program[1] has shown small providers making purchasing or licensing decisions often lack the time and resources to keep up with emerging health IT trends and products. Furthermore, interoperability and data liquidity could enable providers to more easily change health IT, increasing competition between technology developers.

Finally, the fragmented nature of the health care marketplace poses fundamental challenges to interoperability. Where other industries have achieved desired results from common standards and shared infrastructure, they have often relied on the market power of a few major actors that are able to drive standardization by virtue of their size and reach. Certain care delivery organizations may be dominant in a local or regional market, but have little presence elsewhere, while large payer organizations may have national reach but only a limited presence in any given market. Within this landscape, the federal government is unique in its market reach, but is still limited in its capacity to drive standardization. Achieving greater interoperability, with common policies and standards, will require coordinated commitments across health care stakeholders to overcome these fragmentation challenges.

Over the past several years, the public and private sector alike have made progress toward changing the way health care is paid for, laying the groundwork for a value-based and person-centered learning health system. Under new "value-based payment" programs, providers are reimbursed based on the quality of care delivered and the degree to which providers can keep costs low and increase efficiency. These programs strengthen the business imperative to adopt common standards and exchange information across the care continuum to provide more coordinated and effective care.

With value-based payment, having up-to-date information to support individuals is critical for providing timely and necessary care and services. For example, knowing that a discharged patient with congestive heart failure is gaining weight the week after they are discharged can trigger home-based interventions that can help prevent the patient from being readmitted, saving significant costs overall and preventing negative patient outcomes. Models that emphasize shared accountability for value across different organizations, including non-traditional stakeholders such as community-based services, are also creating incentives to seamlessly share information with an expanded care team.

However, paying for outcomes alone will not be sufficient to change the way providers deliver care. The transition to value-based payment is a long-term, incremental process and providers will need to master new tools and ways of working together before they are willing to take on more substantial levels of risk. Payment policy should encourage incremental steps toward interoperability and data liquidity and address those disincentives that stakeholders perceive as making the transition to interoperability too costly.

1 The Regional Extension Center (REC) program provides implementation assistance to priority practices—those with limited financial, technical and organizational resources—but the assistance is time limited. http://www.annfammed.org/content/13/1/17.full

While the Medicare and Medicaid EHR Incentive Programs (EHR Incentive Programs) have provided significant incentives to adopt health information technology that can share information according to common standards, further action may be needed to counter the powerful business drivers described above. In addition, the EHR Incentive Programs were not designed to include all providers across the continuum of care, such as long-term care and behavioral health providers, which are some of the most significant cost drivers in the care delivery system.

As HHS continues to test and advance new models of care that reward providers for outcomes, it will help to create an environment where interoperability makes business sense. Additional policy and funding levers across the public and private sector could also be leveraged to encourage interoperable health IT, including: 1) new incentives to adopt and use interoperable health information systems to create additional demand for interoperability; and 2) requirements/ penalties that raise the costs of not moving to interoperable systems.

Federal Agencies

HIE Elements in Public Value-Based Payment Models

Value-based payment programs established under the Affordable Care Act have already begun to create the incentives for interoperability and information exchange across the care continuum. Under the Center for Medicare and Medicaid Innovation, HHS continues to expand its portfolio supporting new approaches to care delivery. Accountable care models, which encourage doctors and hospitals to reduce the total cost of care for patients in exchange for an opportunity to share in savings, are designed to reward more effective care coordination. More than 400 Medicare Accountable Care Organizations (ACOs) have been established in 47 states, serving over 7.8 million Medicare beneficiaries, through the Medicare Shared Savings Program, Pioneer ACO program and other initiatives. Another promising model, the Comprehensive Primary Care Initiative, provides funding for advanced primary care approaches, as well as an opportunity to share in savings with both public and commercial payers, in seven markets across the country.

The parameters of federal value-based payment models offer a number of opportunities to reinforce the adoption of capabilities to exchange health information and HIT tools that are instrumental to providers succeeding within these models. Initially, value-based payment models can incentivize or require basic adoption of certified HIT, for instance, requiring a certain percentage of participating providers to have attested for meaningful use stage 1 (e.g., CMMI's Pioneer ACO program), or including health IT adoption as part of the quality measurement framework for a given program (e.g., the Medicare Shared Savings Program). As providers become more sophisticated, HHS can consider transitioning requirements to other measures that reflect interoperability capabilities, such as measures of care coordination. These models, in addition to existing efforts to increasingly tie fee-for-service payment to quality and value, present a natural pathway to ensure that incentives for interoperability gradually reach larger populations of patients and providers.

In addition to launching new value-based payment models for testing, HHS will seek to adopt existing models that have demonstrated value as part of permanent Medicare and Medicaid policy, with the opportunity to codify program design elements around interoperability similar to the requirement for summary record exchange and use of certified health IT for reimbursement under Medicare Part B for chronic care management. The Department of Health and Human Services (HHS) has set a goal of having 30% of Medicare health care reimbursements through alternative, value-based payment models by the end of 2016 and 50% of Medicare health care reimbursements in alternate payment models by the end of 2018. HHS has developed an approach that it believes will achieve these goals, including action steps outlined in this Roadmap to advance interoperability.

Linking Exchange of Information to Medicare Requirements

The federal government sets extensive requirements for organizations paid under the Medicare program that address core quality and safety expectations for any organization participating in the program. Ultimately, as electronic, interoperable exchange of health information becomes more ubiquitous, conditions of participation required for Medicare could be linked to electronic processes when consistent with clinical and safety statutory requirements. For instance, electronic sharing of summary care records between hospitals, skilled nursing facilities (SNFs) and home health agencies could be established as the routine standard for transmitting the information these facilities are required to share across care settings.

Federal Health Plan Contracting

A number of federal government agencies contract directly with health plans to care for employees and other beneficiaries. The Federal Employee Health Benefits program, administered by the Office of Personnel Management, contracts with health plans covering 8 million federal employees and their dependents. Tricare, the health program covering active duty military service members, also contracts with plans to provide out of network care for beneficiaries. Finally, the Department of Veterans Affairs contracts with plans providing out-of-network care as well. In their role as large purchasers of health care, these agencies have a significant opportunity to encourage exchange of health information across their provider networks.

Aligning Federal Contracting Guidelines

In addition to health plans, federal contracts and grants often support acquisition of health IT infrastructure and services across a wide range of agencies. HHS can work with selected agencies to ensure funding streams for capital investments for health information systems include consistent requirements around interoperability standards that all systems must meet. For instance, Health Resources and Services Administration (HRSA) investments in health center controlled networks would require health IT acquisitions to comply with specified standards.

States

State Innovation Models Funding

CMS is supporting delivery system and payment reform through Medicaid policy and through the State Innovation Models (SIM) initiative. Including the Round Two awardees and six Round One Model Test states, now over half of states representing 61 percent of the U.S. population (38 total SIM awardees, including 34 states, three territories and the District of Columbia) will be working on efforts to support comprehensive state-based innovation in health system transformation. As part of their SIM approaches, states can leverage federal funding to advance interoperability across the care continuum.

Medicaid Managed Care

Medicaid managed care plans also offer significant opportunities for states to advance interoperability. Currently, 41 states and the District of Columbia deliver Medicaid and/or CHIP services through a managed care arrangement. As part of state quality strategies, states can include references to health IT (including EHRs) or health information exchange (HIE) in any sections that are pertinent to strategic improvement efforts planned by the state, such as identifying enrollees with special needs or health care disparities, collection of data for use in reporting performance measures, use of health IT to assess access, or use of a new health information/exchange technology as an intervention in a performance improvement project or focused study. States can also more aggressively require health information exchange usage as part of managed care organization request for proposals and contracts. A number of these have already made progress with these types of strategies. For instance, Arizona Medicaid requires its managed care health plans through contract to join the state level HIE, while Louisiana's recently launched managed care strategy requires hospitals in participating networks to contribute data to the state health information exchange to support care coordination.

Managed care contracting represents an important lever states can use to require and implement measures and incentives for health information exchange and health IT adoption by providers and managed care entities participating in their programs. HHS could work with states to encourage more widespread inclusion of interoperability elements in these contracts going forward, ensuring provider networks are delivering high quality, safe care to Medicaid beneficiaries across the country through the use of health information technology, including health information exchange.

Section 1115 Waivers

Integration of health information exchange and health IT into state Medicaid programs can also be accomplished under demonstration authority at section 1115 of the Social Security Act (1115 demonstrations). Improved coordination of care through the exchange of health data is a key component that the demonstration programs can leverage and promote commercial health plans' efforts to improve quality of care and health outcomes and lower the

growth in costs of health care.[2] In addition, several states are advancing health information exchange in support of payment and delivery reform through Medicaid Delivery System Reform Incentive Payment (DSRIP) programs whereby the state can receive federal financing under a waiver for projects designed to improve access, quality and efficiency in the healthcare delivery system.

State Plan Amendments

States can also use the State Plan Amendment process to integrate health IT and health information exchange within their Medicaid state plans. Several states implementing health homes have done this to ensure health information exchange is enabling care planning and/or care coordination and successful implementation of their programs.

Medicaid Enhanced Funding: MMIS and HITECH Administrative Funding

CMS is able to provide funding for state administrative activities related to core interoperability services (e.g., designing and developing a provider directory, privacy and security applications and/or data warehouses), public health infrastructure, electronic Clinical Quality Measurement (eCQM) infrastructure and provider on-boarding. Funding for interoperability activities is already available to states through the Medicaid EHR Incentive Program. States may request 90/10 HITECH administrative funding for a wide range of interoperability activities that support meaningful use, including planning activities. States can also leverage existing Medicaid Enhanced funding authorities for multiple activities, including allowing patients to download their claims and/or clinical data that are housed in the states' MMIS.

State-Level Policy Levers for Reinforcing Interoperability and Exchange

In addition to leveraging federal funding, states can use state authorities in a variety of ways to drive interoperability, including: using state-level policy and programs to create a more supportive business environment for interoperability, operating health information exchange services directly according to standards-based approaches (as either an HIE or health care provider) and taking advantage of convening powers to encourage interoperability across state-level stakeholders.

State Policy and Programs

For the purposes of the Roadmap, state level policy generally means state laws, state regulations, state funding, and state programs (again, outside of Medicaid) that direct the spending of state money on providing care or influencing it in some way. The following represent examples of health IT-specific state level policy levers that states are currently employing or have proposed in support of exchange and interoperability:

- **Mandated connection to health information exchange.** Currently states such as Maryland, North Carolina and Vermont all have some form of mandated HIE connection.

2 http://www.medicaid.gov/medicaid-chip-program-information/by-topics/data-and-systems/section-1115-demonstration-hie-policy.html

- **State-level, standards-based interoperability requirements.** Minnesota law dictates that hospitals and care providers have an "interoperable electronic health records system."
- **Specific health IT mandates (e.g., eRx or electronic lab exchange).** Minnesota passed an e-prescribing mandate in 2011.
- **Creation of a dedicated state fund for health IT financed through claims transaction fees or other mechanisms.** Vermont currently assesses a fee (2/10ths of 1%) on health insurance claims for a state fund to support health IT and health information exchange.
- State-driven health IT adoption support. The state of North Dakota created a loan program for providers in the state to adopt health IT.
- **Leveraging health IT infrastructure for other uses within health care and beyond.** This may include alignment with states' Health Benefits Exchanges, advanced directives registries, PDMPs, non-health programs like Supplemental Nutrition Assistance Program enrollment and existing provider directories. One example of this is Maryland's health information organization (the Chesapeake Regional Information System for our Patients), which has partnered with the state Health Benefits Exchange to create a provider directory for patients to look up whether their providers accept certain insurance.
- **Leveraging state employee benefit requirements.** For example, the state of Arkansas has partnered with the Employee Benefits Division of the Arkansas Department of Finance and Administration to encourage the use of its state health information organization with all of its affiliated providers. Local governments also can take steps to leverage their purchasing power to reinforce interoperability.
- **Requiring health information exchange infrastructure as a public health conduit.** For example, in Alaska, all public health Meaningful Use measures must be submitted through the State health information organization.
- **Removing barriers to exchange through revised privacy and security policies.** Arizona, for example, passed two legislative packages in 2011 and 2012 affecting the state's consent policy and the state's notice of Health Information Practices to patients.

Operating Health Information Exchange Services

States can play a major role in driving interoperability when they directly operate exchange services or designate a third party to do so. While a number of states directly control the operations of a statewide health information exchange itself, others may develop exchange infrastructure to help coordinate care and share information across specific providers where the state has a significant interest, such as public health providers.

States directly enable interoperability when operating or establishing a third party to become a health information exchange entity. They can choose the architecture of their approach, which includes such decisions as what providers focus their connectivity efforts on, whether and how to allow for patient access, and even the standards they use for storing and transporting data. This role also allows states to determine fee structures for their services, which has major impacts on interoperability and exchange. Perhaps most importantly, states that are operating exchange entities also

control the governance/oversight of exchange activities. States can also take steps to ensure connectivity for providers ineligible for Meaningful Use. For example, Florida funded a survey of the perceptions of health information exchange by behavioral health centers.

States as Conveners

States have also had success in driving interoperability via their role as conveners, outside of the state's exchange oversight roles. This is important in the context of states' activities related to multi-payer alignment as part of delivery system reform efforts. Such convening may not directly consider exchange, but nevertheless has significant impacts on exchange across a variety of stakeholders. For example, states can convene stakeholders on quality measure alignment, which has the indirect benefit of making exchange of data more interoperable.

Convening can include broad-based listening sessions as a precursor to concrete planning activities. For example, the State of Vermont conducted public listening sessions related to health IT as part of the creation of the state's Blueprint for Health. It can also mean strategy sessions in pursuit of a particular goal such as the State of Michigan holding meetings to support its efforts to become a Learning Health State. Ultimately, states could create their own operational plans for supporting interoperability.

Health Plans

Value-based Payment Programs

Health plans have significant opportunities to advance interoperability within value-based payment arrangements they develop with providers. For instance, payers can make adoption of certified health IT systems or demonstration of interoperability a requirement for payment for providers that wish to take part in these programs. In markets with more advanced infrastructure for health information exchange, such as an active HIE, payers can consider partnering with the HIE and requiring participation by providers seeking to join these programs.

Within entry-level pay for value and pay for performance programs with individual practices, payers can make use of certified health IT a condition or link payments to other programs referencing IT requirements, such as medical home certification. Private plans can mirror Medicare policy to support chronic care management and require use of certified health IT. Payers can also include these requirements within more sophisticated arrangements, such as accountable care contracts covering commercial populations, in which groups of providers share in savings generated from more efficient care.

For private payers, these requirements help to ensure that participating providers are able to succeed within value-based payment programs through access to infrastructure that can support robust care coordination across settings of care and reduce unnecessary spending. Payers can also benefit from electronic reporting capabilities associated with use of interoperable health IT to streamline program administration.

Incentivizing Consumers

Private payers also have opportunities to advance consumer demand for interoperability by incentivizing consumers to choose providers that have advanced IT-enabled capabilities around care coordination. Today, payers are increasingly seeking to drive consumers to those providers that have a record of offering high-value, high-quality services. Payers can expand the parameters for high-value providers to take into account use of certified health IT, participation in a health information exchange or other indicator of advanced capabilities. Accordingly, consumers would receive a small incentive to choose these providers, such as lower copays.

Interoperability Requirements for Credentialing

Much in the same way that public payers could eventually include interoperability as part of the basic standard of care delivered by providers paid under public programs, commercial payers can also explore adding health IT and interoperability requirements to the factors included as part of credentialing processes for providers in their networks. If information regarding health IT capabilities were included as a standard component of credentialing information, payers could determine how to give preference to these attributes when identifying their networks.

Alignment for Value-Based Payment

To truly improve care across their patient populations, providers need access to information on patients' total cost of care across payers. Moreover, providers face considerable administrative burden related to managing multiple value-based programs that may have unique incentive and measurement requirements. To support greater alignment across payers, value-based payment models with multi-payer elements, such as the Comprehensive Primary Care Initiative, are providing an important Roadmap for public and private payers to work together.

Alignment of private payer efforts with CMS policies and programs, including incentives for health information exchange and e-clinical quality measures, will enable the three- and six-year goals in the Roadmap. In 2015, CMS intends to support a public-private partnership to increase alignment of key value based payment model attributes among payers and purchasers to facilitate adoption of payment reform goals. This partnership will provide a venue to collaborate across sectors and disseminate best practices and policies that could facilitate broader exchange of common clinical information to support care coordination across the care continuum.

Technical and Policy Components

Appendix B: Privacy Protections for Health Information

Ubiquitous, Secure Network Infrastructure

Cybersecurity

There are increasing cyber-attacks on electronic health information, particularly large stores of information. In 1998, Presidential Decision Directive (PDD) 63 acknowledged the need to protect the nation's critical infrastructure from both physical and cyber-attacks.[3] A major outcome of the PDD was the development of Information Sharing and Analysis Centers (ISACs) for each critical infrastructure sector. ISACs are, "privately led sector-specific organizations advancing physical and cyber security critical infrastructure protection by establishing and maintaining collaborative frameworks for operational interaction between and among members and external partners."[4]

One of the goals of an ISAC is to promote and enhance the bi-directional sharing about cyber threats and vulnerabilities within its sector-specific organizations and the federal government. This information sharing advances resilience, which is the ability to prepare for and respond to threats and vulnerabilities within a specific industry. ISACs are currently established for critical infrastructure sectors such as financial services, electricity and water. The National Health ISAC (NH-ISAC) is a non-profit industry-led effort to address the cyber security threats to health care and public health. In 2003, the Department of Homeland Security's *Presidential Directive 7: Critical Infrastructure Identification, Prioritization and Protection*, designated HHS as the Sector-Specific Agency responsible for ensuring the integrity of the health system.[5] A subsequent Presidential Policy Directive identified health care and public health (HPH) as a critical infrastructure sector.[6] Despite being identified as critical infrastructure for the nation, health care is one of the industry sectors least prepared for a cyber-attack, as it is not technically prepared to combat against cyber criminals' basic cyber intrusion tactics, techniques and procedures, much less against more advanced persistent threats.[7]

---

3 The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63. May 22, 1998. http://www.fas.org/irp/offdocs/paper598.htm

4 NIST Cybersecurity Framework

5 Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization and Protection. December 17, 2003. http://www.dhs.gov/homeland-security-presidential-directive-7

6 Presidential Policy Directive 21: Critical Infrastructure Security and Resilience. February 12, 2013. http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

7 http://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf

There are various factors within health care that contribute to the aforementioned cyber security challenge. The health IT ecosystem is composed of multiple systems that are interconnected, including EHRs, laboratory systems, patient portals, medical devices and many other systems. Consequently, the ecosystem is incredibly complex, with these systems being managed across an exponential number of organizations. As all of these health IT systems become connected to each other, the cyber threats increase at a significant rate, as an intrusion in one system could allow intrusions in multiple other systems

There are increasing cyber-attacks on electronic health information, particularly large stores of information. Despite being identified as critical infrastructure for the nation, the health care system could do more to prepare for a cyber-attack.[8],[9] There are various factors within health care that contribute to this aforementioned cyber security challenge. The health IT ecosystem is composed of multiple systems that are interconnected, including a wide variety of inputs that need security controls such as EKG machines, EHRs, robots and many other systems. Consequently, the ecosystem is incredibly complex, with these systems being managed across an exponential number of organizations. As all of these health IT systems become connected to each other, security risk can rise, as an intrusion in one system could allow intrusions in multiple other systems.

Additionally, there is high variability in the capabilities and resources that health care organizations have deployed to prevent cyber-attacks. Large organizations have the resources and expertise to have a dedicated information security team to address cyber security; however, small and mid-sized organizations may not have these resources and some may not be able to afford them. Finally, significant behavioral and cultural changes are necessary in the industry regarding the relevance of cyber security risks. Many in health care do not realize the significant risk to their systems and do not understand the importance and urgency of implementing security best practices to prevent cyber-attacks.

Encryption

Encryption of data both at rest and in transit is another component of a ubiquitous, secure network infrastructure. Encryption is a method of scrambling or encoding data so that it cannot be read without the appropriate key to unscramble the content. Two common ways encryption is used or applied are to send messages (particularly over networks that are not secure otherwise, like the Internet) and store data. These are sometimes referred to as information in transit and information at rest, respectively. In both cases, the core mechanism is the same. A program takes a piece of information (a string of data bytes) and changes it into another piece of information (a different string of bytes, and not necessarily the same number of bytes). The original piece of information is commonly referred to as being in the clear and the piece of information into which it is changed is referred to as encrypted. For encryption

8 http://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf

9 Note that on October 2, 2014 the FDA issued final guidance, "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices" that contains recommendations to medical device manufacturers on cybersecurity management and information that should be included in a pre-market submission.

to work, it must be possible for another program (or possibly another algorithm in the same program) to reverse the process and change the encrypted information back into the information in the clear. This is called decrypting. Another constraint is that the algorithm to decrypt should not be obvious; otherwise, unwanted recipients would be able to recover the original information.

Encryption of data at rest is in some aspects simpler than encryption of data in transit. Data at rest is encrypted and decrypted through capabilities of most major database management systems, most laptop operating systems and at least some mobile operating systems. Encryption of data in transit, however, may require appropriate software compatibility across a learning health system's technology as well as effective management of a public/private key environment.

Encryption technology is not being fully utilized in health care. OCR, in promulgating the breach notification regulations, created a safe harbor for electronic health data that was encrypted such that if that data was accessed, used, or disclosed while encrypted, it did not result in a reportable, remediable breach of electronic protected health information (ePHI). Despite this safe harbor, health IT systems have been slow to adopt encryption technology, both of data at rest and in transit and the result is that 33% of 2014 large breaches (affecting 500 or more individuals) reported to HHS were the result of a theft or loss of an unencrypted device containing protected health information.[10]

Permission to Disclose Identifiable Health Information

ONC's Fair Information Practice Principles

The Fair Information Practice Principles (FIPPs) are an internationally-recognized set of overarching principles that guide information practices while advancing technology.[11] They are foundational to many laws, regulations and policies in the public and private sector, including the HIPAA Privacy Rule, the Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information and many state laws and organization-level policies.[12] So too, this roadmap uses the FIPPS as a touchstone for building a privacy and security framework for

---

10 OCR data on large breaches (affecting 500 or more individuals) as of August 4, 2015, available at http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html

11 In 1973, the Department of Health, Education and Welfare (HEW) released its report, Records, Computers and the Rights of Citizens, which outlined a Code of Fair Information Practices that would create "safeguard requirements" for certain "automated personal data systems" maintained by the Federal Government. This Code of Fair Information Practices is now commonly referred to as fair information practice principles (FIPPs). See Department of Health, Education and Welfare, *Records Computers and the Rights of Citizens* (July 1973), available at http://www.justice.gov/opcl/docs/rec-com-rights.pdf. Note, the HEW eventually was re-named the Department of Health and Humans Services, HHS, which it is called to this day.

12 There are many versions of the FIPPs; the ONC FIPPs are in the Nationwide Privacy and Security Framework for Electronic Health Information Exchange ("Nationwide Privacy and Security Framework") released in 2008: http://www.healthit.gov/sites/default/files/nationwide-ps-framework-5.pdf. In 2012, ONC issued privacy and security guidance to the state health information exchange cooperative agreement program that is based on the Nationwide Privacy and Security Framework for Electronic Health Information Exchange. See ONC's State Health Information Exchange Program Instruction Notice (PIN), Privacy and Security Framework Requirements and Guidance for the State Health Information Exchange Cooperative Agreement Program, March 2012, http://www.healthit.gov/sites/default/files/hie-interoperability/onc-hie-pin-003-final.pdf.

Nationwide Privacy and Security Framework (based on the FIPPs)

1. INDIVIDUAL ACCESS: Individuals should be provided with a simple and timely means to access and obtain their individually identifiable health information in a readable form and format.
2. CORRECTION: Individuals should be provided with a timely means to dispute the accuracy or integrity of their individually identifiable health information and to have erroneous information corrected or to have a dispute documented if their requests are denied.
3. OPENNESS AND TRANSPARENCY: There should be openness and transparency about policies, procedures and technologies that directly affect individuals and/or their individually identifiable health information.
4. INDIVIDUAL CHOICE: Individuals should be provided a reasonable opportunity and capability to make informed decisions about the collection, use and disclosure of their individually identifiable health information.
5. COLLECTION, USE, AND DISCLOSURE LIMITATION: Individually identifiable health information should be collected, used, and/or disclosed only to the extent necessary to accomplish a specified purpose(s) and never to discriminate inappropriately.
6. DATA QUALITY AND INTEGRITY: Persons and entities should take reasonable steps to ensure that individually identifiable health information is complete, accurate and up-to-date to the extent necessary for the person's or entity's intended purposes and has not been altered or destroyed in an unauthorized manner.
7. SAFEGUARDS: Individually identifiable health information should be protected with reasonable administrative, technical and physical safeguards to ensure its confidentiality, integrity and availability and to prevent unauthorized or inappropriate access, use, or disclosure.
8. ACCOUNTABILITY: These principles should be implemented and adherence assured, through appropriate monitoring and other means and methods should be in place to report and mitigate non-adherence and breaches.

SOURCE: http://www.healthit.gov/sites/default/files/nationwide-ps-framework-5.pdf

interoperability. The Nationwide Privacy and Security Framework (based on the FIPPs) are specific objectives ONC identified in earlier work. Proposals below reference these principles.

The Nationwide Privacy and Security Framework FIPPs identify that individuals should be provided a reasonable opportunity and capability to make informed decisions (choice) about the collection, use and disclosure of their individually identifiable health information and that individuals need to understand their choice and how their information is used. ONC developed these FIPPS in a rules environment governed with a baseline of the HIPAA Rules, which permits the entities it regulates to access, use or disclose (exchange) protected health information (PHI) without an individual's written permission for treatment, payment and health care operations purposes (TPO) and which in certain other circumstances requires that the individual about whom the PHI pertains give written permission, in a document called an authorization, in order for the information to be shared.[13]

13 42 CFR § 164.508 (HIPAA authorization).

HIPAA Privacy Rule

The Health Insurance Portability and Accountability Act of 1996 (HIPAA), a federal law, serves as the foundation for federal protection of the privacy and security of individually identifiable health information. The HIPAA Privacy Rule, adopting principles established in the original 1973 HHS' FIPPs, sets standards governing the use and disclosure of PHI by covered entities (i.e. health plans including self-insured employer plans and insurance companies, health care clearinghouses and most health care providers – those who transmit any health information in electronic form in connection with specified administrative simplification transactions) and their business associates.[14],[15]

The HITECH Act mandated that the HIPAA Privacy and Security Rules be amended to directly apply parts of the HIPAA Privacy Rule and all of the HIPAA Security Rule to covered entities' business associates (i.e., third parties that perform certain functions or activities on behalf of the covered entity that require the use or disclosure of PHI including, for example, claims processing or data analysis). The HIPAA Privacy Rule also requires that covered entities supply individuals with a Notice of Privacy Practices, intended to fulfill the fair information privacy practices of transparency and notification.[16]

In general, the Privacy Rule provides that a covered entity may only use, or disclose protected health information without an individual's written permission, if the purpose of the use or disclosure is specifically permitted or required by the Rule. And it also specifies the circumstance in which the individual's written authorization is required before use or disclosure of the individually identifiable health information can occur and thus before an electronic exchange of health information (a disclosure) could occur. Of particular importance to a learning health system is the fact that the Privacy Rule permits the use and disclosure of PHI for TPO without express individual permission (called "consent" in this Roadmap and in other venues). Specifically, a covered entity may:

1. Use and disclose PHI for its own TPO activities,
2. Disclose PHI for the treatment activities of any other health care provider (regardless of whether the receiving provider is subject to the Privacy Rule)
3. Disclose PHI for payment activities of another covered entity and of any health care provider and
4. Disclose PHI for the health care operations of another covered entity involving either quality or competency assurance activities or fraud and abuse detection and compliance activities, if both covered entities have or

14 45 C.F.R. § 160.103.

15 45 CFR Parts 160, 162 and 164. Administrative simplification standards include the following transactions: (A) health claims or equivalent encounter information, (B) health claims attachments, (C) enrollment and disenrollment in a health plan, (D) eligibility for a health plan, (E) health care payment and remittance advice, (F) health plan premium payments, (G) first report of injury, (H) health claim status and (I) referral certification and authorization.

16 For model Notices of Privacy Practices, please visit http://www.healthit.gov/providers-professionals/model-notices-privacy-practices.

had a relationship with the individual and the PHI pertains to the relationship. Health Care Operations that meet this category are:

a. Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination; contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment;

b. Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance; health plan performance; conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers; training of non-health care professionals; accreditation, certification, licensing, or credentialing activities; and

c. Conducting or arranging for fraud and abuse detection and compliance programs.[17]

Under the HIPAA Privacy Rule, an individual's written authorization is not required for the sharing of health information for TPO. Although individual consent is not required, covered entities may (and often do) voluntarily choose to obtain an individual's consent, either opt-in or opt-out, ("Basic Choice") to use and disclose information about them for TPO.

Additional Requirements for Written Permission

Unlike the HIPAA basic structure, some state and other federal laws and regulations may require an individual's written permission before disclosing particular types of individually identifiable health information. In particular, these limits are often found in laws and regulations pertaining to "sensitive" health information. Thus, this type of law or regulation may impose additional limitations on the exchange of certain health information. A number of existing federal and state laws impose specific confidentiality requirements on particular types of health information in order to encourage patients to seek treatment (e.g., mental health related information). Some laws require that when sensitive health information is disclosed, the receiving organization be notified that it cannot further disclose the information without obtaining the patient's consent to do so. This restriction is often called a "prohibition on re-disclosure." One federal law that has this requirement is 42 U.S.C. § 290dd-2, which protects the confidentiality of information related to substance use treatment received through federally assisted programs. Many states currently have laws requiring an individual's consent to disclose health information related to mental health conditions, HIV status and substance use.[18]

17 45 CFR § 164.501, 45 CFR § 560(c); Disclosure of this type is subject to "necessity;" that is, only the information necessary for the purpose may be accessed, used or disclosed.

18 Consumer Partnership for eHealth. Protecting Sensitive Health Information, June 2010, at 2-3. Available at: http://www.nationalpartnership.org/site/DocServer/Sensitive-Data-Final_070710_2.pdf?docID=7041

Typically, the underlying purpose of these laws is to encourage greater participation and trust in the health care system by protecting a patient's most private and personal health information, and to prevent discrimination against the individual due to health status. The HIPAA Privacy Rule does not preempt these laws that require consent (where HIPAA does not), in part, because they are more protective of privacy than the HIPAA Privacy Rule.[19] Furthermore, in the wake of HITECH, some states also enacted laws to specify that among the conditions for which patients' consent was required to make their health information available for electronic health information exchange, [20] but this type of law has not been enacted in majority of states. Nor, does HIPAA require such a choice as its rules for accessing, using, disclosing and exchanging health information apply the same for all media (the HIPAA Security Rule applies to electronic transmission of data, but the Privacy Rule is not specific to electronic forms of data).

In addition to these laws, some organizations have developed their own internal policies requiring patient consent in order to share particularly sensitive information, or have adopted policies such that non-sensitive information may not be exchanged without a patient's written consent (despite the provisions of the Privacy Rule). Further, many stakeholders believe that individuals should have the ability to control access to the specific health information, or to specify which providers may have electronic access to it, even though democratically debated laws do not require that level of control.

The preceding paragraphs demonstrate that the U.S. legal, regulatory and policy landscape for sharing health information is complex. While HIPAA sets a "floor" as a federal law with its implementing regulations, state laws are often more restrictive than HIPAA and vary from state-to-state. This complexity hinders interoperability because stakeholders do not have the same standards for determining when patient "consent" is required, or when they may exchange health information without patient consent. Because stakeholders lack consensus and because the underlying laws and regulations may vary from state-to-state, it is difficult to develop nationwide-technical standards for documenting what access, use or disclosure rule applies and whether, when a patient's consent is legally required, it has been given.

Additional Policy Work on Individual Choice

ONC has received significant advice from federal advisory committees regarding a patient's choice to share his/her ePHI. In 2006, the National Committee on Vital and Health Statistics (NVCHS) made a number of recommendations to the Secretary of HHS regarding privacy and the Nationwide Health Information Network (NwHIN), [21]including a

19 Health Insurance Portability and Accountability Act of 1996, Pub. Law 104-191, § 1178 (a); 45 C.F.R. § 160.203 (2009).

20 NGA Center for Best Practices, State and Federal Consent Laws Affecting Interstate Health Information Exchange, March 2011, http://www.nga.org/files/live/sites/NGA/files/pdf/1103HIECONSENTLAWSREPORT.PDF

21 National Committee on Vital and Health Statistics (NCVHS). Letter to the Secretary of Health and Human Services re: Recommendations Regarding Privacy and Confidentiality in the National Health Information Network, June 22, 2006, http://ncvhs.us/wp-content/uploads/2014/05/privacyreport0608.pdf.

specific recommendation that patients be provided with choice regarding whether their ePHI is accessible via the NwHIN. The NwHIN exchange model was the only one in existence at the time of the NCVHS recommendations. Additionally, NCVHS recommended that HHS evaluate whether a national opt-in or opt-out policy would be appropriate and assess whether individuals should be able to control access to specific content within their health records.

In 2008 and 2010, NCVHS provided further recommendations focused on the exchange of sensitive health information. The recommendations emphasized that the NwHIN should be designed to permit individuals to "sequester," or restrict access to, specific sections of their health record in one or more predefined categories. NCVHS recommended defining this list of potentially sensitive categories and their contents on a national basis in order to achieve greater uniformity. Additionally, the group submitted a number of recommendations related to how these choices should be implemented in practice. For example, NCVHS recommended that where sensitive information has been sequestered, notations in the record transmitted should indicate that the record is not complete and access to the information should be provided in emergency situations.[22]

In 2010, the HITPC held public hearings on policies related to patient consent for participating in health information exchange, as well as technological means for implementing consent in an electronic environment.[23] While recognizing the promise of early developments, the HITPC recommended that ONC conduct further research into data segmentation and other such technologies in pilot studies to determine their workability and scalability.[24] "The same considerations and customary practices that apply to paper or fax exchange of patient health information should apply to direct electronic exchange. As always, providers should be prepared and willing to discuss with patients how their information is disclosed; to take into account patients' concerns for privacy; and also ensure the patient understands the information the receiving provider or clinician will likely need in order to provide safe, effective care."[25],[26]

Thus, as early as 2010, it was recognized that laws and regulations did not always require patient consent for exchange; instead it was recognized that consent was just one of eight FIPPs. This of course did not diminish the need for appropriate and interoperable technical standards for adjudicating permission and ensuring that downstream use complies with the permissions ("persistence") throughout the health information system. The HITPC recommendations

---

22 NCVHS. Letter to the Secretary of Health and Human Services re: Individual Control of Sensitive Health Information via the Nationwide Health Information Network for Purposes of Treatment, Feb. 20, 2008, http://www.ncvhs.hhs.gov/wp-content/uploads/2014/05/080220lt.pdf; NCVHS. Letter to the Secretary of Health and Human Services re: Recommendations Regarding Sensitive Health, Nov. 10, 2010, http://www.ncvhs.hhs.gov/wp-content/uploads/2014/05/101110lt.pdf

23 http://www.healthit.gov/sites/default/files/archive/index.php?dir=FACA%20Hearings/2010/2010-06-29%20Policy%3A%20Privacy%20%26%20Security%20Tiger%20Team%2C%20Consumer%20Choice%20Technology%20Hearing or http://healthit.gov/archive/?dir=archive_files/FACA%20Hearings/2010

24 http://www.healthit.gov/facas/sites/faca/files/hitpc_transmittal_p_s_tt_9_1_10_0.pdf

25 http://www.healthit.gov/facas/health-it-policy-committee/health-it-policy-committee-recommendations-national-coordinator-health-it

26 http://www.healthit.gov/facas/sites/faca/files/HITPC_Transmittal_08212013.pdf

did however, identify that consent was not required by law and regulation for a significant majority of potential health care exchange purposes that were not covered by more restrictive state or federal rules and regulations as discussed generally above.

In September 2011, to address these HITPC recommendations, ONC funded the Data Segmentation for Privacy (DS4P) Initiative [27] through the S&I Framework. DS4P gathered a community of experts, including software developers, health care providers, patient advocates and health informaticists, to assess health IT data standards and their practicality. Also in 2011, ONC funded the eConsent Trial project to develop and implement electronic and innovative ways to gather patients' input on areas in which they want to learn more about consent, to educate patients in a provider setting about the electronic sharing of their health information through an EHR and to capture and record choices patients make.[28]

In 2012, ONC released privacy and security guidance for the State Health Information Exchange Cooperative Agreement Program in response to these 2010 HITPC recommendations including individual choice. The guidance included the following: "Where HIE entities serve solely as information conduits for directed exchange of individually identifiable health information (IIHI) and do not access IIHI or use IIHI beyond what is required to encrypt and route it, patient choice is not required beyond existing law. Such sharing of IIHI from one health care provider directly to another is currently within patient expectations. Where HIE entities store, assemble or aggregate IIHI beyond what is required for an initial directed transaction, HIE entities should ensure individuals have meaningful choice regarding whether their IIHI may be exchanged through the HIE entity. This type of exchange will likely occur in a query/response model or where information is aggregated for analytics or reporting purposes."[29]

Also in 2012, ONC, in coordination with the HITPC, issued a Request for Comment (RFC) for Meaningful Use Stage 3 that included questions and considerations regarding patient consent.[30] In 2013, in response to the public comments received regarding the patient consent questions in the meaningful use stage 3 RFC, the HITPC referred to its recent recommendations on Query/Response regarding the technical mechanisms to support communication of patient consent requirements.[31]

---

27 http://www.healthit.gov/providers-professionals/ds4p-initiative

28 http://www.healthit.gov/providers-professionals/econsent-toolkit

29 ONC's Program Instruction Notice (PIN), Privacy and Security Framework Requirements and Guidance for the State Health Information Exchange Cooperative Agreement Program, March 2012, http://www.healthit.gov/sites/default/files/hie-interoperability/onc-hie-pin-003-final.pdf

30 http://www.healthit.gov/sites/default/files/hitpc_stage3_rfc_final.pdf

31 In particular, data holders and requesters should comply with applicable law and policy and should have a technical way to communicate applicable consent or authorization needs and requirements. They should also have a means to maintain a record of such transactions. http://www.healthit.gov/FACAS/sites/faca/files/HITPC_Transmittal_08212013.pdf

The HITPC recommended that the Health IT Standards Committee should further consider technical methods for giving providers the capacity to comply with applicable patient authorization requirements or policies. On the question related to data segmentation, [32] the HITPC deferred further discussion on the topic until it receives an update on the DS4P initiative pilot projects.[33] In 2013, ONC also released the *Principles and Strategy for Accelerating Health Information Exchange*, which noted that HHS will develop standards and policies to enable electronic management of consent and health information exchange among providers treating patients with sensitive health information such as those with behavioral health conditions or HIV.[34]

In 2014, as part of the HHS Secretary's Strategic Initiative focused on privacy, HHS committed to encouraging the development and use of policy and technology to advance patients' rights to access, amend and make choices for the disclosure of their electronic health information.[35] HHS also noted support for the development of standards and technology to facilitate patients' ability to control the disclosure of specific information that is considered by many to be sensitive in nature (such as information related to substance abuse treatment, genetic information, reproductive health, mental health, or HIV) in an electronic environment.

Most recently, the HITPC's Privacy and Security Tiger Team revisited the discussion of data segmentation's applicability to behavioral health information and in July 2014, the HITPC submitted recommendations to ONC for voluntary EHR certification criteria, contingent on readiness of specific standards that a recipient EHR can receive and automatically recognize documents from Part 2 providers, but the document is sequestered from other EHR data.[36] A recipient provider using DS4P would have the capability to view the restricted C-CDA (or data element), but the C-CDA or data cannot be automatically parsed/consumed into the EHR. Document level tagging can help prevent re-disclosure. In March 2015, ONC promulgated the 2015 Edition Health Information Technology (Health IT) Certification Criteria NPRM that included voluntary certification criteria that included the DS4P standard.[37] In June 2015, ONC released *The Consent Management Technology Landscape Assessment* on whether there are significant technical barriers to widespread electronic consent management.[38]

---

32 http://www.healthit.gov/providers-professionals/data-segmentation-overview

33 http://www.healthit.gov/providers-professionals/ds4p-initiative

34 Principles and Strategy for Accelerating Health Information Exchange (HIE). ONC. August 2013, http://www.healthit.gov/sites/default/files/acceleratinghieprinciples_strategy.pdf

35 Excerpt from HHS Secretary Strategic Initiative, Protect Patients Health Information and Privacy Rights, March 2014.

36 HITPC Recommendations to ONC, July 2014, http://www.healthit.gov/facas/sites/faca/files/PSTT_DS4P_Transmittal%20Letter_2014-07-03.pdf

37 ONC, 2015 Edition Health Information Technology (Health IT) Certification Criteria, Base Electronic Health Record (EHR) Definition, and ONC Health IT Certification Program Modifications, Mar. 30, 2015, http://www.gpo.gov/fdsys/pkg/FR-2015-03-30/pdf/2015-06612.pdf.

38 MITRE, commissioned by ONC, Electronic Consent Management Final Report, June 2015, http://www.healthit.gov/sites/default/files/privacy-security/ecm_finalreport_forrelease62415.pdf

Next Steps

Policy debates about the degree of control that individuals should have over health information are ongoing and will continue into the future, particularly as technology and cultural norms around privacy evolve and as the desire to exchange and use health information extends beyond the boundaries of traditional health care.[39] There are many details to be worked out in the interplay of state privacy laws enacted through open democratic processes, individual preferences, rights of individuals to access their records and providers' permissions to access, use and disclose under federal law (HIPAA).

Step one is to ensure that all health care stakeholders, from providers to individuals to lawmakers, understand how HIPAA as a legal baseline currently supports electronic, interoperable exchange of PHI among providers for TPO in a media neutral way, and understand how HIPAA requires that individuals be given access to their PHI, even in an electronic format, except under extremely limited circumstances. ONC, working with OCR, has begun this work with the publication in April 2015 of a new version of their Privacy & Security Guide aimed at small to medium-sized physician practices.[40]

Step two is to ensure that where organizations or states offer individuals a choice about whether their health information is available for electronic exchange for purposes of TPO, even though the HIPAA Privacy Rule does not require permission for information to be shared, it is clear what that choice is and when it is offered. We called this in the draft Roadmap, "Basic Choice." To start this second step, we clarify that "Basic Choice" refers to the choice offered to an individual to prevent their ePHI from being available for electronic exchange when it otherwise would be for purposes of TPO (without an individual's permission) because it is allowed by the HIPAA Privacy Rule, and no other laws requiring permission such as 42 CFR Part 2, or state enacted laws, apply.[41] The Privacy Rule, the nationwide health privacy law, does not require that individuals be provided Basic Choice when health information is exchanged for purposes of TPO. Some states have enacted laws regarding Basic Choice.[42],[43],[44]

There are many components to step two, including:

---

39 Health IT Policy Committee's Privacy and Security Working Group's Public Comments, April 2015, http://www.healthit.gov/sites/faca/files/Appendix_C_HITPC_PSWG_Interoperability_Roadmap_Comments_2015-04-07.pdf

40 http://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf

41 Basic Choice is a term ONC is using to describe the circumstance as defined. It is not intended to encompass a description of any other circumstance in which an individual may be offered or required to make a choice about where information about them is held or made available.

42 The National Governors Association, funded by ONC, published a landscape analysis of these laws that concern whether the patient wants to allow any of their information to be exchanged, often called "opt in/opt out." http://www.nga.org/files/live/sites/NGA/files/pdf/1103HIECONSENTLAWSREPORT.PDF

43 RTI International prepared for ONC, *Report on State Law Requirements for Patient Permission to Disclose Health Information*, August 2009, http://www.healthit.gov/sites/default/files/disclosure-report-1.pdf.

44 *Privacy and Security Solutions for Interoperable Health Information Exchange Report on State Medical Record*, Access Laws, August 2009, http://www.healthit.gov/sites/default/files/290-05-0015-state-law-access-report-1.pdf

- Ensuring that organizations or states that decide to offer individuals Basic Choice understand that if an individual chooses not to make their data available for electronic exchange, HIPAA will still permit an individual's providers to access, use, or disclose PHI to each other for purposes of TPO by other media without the individual's permission; mail, telephone, fax, etc.
- Ensuring that organizations or states that choose to offer individuals Basic Choice understand the different impacts an "opt in" model of choice has on individual health and a learning health system compared to "opt out", including:
  - Electronic health information may not be available to help treat the individual in an emergency if information is not made available, even where "break the glass" provisions exist;
  - Electronic health information available for a learning health system may be inadequate if insufficient people "opt in" or may be skewed by the demographics of the individuals who do opt in vs. those who do not opt in.
- Providing Health IT developers, policy-makers, providers, and patients with more concrete examples of the scenarios in which it is recommended that individuals be offered Basic Choice, even if not required, based on recommendations from the HITPC.
- Identifying technical standards the health care stakeholder can adopt so that Basic choice, if offered to individuals, is offered in a technically standard way and individuals can more easily make choices electronically and online, including:[45]
  - Guidance that defines computable, discrete data fields needed for negotiating individual permission and access to health information. Common semantics for discrete data fields would further assist in determining whether the protected health information or personally identifiable information should be shared, and documentation protocols consistent with eSIGN Act.[46]
- Helping to ensure that individuals understand the choice they are making when they make a Basic Choice, as discussed above: Individuals understand how their electronic health information is being moved (exchanged) for TPO, what their options are for "Basic Choice" and how their information will be protected, used or disclosed even if an individual does not document a choice.

Step three is tackling the wide variety of laws and organizational-level policies regarding health information divided into many different sub-categories, some of which require written permission from the individual before others can access, use or disclose the information even for treatment. There are two subcategories of what the Roadmap calls "granular choice":

---

45 For example, if a data holder is subject to laws, to assist providers in complying with applicable law and policies, parties to a query/response should have a technical way to communicate applicable consent/authorization needs or requirements, and maintain a record of such transactions. HITPC Recommendations to the National Coordinator, Aug. 2013, http://www.healthit.gov/FACAS/sites/faca/files/HITPC_Transmittal_08212013_0.pdf. Query Response Public Hearing, June 2013 http://healthit.gov/archive/?dir=archive_files/FACA%20Hearings/2013/2013-06-24%20Policy%3A%20Privacy%20%26%20Security%20Tiger%20Team%20Hearing.

46 The Electronic Signatures in Global and National Commerce Act (ESIGN, Pub.L. 106–229, 114 Stat. 464, enacted June 30, 2000, 15 U.S.C. ch. 96) http://www.gpo.gov/fdsys/pkg/PLAW-106publ229/html/PLAW-106publ229.htm

- Where law requires that an individual actively choose to allow information about them to be accessed, used or disclosed because of the *clinical nature of the information*, such as a specific type of disease or the age of the individual.
- Where an individual might want to make a choice to share or to withhold information for a reason not specified in law, for example by specific provider or payer types, or to specific organizations for purposes such as research.

To fully enable computable granular choice, an important first step is harmonizing the content of applicable laws themselves—laws that fall into the first category of granular choice. Increasing harmonization reduces variation in laws so that rules-engines can process and act on electronic documentation of granular choice.

When we have successfully brought the power of technology to the compliance task of the first category of granular choice, we will build the second category of granular choice using standards developed for the first category.

While the health IT ecosystem should support efforts to more deeply discuss how to harmonize such laws so that computing power can be applied to granular choice, the health IT ecosystem needs to collectively ensure that special legal protections that apply as a result of deliberative legislative processes remain in place.[47] Through the course of harmonization, individual privacy rights as specified in state and federal laws must not be substantively eroded.

Appendix C: Core Technical Standards and Functions

National Information Exchange Model (NIEM)

The National Information Exchange Model (NIEM) is a national program to increase information sharing among organizations at the federal, state and local levels. Its Human Services Domain is used increasingly across HHS to help standardize interoperability of human services exchange use cases. The NIEM model is designed for exchanging information between disparate systems without being intrusive to those domains. NIEM is implementation agnostic, meaning it can serve as an overlaying system-to-system exchange model without ever touching or changing the underlying systems' software code or structure. NIEM is focused on the reusability and standardization of its data model: an expansive, carefully curated XML schema. NIEM enables the structured use of standards, documented in an online repository of information exchange package documentations (IEPDs) to support information sharing.

NIEM is increasingly utilized across HHS, with the Agency for Children & Families playing an important leadership role in the NIEM Human Services domain.[48] ONC is the steward of the NIEM Health domain.[49] There are opportunities to extend

47 ONC's Report to Congress: Health Information Blocking, April 2015, p. 37 – 38, http://www.healthit.gov/sites/default/files/reports/info_blocking_040915.pdf

48 https://www.niem.gov/communities/hs/Pages/about-hs.aspx

49 https://www.niem.gov/communities/emc/health/Pages/about-health.aspx

NIEM's extensive catalog of exchange protocols and procedures to include examples of bi-directional, health care to human services interoperability. States are currently using NIEM to define and pilot State-to-State exchange between PDMP registries. The CMS Federal Hub that authenticates individuals for the CMMI Health Marketplace subsidy and CMCS Medicaid eligibility uses NIEM to document the exchange requirements between the States, CMS, IRS, SSA and DHS.

A multi-pronged approach and engagement on the part of stakeholders across the ecosystem will be required to clarify NIEM's potential and to develop and recommend strategies for use of the NIEM model for approaches to health care and human services information sharing. While ONC can assist in the coordination of delivery system reform efforts working on bi-directional health care exchange with human services to encourage collaboration across jurisdictions, states and other stakeholders across the ecosystem will need to play an active role in determining the role of NIEM to support health care and human services interoperability.

A key area of focus for the role of NIEM could be in relation to the Medicaid Information Technology Architecture (MITA) and interoperable exchange between State Medicaid systems and Health Information Exchange organizations. States and others should develop one or more use cases for health care and human services information sharing and produce one or more Information Exchange Package Documentation Specifications (IEPDs) based on the requirements of evolving accountable, outcomes-focused payment arrangements and delivery system innovations. Such work will form the basis for widespread sharing of health and human services that impact health data to support coordination of care and services across the health and human services ecosystem.

Accurate Individual Matching

In 2013, ONC undertook an environmental scan on identity matching across the country. The scan included health systems, EHR developers, health information exchange developers and master patient index developers. The report from the environmental scan released in 2014 found that data quality was identified by nearly all participants as a key issue in identity matching. Additionally, few organizations had insight into how well they are performing on identity matching, with very few able to report false positive and false negative rates and in fact, disagreement amongst the organizations on what should be being measured in matching. Finally, there was not unilateral agreement in the industry on which match methods work the best. When requesting patient records from electronic health record systems, there are at least two technical profiles for identity matching in common use today. Both profiles were created and are maintained by IHE[50]: Patient Identifier Cross Referencing (PIX)/Patient Demographics Query (PDQ), for internal system use and Cross-Community Patient Discovery (XCPD) for external use. These profiles describe the method used to send patient data element queries within an organization (PIX/PDQ), or externally to another organization (XCPD) to ask if it has records matching a specific patient and for that receiving organization to respond whether or not it has records.

50 http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol1.pdf and http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol2b.pdf

The second major component to matching is the matching method itself. There are two primary methods in use today: deterministic matching and probabilistic matching (i.e. algorithm and tuning). Deterministic matching uses sets of pre-determined rules to guide the matching process and normally requires that data elements match exactly. Probabilistic matching is a process where an estimate is made of the probability that two records are for the same person based on the degree to which certain fields in the two records match. Two thresholds are then set: all record pairs whose probability is above the higher threshold are considered to be matches. All record pairs whose probability is below the lower threshold are not considered matches. The disposition of record pairs whose probability falls in between the two thresholds is considered to be uncertain and they require additional review, likely by a trained staff member.[51] Both of these matching methods, as well as a combination of the two, are used across the industry and there has not been a significant study on which method performs better.

These methods utilize a statistical matching approach, which presents a higher chance of ambiguity—that a record might belong to more than one individual. The process for parsing ambiguous records to ensure a correct match between a patient and records—known as *disambiguation*—is both more essential and more complex in statistical matching, because the number of potential matches and the types of information available are greater. As the need for this kind of parsing becomes greater, it often requires human involvement, at which point the advantages of automation maybe lost, particularly efficiency and interoperability. Both of these matching methods, as well as a combination of the two, are used across the industry and there has not been a significant study on which method performs better.

Health Care Directory Standards

A number of technical standards have been developed and implemented to support directory services for resource location. For example, the eHealth Exchange specifications use Universal Description Discovery and Integration (UDDI) as the method to search and retrieve information about organizations, including how to perform patient discovery, query for documents, retrieve documents and submit documents. However, eHealth Exchange is largely phasing out the UDDI specification due to its lack of extensibility and is instead looking to use IHE's HPD specification to support its directory needs. IHE has also created and maintains three profiles for standards-based health care-related directories including the Personnel White Pages (PWP) profile,[52] the Care Services Directory (CSD) profile[53] and the Healthcare Provider Directory (HPD) profile.[54] The profile receiving the most industry attention, including among eHealth Exchange, is HPD which provides mechanisms to locate individuals and organizations, the relationships between them and Direct addresses or electronic service information.

---

51 Record linkage software in the public domain: A comparison of Link Plus, the Link King and a "basic" deterministic algorithm. Campbell, K. M., Deck, D., & Krupski, A. Health Informatics Journal, 14(1), 5–15: 2008. http://jhi.sagepub.com/content/14/1/5.long

52 http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol1.pdf

53 http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_CSD.pdf

54 http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_HPD.pdf

The EHR I HIE Interoperability Work Group (IWG) created a significant extension to the HPD standard including the creation of additional objects in the HPD Lightweight Directory Access Protocol (LDAP)-based data model to support organizations, sub-organizations, relationships among them and the electronic services they offer. Early in 2013, ONC launched a ModSpec project to produce a testable set of requirements and funded the Exemplar HIE Governance Program to pilot test HPD+ and a new specification resulting from the ModSpec efforts. The pilot had four significant findings:

1. The multitude of HPD standards and implementation guides has resulted in an incompatible set of provider directory deployments across the country.
2. The use of different provider specialty nomenclatures in different provider directories could affect interoperability between directories.
3. There was broad agreement that the new ModSpec specifications needed to go through the IHE approval process, in order to ensure widespread technology developer acceptance.
4. The scope of all of the published implementation guides for provider directories did not include federation, nor any guidance regarding harmonization across an environment involving multiple provider directories.

After the pilots, ONC worked with IHE to update the HPD specification and include an optional extension to support federation. The IHE HPD implementation guide was released in October 2014 and can currently be tested on ONC's Standards Implementation & Testing Environment site.[55] The HPD standard may have limitations, as it was built to support directories of individuals and organizations, not services or even Direct addresses. It can be used to discover electronic services, but may not be efficient or flexible enough for the future needs of a learning health system. For example, it can easily hold a URL, but perhaps not the WSDL or content constraints, and therefore does not completely describe an API.

Finally, the CSD profile has been on IHE's planning Roadmap to move beyond HPD. Unlike HPD, CSD was intended as a way to discover services for individuals and organizations. Services in CSD include both clinical services (to answer questions like "what dermatologists are there within 10 miles of my home and when are they available for an appointment?"), as well as technical or electronic services (to answer questions like "what is the service for discovering patients at Private Dermatology Specialists where Dr. Smith practices?"). A portion of the CSD standard includes busy status and therefore it supports scheduling. CSD has similar data elements as the current version of HPD, but a different architecture. It is not based on LDAP but it does have a federation model that is part of the profile. It can represent individuals and organizations, their relationships and clinical and electronic services associated with those relationships. CSD is a new standard, just approved for test implementation in 2014. As such, it is not yet clear whether CSD will be better suited to support the type of resource location necessary in a learning health system.

55 www.sitenv.org

Outcomes

Appendix D: Efforts to Promote Individuals' Engagement with Their Health and Health Care

Over the last few years, ONC, CMS and other stakeholders have implemented a number of policies and programs to promote individual engagement with their health care. These activities are described in detail below.

Meaningful Use Stage 2

One objective of Meaningful Use Stage 2 regulations is to provide patients with the ability to view online, download and transmit (VDT) their health information within four business days of the information being available to the Eligible Professional (EP). On the inpatient side, eligible hospitals are required to provide patients the ability to view online, download and transmit information within 36 hours of discharge. Providing patients with an electronic copy of their health information helps them and their caregivers have the information they need to engage more in their care and enables them to identify potential errors or omissions in their records. In addition, having information readily available is useful when patients change providers, seek a second opinion, or are seeing multiple providers during the same time period. They have the ability to share their health information to make sure everyone is on the same page to support care coordination and self-management. This is increasingly important given that one in three individuals reported experiencing one or more gaps in health information exchange within the past year. Even as electronic health information exchange becomes more prevalent, consumers will play an important role managing their own and their loved ones' health information.

Blue Button

Through the public-private Blue Button Initiative,[56] ONC and its supporters are increasing individuals' electronic access to their clinical and claims-related health information from diverse sources. The voluntary Blue Button Pledge program has over 500 organizations, including federal agencies, health care provider systems, health insurance plans, labs, retail pharmacies and others who have committed to enabling consumer access to their online health data or to getting the word out to fuel more consumer awareness and demand for access to their digital health data. In 2013, ONC convened focus groups, did consumer testing and developed a set of public service announcement (PSA) videos and posters about Blue Button, customized to three diverse population groups and secured commitments from influential organizations to distribute these materials in 2014 via an ongoing national Blue Button Campaign.[57]

56 www.HealthIT.gov/bluebutton

57 http://www.healthit.gov/buzz-blog/consumer/launching-fall-national-blue-button-consumer-campaign/

ONC also worked closely with the public to outline the technical standards supporting the ability for consumers to access their health information and for data holders and developers to go a step further and allow consumers to move their data from provider systems to the tools and services they designate. These standards and guidance can be found in the Blue Button Toolkit, formerly known as Blue Button +. ONC has also seeded competitions to help spur the development of consumer-friendly health applications that are able to ingest structured health data from traditional EHR systems. The Blue Button Co-Design Challenge[58] for example, has led to the development of seventeen consumer apps that accept Blue Button structured data.

Consumer eHealth Program

Through its Office of Consumer eHealth (OCeH), ONC catalyzes, coordinates and inspires others to support consumer engagement via eHealth by influencing policy and standards development, convening diverse stakeholders, building public-private partnerships and providing thought leadership through writing and public speaking. OCeH's efforts span its "three A's" strategy for consumer engagement via eHealth: increase people's access to their own digital health information; ensure that information is actionable via apps and tools; and promote a change in attitudes regarding traditional consumer and provider roles. OCeH works closely with several other offices at ONC (including the Office of Policy and Planning), federal partners and members of the private sector on a variety of activities to advance consumer engagement priorities. OCeH works to integrate the consumer voice across ONC, to make sure that policies, standards, definitions, certification and privacy work relate to both patients and providers.

Federal Advisory Committee Workgroups

Two workgroups made up of volunteer subject matter experts, the HIT Policy Committee's (HITPC) Consumer Empowerment Workgroup and the HIT Standards Committee's (HITSC) Consumer Technology Workgroup, issued joint recommendations to the two committees in 2014 about how to support the use of patient-generated health data in the next stage of meaningful use of EHRs. A third workgroup, the HITPC Accountable Care Workgroup, plans to consider how to increase patient activation as a member of a defined care team, engage patients in assessments of their health and use technology to deliver care to patients outside of traditional care settings.

Investing in Innovation (i2) Program

ONC created the Investing in Innovation (i2) program to award prizes competitively to stimulate innovation. The competitions offered by this program, also referred to as health IT developer challenges, focus on innovations that support the following: 1) the goals of HITECH and clearing hurdles related to the achievement of widespread health IT adoption and meaningful use; 2) ONC's and HHS' programs and programmatic goals; and 3) the achievement of a nationwide learning health system that improves quality, safety and/or efficiency of health care. Through the challenges, ONC has spurred industry innovation in Consumer eHealth, including the development of apps that use

58 http://www.healthit.gov/buzz-blog/health-innovation/onc-announces-winners-blue-button-challenge/

Blue Button + structured data, of which there are now more than 17. The program also hosted a Blue Button Design Challenge in 2013 to challenge designers across the country to reimagine the patient health record.

VA's Innovation Program

The US Department of Veterans Affairs manages the VA Center for Innovation that includes an Industry Innovation Competition. The VA Center for Innovation identifies, tests and evaluates new approaches to efficiently and effectively meet the current and future needs of veterans through innovations rooted in data, design-thinking and agile development. It has been in existence since 2010 with over 18,000 ideas submitted and numerous innovations that have led to improvements at the VA.

Care Planning

As the capabilities of health IT tools increase and a national infrastructure for electronically sharing health information becomes more ubiquitous, individuals and stakeholders across the care continuum are converging around a vision where a single care plan can be captured, dynamically updated and utilized in a secure and appropriate fashion by individuals, caregivers and any member of the individual's virtual, interdisciplinary care team. A range of program requirements within Medicare and Medicaid and other federal programs indicate that participating clinicians must develop care plans as part of their services for beneficiaries.

New initiatives continue to emphasize the importance of a care management program in the Physician Fee Schedule. In addition, payment reform models being advanced at the local, state and federal levels are increasingly pointing to care plans as a way to support needed care coordination, quality improvement and cost reductions. Finally, care coordination has been established as one of the six priorities of the National Quality Strategy developed under the Affordable Care Act; effective shared care planning across institutions is widely acknowledged as one of the key tools for achieving more robust care coordination. Through the S&I Longitudinal Work Group, several sites have implemented the pre-ballot C-CDA R2.0 and several organizations demonstrated Care Plan exchange using pre-ballot C-CDA R2.0.

Patient-Generated Health Data

Patient-generated health data are health-related data—including health history, symptoms, biometric data, treatment history, lifestyle choices and other information—that is created, recorded, gathered or inferred by or from patients or their designees (i.e., , care partners or those who assist them). This data is distinct from data generated in clinical settings and through encounters with providers in two important ways. First, patients, not providers, are primarily responsible for capturing or recording these data. Second, patients direct the sharing or distributing of these data to recipients of the individual's choosing, which range from caregivers to health care providers and other stakeholders. There are no widely established policies and practices to define the optimal use of patient generated health data, much less support it. A framework of policies and good practices can help to successfully engage physicians and patients

and ensure the privacy, security and appropriate use of this data. ONC has initiated several activities to advance knowledge of the field and identify policies and promising practices to support it.[59]

Personalized Health Care

While the concept of personalized health care is not new, genomic, proteomic and other discoveries are accelerating the tailoring of patient treatments, risk assessment and diagnostic reasoning. The 2008 publication of the *Priorities for Personalized Medicine* report to the President's Council of Advisors on Science and Technology (PCAST) described personalized medicine as, "the tailoring of medical treatment to the specific characteristics of each patient… [involving]… the ability to classify individuals into subpopulations that are uniquely or disproportionately susceptible to a particular disease or responsive to a specific treatment."[60]

The use of health IT can support shared decision-making and increased communication in clinical practice, helping providers and patients to manage and use patient-specific information. In 2012, ONC conducted some initial research on personalized health care to better understand the current landscape and the definition of the topic. As a result, challenges were identified and health IT-related policy areas are under consideration.

Appendix E: Medication Use and Management

Use of pharmaceuticals is a mainstay in the delivery of evidence-based medical care. In fact, approximately half of all Americans take a prescription medication each month and in 2010, there were 2.6 billion medications ordered or prescribed.[61] The need remains to build health IT infrastructure that supports both optimal and safe use of pharmaceuticals. There are more than 770,000 injuries and deaths each year due to adverse drug events.[62]

Electronic prescribing (or e-prescribing) refers to the process where a prescriber generates and transmits an "accurate, error-free and understandable" prescription directly to a pharmacy through a secure network.[63],[64] With the advent of e-prescribing[65] and associated clinical decision support systems, many of the safety concerns inherent in paper-

---

59 http://www.healthit.gov/policy-researchers-implementers/patient-generated-health-data.

60 http://www.whitehouse.gov/files/documents/ostp/PCAST/pcast_report_v2.pdf

61 CDC. 2014. http://www.cdc.gov/nchs/data/hus/hus13.pdf

62 Reducing and Preventing Adverse Drug Events to Decrease Hospital Costs, Publication #01-00. Agency for Healthcare Research and Quality (AHRQ). 2001.

63 CMS. E-prescribing. http://www.cms.gov/Medicare/E-Health/Eprescribing/index.html?redirect=/eprescribing/.

64 Department of Health and Human Services Health Information Technology and Quality Improvement. How does e-prescribing work? http://www.hrsa.gov/healthit/toolbox/HealthITAdoptiontoolbox/ElectronicPrescribing/epreswork.html.

65 IOM Committee on Identifying and Preventing Medication Errors. Preventing Medication Errors: Quality Chasm Series. Washington, DC: National Academies Press; 2007

based prescribing have been eliminated.[66] Despite these advances, the full potential of e-prescribing is yet to be realized. A high quality e-prescribing process can support higher-level functions, such as medication reconciliation and medication adherence.

Apart from the gains in efficiency and safety that e-prescribing allows, the opportunity exists to use these processes to address growing challenges in health care, such as the prescription drug abuse epidemic.[67],[68],[69] Although 49 states now allow electronic prescribing of controlled substances, less than 1% of providers are currently sending prescriptions for controlled substances electronically.[70] Ubiquitous use of electronic prescribing of controlled substances will enable health care providers, as well as state entities, to better track use of highly addictive medications and deploy appropriate resources and interventions to areas in need. A second component to addressing this epidemic is Prescription Drug Monitoring Programs (PDMPs).

PDMPs are secure, state-administered electronic databases that track the prescribing and dispensing of controlled substances and other prescription drugs of concern. PDMPs can be a powerful tool in the hand of health care providers. Evidence continues to accumulate that PDMPs are effective in improving clinical decision-making, reducing "doctor shopping" (utilizing more than one prescriber to obtain controlled substance prescriptions) and the diversion of controlled substances and assisting in other efforts to curb the prescription drug abuse epidemic. However, a significant barrier to increased use and interoperability is the lack of standard methods to exchange and integrate data from PDMPs to health IT systems, meaning that accessing PDMP data is not easily integrated into the e-prescribing workflow.

Today, 49 states and one U.S. territory (Guam) currently have a PDMP that is operational (meaning collecting data from dispensers and reporting information from the database to authorized users). Despite progress in making PDMPs operational, efforts are needed to further facilitate the exchange of PDMP data across state lines. Secure and standardized interstate data sharing would allow prescribers full visibility into patient prescription fill patterns and reduce or eliminate doctor and pharmacy shopping that occurs across state lines. As of November 2014, 29 state PDMPs can share data across state lines with other states' databases.

---

66 Sirajuddin AM, Osheroff JA, Sittig DF, Chuo J, Velasco F and Collins DA. Implementation Pearls from a New Guidebook on Improving Medication Use and Outcomes with Clinical Decision Support. Effective CDS is Essential for Addressing Healthcare Performance Improvement Imperatives. J Healthc Inf Manag. 2009 Fall; 23(4): 38–45

67 Fischer MA, Vogeli C, Stedman M, Ferris T, Brookhart MA, Weissman JS. Effect of electronic prescribing with formulary decision support on medication use and cost. Arch Intern Med 2008; 168(22):2433-39.

68 Fischer MA, Stedman MR, Lii J, Vogeli C, Shrank WH, Brookhart MA et al. Primary medication non-adherence: analysis of 195,930 electronic prescriptions. J Gen Intern Med 2010; 25(4):284-90.

69 Lapane KL, Rosen RK, Dube C. Perceptions of e-prescribing efficiencies and inefficiencies in ambulatory care. Int J Med Inform 2011; 80(1):39-46.

70 Gabriel MH, Yang Y, Vaidya V and Wilkins TL. Adoption of Electronic Prescribing for Controlled Substances Among Providers and Pharmacies. Am J Manag Care. 2014;20(11 Spec No. 17):SP541-SP54.

Comprehensive Medication Management (CMM) is a process by which the appropriateness, effectiveness, safety and compliance of pharmaceutical treatments is evaluated. There are four general steps in the process that require involvement of multiple members of the health care team: 1) assessing the patient's medication needs; 2) identifying any medication-related problems; 3) developing a care plan that includes the patient's personalized goals; and 4) monitoring and follow-up to determine and document patient outcomes.[71] There is evidence to suggest that current efforts at practice transformation and care redesign still require additional effort in order to achieve quality benchmarks through optimal medication use.[72]

Pharmacists are health care professionals with skills and expertise that uniquely position them to work with other health care providers to successfully manage patient mediation therapies. Pharmacists routinely consult on choice and selection of appropriate medication therapies, evaluate the effectiveness of treatment by monitoring clinical endpoints such as laboratory values and patient-reported outcomes, recommend dosing adjustments to tailor clinical response, assess the safety profile of medications and evaluate patient risk for adverse outcomes, monitor and evaluate patient adherence and counsel patients on appropriate use and understanding of their treatments. One such activity of CMM routinely performed by pharmacists is medication therapy management (MTM). MTM consults are now required by the CMS Part D Prescription Drug Program and are particularly valuable at points when patients are transitioning between settings of care, when the risk of lost information and gaps in care is increased. Despite the known value of MTM services, technological barriers to information exchange limit the ability of MTM documents and associated recommendations to be shared with ease between settings of care.

Appendix F: Glossary

Access Control Services (ACS)

Access Control service provides the mechanism for security authorizations that control the enforcement of security policies including: role-based access control, entity based access control, context based access control and the execution of consent directives.
http://www.hitsp.org/ConstructSet_Details.aspx?&PrefixAlpha=12&PrefixNumeric=108

Accountable Care Organizations (ACO)

Groups of doctors, hospitals and other health care providers, who come together voluntarily to give clinically coordinated care to their patients, often using payment forms other than fee-for-service.
https://www.cms.gov/Medicare/Medicare-Fee-for-Service-Payment/ACO/index.html?redirect=/aco/

71 Patient Centered Primary Care Collaborative. The Patient-Centered Medical Home: Integrating Comprehensive Medication Management to Optimize Patient Outcomes Resource Guide 2012 2nd Edition.

72 Dubois RW, Feldman M, Lustig A, Kotzbauer G, Penso J, Pope SD and Westrich MA. Are ACOs Ready to be Accountable for Medication Use? J Manag Care Pharm. 2014;20(1):17-21.

Accredited Standards Committee (ASC) X12

Develops and maintains electronic data interchange standards for global business markets, including standards for health care, insurance, transportation, finance, government, supply chain and other industries.
http://www.x12.org/

Admit/Discharge/Transfer (ADT) messages

Admission, Discharge and Transfer (ADT) messages are used to communicate episode details. ADT messages carry patient demographic information for HL7 communications, but also provide important information about trigger events (such as patient admit, discharge, transfer, registration, etc.). ADT messages are extremely common in HL7 processing and are among the most widely used of all message types.
http://www.gillogley.com/hl7_glossary.shtml
http://www.corepointhealth.com/resource-center/hl7-resources/hl7-adt

Agency for Healthcare Research and Quality (AHRQ)

The Nation's lead federal agency for research on health care quality, costs, outcomes and patient safety. The AHRQ's mission is to produce evidence to make health care safer, higher quality, more accessible, equitable and affordable and to work within the U.S. Department of Health and Human Services and with other partners to make sure that the evidence is understood and used.
http://www.ahrq.gov/cpi/about/

American Health Information Community (AHIC)

The American Health Information Community was a federally chartered advisory committee that was formed in 2005-2008 to make recommendations to the Secretary of the U.S. Department of Health and Human Services on how to accelerate the development and adoption of health information technology.
http://www.phdsc.org/health_info/american-health-info.asp

Application Program Interface (API)

An acronym standing for "Application Program Interface," an API is a software application function that can be invoked or controlled through interactions with other software applications. APIs allow the user experience to be seamless between two or more software applications since the APIs are working behind the actual user interface. For the purpose of the Roadmap the term is further defined as being specific API's that are in wide use and universally supported for particular functions across multiple technology developers' products. They are published and accessible in a way that makes them easy for interested developers to find and use without a program host system intervention and for which there are no fees or other intellectual property restrictions that limit their availability to any competent and interested programmer. *Note: for this interoperability roadmap, the term is used as defined in this glossary.*

Architecture

The term "Architecture" is used in this report to refer to the collective components of a software system that interact in specified ways and across specified interfaces to ensure specified functionality.
http://healthit.gov/sites/default/files/ptp13-700hhs_white.pdf

Authentication

Authentication and access control measures should ensure appropriate access to information and information processing facilities – including mainframes, servers, desktop and laptop clients, mobile devices, applications, operating systems and network services – and prevent inappropriate access to such resources.
http://it.med.miami.edu/x2232.xml

Authorization

Authorization represents the amount or type of information a person or system is allowed to access. For example, the absence of any authorization means a person or system may not access any information. Authorization to access all information means a person or system may access 100% of the information in the system. Authorization to access information regulated by 42 U.S.C. § 290dd-2, means that information about that patient's substance abuse treatment could be released to the particular person who has been authorized to receive it. *Note: in other and prior health care contexts the term "authorization" may have been used in other ways, but for this interoperability roadmap, the term is used as defined in this glossary.*

"Basic" Choices

The choice offered to an individual to prevent their ePHI from being available for electronic exchange when it otherwise would be for purposes of TPO (without an individual's permission) because it is allowed by the HIPAA Privacy Rule, and no other laws requiring permission such as 42 CFR Part 2, or state enacted laws, apply. *Note: for this interoperability roadmap, the term is used as defined in this glossary.*

Blue Button Initiative

Blue Button is a tool to make patient medical records easily available for patients to download and share with members of their health care team. It allows individuals to create a single electronic file that can include all of their available personal health information.
http://www.va.gov/bluebutton/
http://bluebuttonconnector.healthit.gov/

Business Associate Agreement (BAA)

A contract between a HIPAA covered entity and its business associate or a business associate and its subcontractor that must contain the elements specified at 45 CFR § 164.504(e). For example among other requirements, the

contract must: Describe the permitted and required uses of protected health information by the business associate; Provide that the business associate will not use or further disclose the protected health information other than as permitted or required by the contract or as required by law; and Require the business associate to use appropriate safeguards to prevent a use or disclosure of the protected health information other than as provided for by the contract.

Care Connectivity Consortium

Founded in April 2011, the CCC is a consortium of health care providers working to improve and advance the technology available for comprehensive, secure, reliable and innovative electronic health information exchange across the country. Founded by five organizations — Geisinger Health System, Kaiser Permanente, Mayo Clinic, Intermountain Healthcare and Group Health Cooperative — its missions are to: develop solutions that enhance the capabilities of current technologies; allow more secure, reliable and effective sharing of data among disparate health record systems; offer these solutions to the broader HIE community; and accelerate the adoption of national HIE standards.
http://www.careconnectivity.org/about/details/

Centers for Disease Control and Prevention (CDC)

The Centers for Disease Control and Prevention (CDC), an agency within the U.S. Department of Health and Human Services, is the primary federal agency for conducting and supporting public health activities in the United States. CDC's mission is to collaborate to create the expertise, information and tools that people and communities need to protect their health — through health promotion, prevention of disease, injury and disability and preparedness for new health threats.
http://healthfinder.gov/FindServices/Organizations/Organization.aspx?code=HR0039
http://www.cdc.gov

Centers for Medicare and Medicaid Services (CMS)

An agency within the US Department of Health & Human Services responsible for administration of several key federal health care programs. In addition to Medicare (the federal health insurance program for seniors) and Medicaid (the federal needs-based program), CMS oversees the Children's Health Insurance Program (CHIP) provisions in the Health Insurance Portability and Accountability Act (HIPAA) and its implementing regulations that pertain to national standards for electronic health care transactions and national identifiers for providers, health plans and employers, and the Clinical Laboratory Improvement Amendments (CLIA), among other services.
http://searchhealthit.techtarget.com/definition/Centers-for-Medicare-Medicaid-Services-CMS
http://www.cms.gov

Certification Commission for Health Information Technology (CCHIT)

The Certification Commission for Health Information Technology (CCHIT) was a private, nonprofit initiative to accelerate the adoption of health information technology by creating an efficient, credible and sustainable certification program for electronic health records and their networks. It ceased operations in November 2014.
http://www.phdsc.org/standards/certification-commission.asp

Certified EHR Technology (CEHRT)

Certified EHR technology gives assurance to purchasers and other users that an EHR system or module offers the necessary technological capability, functionality and security to help them meet the meaningful use criteria.
http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Certification.html

Clinical Decision Support (CDS)

Clinical decision support (CDS) provides clinicians, staff, patients or other individuals with knowledge and person-specific information, intelligently filtered or presented at appropriate times, to enhance health and health care. CDS encompasses a variety of tools to enhance decision-making in the clinical workflow. These tools include computerized alerts and reminders to care providers and patients; clinical guidelines; condition-specific order sets; focused patient data reports and summaries; documentation templates; and diagnostic support and contextually relevant reference information, among other tools.
http://www.healthit.gov/policy-researchers-implementers/clinical-decision-support-cds

Clinical Quality Measurement (CQM)

Clinical quality measures, or CQMs, are tools that help measure and track the quality of health care services provided by eligible professionals, eligible hospitals and critical access hospitals (CAHs) within our health care system. These measures use data associated with providers' ability to deliver high-quality care or relate to long term goals for quality health care.
http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/ClinicalQualityMeasures.html

Common Data Element (CDE)

Clinical concepts that contain standardized and structured metadata, have unambiguous intent and a clearly delineated value domain. These CDEs, such as "systolic blood pressure," would define a curated, universal specification for each clinical or administrative concept, optimizing the data to be reused across the QI ecosystem.
http://www.healthit.gov/sites/default/files/HITEnabledQualityImprovement-111214.pdf

Comprehensive Medication Management (CMM)

The standard of care that ensures that a patient's medications are appropriate, effective, safe and taken as intended.
http://cpnp.org/resource/mhc/2013/10/comprehensive-medication-management-patients-mental-illnesses

Computable Privacy

The ability of an electronic health information system to capture, adjudicate, comply with and persist in downstream processing of health information an individual's documented choice about whether information about them should be available for electronic exchange within a learning health system. Basic Choice and Granular Choice are subcomponents of computable privacy.

Computerized Physician Order Entry (CPOE)

Computerized Physician Order Entry (or CPOE) is the process of capturing a physician's instructions for a patient's care electronically to improve the efficiency of care delivery.
http://www.healthcareitnews.com/directory/computerized-physician-order-entry-cpoe

Consent

Agreement to an action based on knowledge of what the action involves and its likely consequences.
http://medical-dictionary.thefreedictionary.com/consent

Consolidated-Clinical Data Architecture (C-CDA)

The HL7 "consolidated" clinical document architecture (C-CDA) standard contains a library of CDA template standards and represents a single, unified implementation guide for multiple electronic clinical documents.
http://www.practicefusion.com/blog/understanding-c-cda-standard-ehr-certification-meaningful-use/

Consumer Data Privacy in a Network World

A framework for protecting privacy and promoting innovation in the global digital economy.
http://repository.cmu.edu/jpc/vol4/iss2/5/

Current Procedural Terminology (CPT)

The Current Procedural Terminology (CPT) code set is a medical code set maintained by the American Medical Association through the CPT Editorial Panel. The CPT coding system offers doctors across the country a uniform process for coding medical services that streamlines reporting and increases accuracy and efficiency.
http://www.ama-assn.org/ama/pub/physician-resources/solutions-managing-your-practice/coding-billing-insurance/cpt/cpt-process-faq/code-becomes-cpt.page

CVX

CVX codes are provided for each available vaccine used in the United States. When an MVX (manufacturer) code is paired with a CVX (vaccine administered) code, the specific trade named vaccine may be indicated.
http://www2a.cdc.gov/vaccines/iis/iisstandards/vaccines.asp?rpt=cvx

Data Access Framework (DAF)

A Standards & Interoperability (S&I) Framework initiative to define the standards and framework necessary for clinicians, providers and health care professionals to gain access to patient data within their own organization and from external organizations that may contain patient data.
http://wiki.siframework.org/Data+Access+Framework+Homepage

Data Provenance

Data provenance refers to the process of tracing and recording the origins of data and its movement between databases and is central to the validation of data. There is a Standards and Interoperability (S&I) Framework initiative working to define standards that support data provenance.
http://db.cis.upenn.edu/DL/fsttcs.pdf
http://wiki.siframework.org/Data+Provenance+Initiative

Data Segmentation for Privacy (DS4P)

The term "data segmentation" refers to the process of sequestering certain data elements from capture, access or view that are perceived by a legal entity, institution, organization, or individual as being undesirable to share. This basic definition, however, does not account for the multiple permutations of segmentation in the health care context (i.e., granularity), nor does it adequately capture the varied considerations required for development of segmentation policy. There is a Standards and Interoperability (S&I) Framework initiative working to define standards that support DS4P.
http://wiki.siframework.org/Data+Segmentation+for+Privacy+Charter+and+Members

Data Use and Reciprocal Support Agreement (DURSA)

The Data Use and Reciprocal Support Agreement (DURSA) is a comprehensive, multi-party trust agreement that was signed by all Nationwide Health Information Network participants, both public and private, wishing to participate in the NwHIN Exchange, now referred to as the eHealth Exchange. The DURSA provides the legal framework governing participation in the eHealth Exchange by requiring the signatories to abide by a common set of terms and conditions.
http://www.healthit.gov/sites/default/files/draft_nhin_trial_implementations_production_dursa-3.pdf
http://www.healthewayinc.org/images/Content/Documents/Application-Package/restatement_i_of_the_dursa_9.30.14_final.pdf

Deterministic Matching Algorithm

Deterministic Matching uses sets of predetermined rules to guide the matching process. The rules rely on a series of exact matches between data elements to identify when records match. It is most successful when the data is of relatively high quality or is dominated by reliable unique identifiers for records. Deterministic matching is less successful when the data is incomplete or inaccurate, when there are many spelling or transcription errors, or lots of inconsistencies (e.g., frequent name changes).
https://www.hln.com/assets/pdf/mpi_generic_final.pdf

Digital Imaging and Communications in Medicine (DICOM)

DICOM is an application layer network protocol for the transmission of medical images, waveforms and accompanying information.
http://whatis.techtarget.com/definition/DICOM-Digital-Imaging-and-Communications-in-Medicine

Direct Protocol

Direct uses established standards and protocols to enable secure health information exchange through a simple, scalable approach. Direct allows authorized users to send authenticated, encrypted health information directly to known recipients via the Internet. Direct offers a means of transmitting health information in support of core Stage 2 meaningful use measures including the communication of summary care records, referrals, discharge summaries and other clinical documents.

http://www.healthit.gov/policy-researchers-implementers/direct-project
http://wiki.directproject.org/

Directed Exchange (push)

Organizations need to send information to one another, often in an unsolicited manner (i.e., without the recipient specifically asking for the information). The Direct protocol was developed by the S&I Framework and utilizes email standards, but in a secure manner, with the primary protocol utilizing secure mail transport (SMTP). Direct supports a secure e-mail transaction that is appropriate for many different uses, including provider-to-provider, provider-to-consumer, provider-to-payer and many other types of transactions. The Direct protocol is an all-purpose protocol; it does not care what type of information is transported. To be used effectively, however, a trust relationship must exist between participants to ensure that a message reaches the intended party and not someone else. Other technologies have also been in use for some time to support unsolicited transmission of information including, secure File Transfer Protocol (sFTP) and Simple Object Access protocol [SOAP] and Representational State Transfer (REST).

http://www.healthit.gov/policy-researchers-implementers/direct-project
http://wiki.directproject.org/

DirectTrust

DirectTrust is an independent, non-profit trade association created by and for participants in the Direct community. It has established a set of technical, legal and business standards, expressed as policy and best practice recommendations, which members of the trust community agree to follow, uphold and enforce. DirectTrust offers an accreditation program that assesses organizations' adherence to these standards.

http://www.directtrust.org/

eHealth Exchange

The eHealth Exchange, formerly known as the NwHIN Exchange, is a group of federal agencies and non-federal organizations that came together under a common mission and purpose to improve patient care, streamline disability benefit claims and improve public health reporting through secure, trusted and interoperable health information exchange.

http://sequoiaproject.org/ehealth-exchange/

EHRIHIE Interoperability Workgroup (IWG)

The EHRIHIE Interoperability Workgroup (IWG) is a New York eHealth Collaborative-led coalition of 19 States (representing 52% of the U.S. population), 20 electronic health record (EHR) developers and 22 health information exchange (HIE) developers. The workgroup was launched in February 2011 to leverage existing standards and develop consistent implementation guides to support interoperability between HIE software platforms and the applications that interface with them.
http://www.nyehealth.org/office-of-the-national-coordinator-for-health-it-awards-the-ehrhie-interoperability-workgroup-exemplar-hie-governance-program-cooperative-agreement/

Electronic Health Record (EHR)

An electronic health record (EHR) is a digital version of a patient's paper chart. EHRs are real-time, patient-centered records that make information available instantly and securely to authorized users. While an EHR does contain the medical and treatment histories of patients, an EHR system is built to go beyond standard clinical data collected in a provider's office and can be inclusive of a broader view of a patient's care.
http://www.healthit.gov/providers-professionals/faqs/what-electronic-health-record-ehr

Electronic Healthcare Network Accreditation Commission (EHNAC)

Founded in 1993, the Electronic Healthcare Network Accreditation Commission (EHNAC) is an independent, federally recognized standards development organization and tax-exempt, 501(c)(6) non-profit accrediting body designed to improve transactional quality, operational efficiency and data security in health care.
https://www.ehnac.org/about/

Encryption/decryption

Encryption is the process of encoding messages or information in such a way that only authorized parties can read it.
http://en.wikipedia.org/wiki/Encryption

eXtensible Markup Language (XML)

Extensible Markup Language (XML) is a simple, very flexible text format derived from SGML (ISO 8879). Originally designed to meet the challenges of large-scale electronic publishing, XML is also playing an increasingly important role in the exchange of a wide variety of data on the Web and elsewhere.
http://www.w3.org/XML/

Fair Information Practices Principles (FIPPs)

FIPPs are the widely accepted framework of defining principles to be used in the evaluation and consideration of systems, processes, or programs that affect individual privacy.
http://www.nist.gov/nstic/NSTIC-FIPPs.pdf

Fast Healthcare Interoperability Resources (FHIR)

Fast Healthcare Interoperability Resources (FHIR, pronounced "Fire") defines a set of "Resources" that represent granular clinical concepts. The resources can be managed in isolation, or aggregated into complex documents. Technically, FHIR is designed for the web; the resources are based on simple XML or JSON structures, with an http-based RESTful protocol where each resource has predictable URL. Where possible, open internet standards are used for data representation.
http://wiki.hl7.org/index.php?title=FHIR

Federal Health Architecture (FHA)

The Federal Health Architecture (FHA) is an e-government initiative managed by the Office of the National Coordinator for Health IT (ONC) within the Department of Health and Human Services (HHS). FHA was formed to coordinate health IT activities among the more than 20 federal agencies that provide health and health care services to citizens.
http://www.healthit.gov/sites/default/files/pdf/fact-sheets/federal-health-architecture.pdf

Granular Choice

The choice an individual makes regarding the distinctions between legally sensitive clinical conditions, such as mental health or HIV/AIDS status and evolves over time to enable choice about disclosure to specifically identified participants in the health care system. *Note: for this interoperability roadmap, the term is used as defined in this glossary.*

Health Information Exchange (HIE)

Electronic health information exchange (HIE) allows doctors, nurses, pharmacists, other health care providers and patients to appropriately access and securely share a patient's vital medical information electronically—improving the speed, quality, safety and cost of patient care.
http://www.healthit.gov/providers-professionals/health-information-exchange/what-hie

Health Information Organization (HIO)

A Health information organization (HIO) is a multi-stakeholder organization created to facilitate health information exchange among stakeholders of that region's health care system.
http://en.wikipedia.org/wiki/Regional_Health_Information_Organization

Health Information Service Provider (HISP)

The term Health Information Service Provider (HISP) has been used by the Direct project both to describe a function (the management of security and transport for directed exchange) and an organizational model (an organization that performs HISP functions on behalf of the sending or receiving organization or individual). In this best practice document, we are mainly concerned with the HISP organization and the implications for privacy, security and transparency when the HISP is a separate business entity from the sending or receiving organization.
http://wiki.directproject.org/Best+Practices+for+HISPs

Health Information Technology for Economic and Clinical Health (HITECH) Act

The Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 provides HHS with the authority to establish programs to improve health care quality, safety and efficiency through the promotion of health IT, including electronic health records and private and secure electronic health information exchange. Learn more about select portions of the HITECH Act that relate to ONC's work.

http://www.healthit.gov/policy-researchers-implementers/health-it-legislation

Health Information Technology Policy Committee (HITPC)

The American Recovery and Reinvestment Act (ARRA) requires the Comptroller General of the United States to appoint thirteen of twenty members to the HIT Policy Committee, a body that makes recommendations on creating a policy framework for the development and adoption of a nationwide health information technology infrastructure, including standards for the exchange of patient medical information.

http://www.gao.gov/about/hcac/hitpc.html

http://www.healthit.gov/FACAS/health-it-policy-committee

Health Information Technology Standards Committee (HITSC)

The Health Information Technology (HIT) Standards Committee is a federal advisory committee (FACA) charged with making recommendations to the Office of the National Coordinator for Health Information Technology (ONC) on standards, implementation specifications and certification criteria for the electronic exchange and use of health information.

http://www.phdsc.org/standards/health-information/HITSC.asp

Health Insurance Portability and Accountability Act (HIPAA)

HIPAA is the acronym of the Health Insurance Portability and Accountability Act of 1996. The Office for Civil Rights (OCR) enforces the HIPAA Privacy Rule, which protects the privacy of individually identifiable health information; the HIPAA Security Rule, which sets national standards for the security of electronic protected health information; the HIPAA Breach Notification Rule, which requires covered entities and business associates to provide notification following a breach of unsecured protected health information; and the confidentiality provisions of the Patient Safety Rule, which protect identifiable information being used to analyze patient safety events and improve patient safety.

http://www.hhs.gov/ocr/privacy/

Health IT Certification Program

The Office of the National Coordinator for Health Information Technology (ONC) Certification Program helps to ensure that Electronic Health Record (EHR) technologies meet the standards and certification criteria adopted by the Secretary of Health and Human Services to allow providers and hospitals to achieve meaningful use and participate in the CMS EHR Incentive Programs.

http://www.healthit.gov/policy-researchers-implementers/about-onc-hit-certification-program

Health Level Seven (HL7)

Founded in 1987, Health Level Seven International (HL7) is a not-for-profit, ANSI-accredited standards developing organization. HL7 develops and maintains a framework and related standards for the exchange, integration, sharing and retrieval of electronic health information, defining how information is packaged and communicated from one party to another and setting the language, structure and data types required for seamless integration between systems.
http://www.hl7.org/about/index.cfm?ref=nav

Health Quality Domain Analysis Model (QI DAM)

This document seeks to define the common concepts and semantics involved in modeling reasoning within the various aspects of the health quality domain, with the goal of providing a common conceptual foundation that other specifications can use whenever the need to express and communicate expression logic arises.
http://www.hl7.org/implement/standards/product_brief.cfm?product_id=359

Healthcare Provider Directory (HPD)

The IHE Healthcare Provider Directory (HPD) profile supports management of health care provider information including public information on people and organizations across enterprises in a directory structure. HPD directory structure is a listing of health care providers that are classified by provider type, specialties, credentials, demographics and service locations.
http://wiki.ihe.net/index.php?title=Healthcare_Provider_Directory

ICD-9-CM/ICD-10-CM/PCS

ICD-9-CM and ICD-10-CM/PCS are forms of medical coding. ICD-10-CM/PCS will enhance accurate payment for services rendered and facilitate evaluation of medical processes and outcomes. The new classification system provides significant improvements through greater detailed information and the ability to expand in order to capture additional advancements in clinical medicine. The International Classification of Diseases (ICD) is maintained by the World Health Organization and is the most widely used disease classification system in the world. In the U.S., the National Center for Health Statistics (NCHS) adapted ICD-9 CM for diagnosis and procedure codes. NCHS and CMS are responsible for maintaining and distributing ICD-9 CM. The U.S. is moving towards ICD-10 CM, with a required implementation date of October 1, 2015.
https://www.uth.edu/dotAsset/2409977.pdf

Information Sharing and Analysis Organizations

Any formal or informal entity or collaboration created or employed by public or private sector organizations, for purposes of (A) gathering and analyzing critical infrastructure information; (B) communicating or disclosing critical infrastructure information; and (C) voluntarily disseminating critical infrastructure information.
https://www.fas.org/sgp/crs/RL31762.pdf

Innovation Community

The innovation community is comprised of entrepreneurs, startups and developers that build new Health IT technology and bring it to market; the early adopters who implement and test emerging technology; and the venture capital firms and incubators/accelerators that invest in Health IT and nurture early stage companies to success and the scientists who are evaluating new Health IT solutions and using Health IT to conduct clinical research. *Note: for this interoperability roadmap, the term is used as defined in this glossary.*

The Institute of Electrical and Electronic Engineers (IEEE)

The Institute of Electrical and Electronic Engineers (IEEE) is a global association and organization of professionals working toward the development, implementation and maintenance of technology-centered products and services. IEEE is a nonprofit organization founded in 1963. It works solely toward innovating, educating and standardizing the electrical and electronic development industry. It is best known for its development of standards such as IEEE 802.11. http://www.ieee.org/education_careers/education/standards/standards_glossary.html

Integrating the Healthcare Enterprise (IHE)

IHE is an initiative by health care professionals and industry to improve the way computer systems in health care share information. IHE promotes the coordinated use of established standards such as DICOM and HL7 to address specific clinical needs through the development of architectures and profiles to meet specific use case needs. http://www.ihe.net/

International Health Terminology Standards Development Organisation (IHTSDO)

Determines global standards for health terminology, most notably for SNOMED CT.

International Telecommunications Union Telecommunication Standardization Sector (ITU-T)

Develops international standards and recommendations defining elements in the global infrastructure of information and communication technologies; most notably within health the standard for X.509 digital certificates.

Internet Engineering Task Force (IETF)

Producing technical documents and standards to guide design, use and management of nearly all interactions on the Internet, including the most basic Internet protocols.

Interoperability

In the context of this Roadmap, interoperability is defined as the ability of a system to exchange electronic health information with and use electronic health information from other systems without special effort on the part of the user. Interoperability is made possible by the implementation of standards. http://www.ieee.org/education_careers/education/standards/standards_glossary.html

JASON

JASON is an independent group of scientists that advises the Federal government on matters of science and technology.
http://www.healthit.gov/buzz-blog/from-the-onc-desk/robust-health-data-infrastructure/
http://healthit.gov/sites/default/files/2014-JASON-data-for-individual-health.pdf

Learning Health System (LHS)

The concept of a continuously Learning Health System (LHS), first expressed by the Institute of Medicine in 2007, is now being rapidly adopted across the country and around the world. The LHS is based on cycles that include data and analytics to generate knowledge, leading feedback of that knowledge to stakeholders, with the goal to change behavior to improve health and to transform organizational practice.
http://healthinformatics.umich.edu/research/charles-friedman-identifying-lhs-research-challenges#overlay-context=research/learning-health-system

Level of Assurance (LOA)

Authentication focuses on verifying a person's identity based on the reliability of a credential offered. LOA refers to how much confidence a relying party has that the credential presented is in the possession of the person whose identity is being asserted. The Office of Management and Budget (OMB 04-04) describes four levels of identity authentication assurance levels, with Level 1 being the lowest level of assurance and Level 4 being the highest level of assurance.
https://www.cio.wisc.edu/security-initiatives-levels.aspx

Lightweight Directory Access Protocol (LDAP)

LDAP (Lightweight Directory Access Protocol) is a software protocol for enabling anyone to locate organizations, individuals and other resources such as files and devices in a network, whether on the public Internet or on a corporate intranet.
http://searchmobilecomputing.techtarget.com/definition/LDAP

Logical Observation Identifiers Names and Codes (LOINC)

LOINC, the Logical Observation Identifiers Names and Codes, is a universal code system for tests, measurements and observations. LOINC started in 1994 by the Regenstrief Institute. LOINC is the standardization of laboratory and other clinical observation values, so that systems can communicate electronically without having to map data elements. Historically, each laboratory, health system and technology developer has recorded laboratory values (such as an HA1C result) with their own proprietary vocabulary or internal code values. Consequently, laboratories and systems could send and receive laboratory results electronically, but only with a significant amount of work to map the values and with no guarantee that the values were interpreted and mapped correctly. LOINC solves this problem by providing universal codes and names that provide the global lingua franca for identifying tests and observations. NLM has provided partial support for the ongoing production and free dissemination of LOINC since 1999.
http://loinc.org/

Long-Term Post-Acute Care (LTPAC)

LTPAC Settings (e.g., Skilled Nursing Facility (SNF), Home Health, Inpatient Rehab, Long Term Acute Care Hospital, Hospice). This category of providers serves some of the nation's most vulnerable individuals and uses a significant portion of the Medicare and Medicaid budgets. Patients served by these providers experience frequent transitions in care and episodes of care coordination with eligible hospitals and professionals. Some of these providers may need interoperable EHR technology to support new care delivery and payment models in the Affordable Care Act and in private sector initiatives.

http://aspe.hhs.gov/daltcp/reports/2013/EHRPlap.shtml#appendE

http://aspe.hhs.gov/daltcp/reports/2013/ehrpi.shtml#ineligible

Long-Term Services & Supports (LTSS)

Assistance with activities of daily living and instrumental activities of daily living provided to older people and adults with disabilities that cannot perform these activities on their own due to a physical, cognitive, or chronic health conditions. LTSS may provide care, case management and service coordination to people who live in their own home, a residential setting, a nursing facility, or other institutional setting. LTSS also include supports provided to family members and other unpaid caregivers. LTSS may be provided in institutional and community settings.

http://www.acl.gov/Programs/CIP/OCASD/docs/2402-a-Guidance.pdf

Longitudinal Health Information

Longitudinal health information is health information that spans a period of time and may come from multiple sources. The availability of longitudinal health information is critical for delivery system reform and a learning health system, particularly to advance the health of individuals with chronic health conditions who require support from multiple care providers and/or services.

Meaningful Use

Meaningful Use describes the use of certified EHR technology (CEHRT) to improve quality, safety, efficiency and reduce health disparities; engage patients and family; improve care coordination and population and public health.

http://www.healthit.gov/providers-professionals/meaningful-use-definition-objectives

Medicaid Delivery System Reform Incentive Payment (DSRIP)

"Delivery System Reform Incentive Payment" or DSRIP programs are another piece of the dynamic and evolving Medicaid delivery system reform landscape. DSRIP initiatives are part of broader Section 1115 Waiver programs and provide states with significant funding that can be used to support hospitals and other providers in changing how they provide care to Medicaid beneficiaries.

http://kff.org/medicaid/issue-brief/an-overview-of-delivery-system-reform-incentive-payment-waivers/

Medicare and Medicaid EHR Incentive Programs

The Medicare and Medicaid Electronic Health Care Record (EHR) Incentive Programs provide incentive payments to eligible professionals, eligible hospitals and critical access hospitals (CAHs) as they adopt, implement, upgrade or demonstrate meaningful use of certified EHR technology.
http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/index.html?redirect=/ehrincentiveprograms/

Medication Therapy Management (MTM)

Medication therapy management is a service or group of services that optimize therapeutic outcomes for individual patients. Medication therapy management services include medication therapy reviews, pharmacotherapy consults, anticoagulation management, immunizations, health and wellness programs and many other clinical services. Pharmacists provide medication therapy management to help patients get the best benefits from their medications by actively managing drug therapy and by identifying, preventing and resolving medication-related problems.
http://www.pharmacist.com/mtm

National Center for Health Statistics (NCHS)

The National Vital Statistics System is the oldest and most successful example of inter-governmental data sharing in public health and the shared relationships, standards and procedures form the mechanism by which NCHS collects and disseminates the nation's official vital statistics.
http://www.cdc.gov/nchs/nvss.htm

National Council for Prescription Drug Plans (NCPDP)

The National Council for Prescription Drug Programs (NCPDP) is an American National Standards Institute (ANSI)-accredited Standards Development Organization. The purpose of The NCPDP Guide is to provide parameters for utilizing an ANSI approved health care ID card standard that clearly and consistently defines the information and format required by the pharmacy provider.
http://www.ncpdp.org/NCPDP/media/pdf/NCPDPpharmacyIdCardFactSheet.pdf

National Council for Prescription Drug Programs (NCPDP) SCRIPT

The National Council for Prescription Drug Programs SCRIPT Standard is used to transmit electronic prescriptions from a physician or prescriber to the pharmacy; specific messages include New, Change, Renewal, Cancellation and Fill Status.
http://healthit.ahrq.gov/key-topics/ncpdp

National Drug Code (NDC)

The NDC, or National Drug Code, is a unique 10-digit, 3-segment number. It is a universal product identifier for human

drugs in the United States. The code is present on all non-prescription (OTC) and prescription medication packages and inserts in the US.
http://www.drugs.com/ndc.html

National eHealth Collaborative (NeHC)

National eHealth Collaborative is a public-private partnership that aims to enable secure and interoperable nationwide health information exchange through education and stakeholder engagement. In December 2013 NeHC was absorbed by the HIMSS Foundation.
http://www.Healthcareitnews.com/directory/national-ehealth-collaborative-nehc

National Information Exchange Model (NIEM)

NIEM—the National Information Exchange Model—is a community-driven, standards-based approach to exchanging information. NIEM brings together diverse communities that collectively leverage tools, processes and technologies to increase efficiencies and improve decision-making.
https://www.niem.gov/aboutniem/Pages/niem.aspx

National Institute of Standards and Technology (NIST)

Founded in 1901, NIST is a non-regulatory federal agency within the U.S. Department of Commerce. NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards and technology in ways that enhance economic security and improve our quality of life.
http://www.nist.gov/public_affairs/general_information.cfm

National Library of Medicine (NLM)

The National Library of Medicine (NLM), on the campus of the National Institutes of Health in Bethesda, Maryland, has been a center of information innovation since its founding in 1836. The world's largest biomedical library, NLM maintains and makes available a vast print collection and produces electronic information resources on a wide range of topics that are searched billions of times each year by millions of people around the globe. NLM also serves as the central coordinating body for clinical terminology standards within the Department of Health and Human Services and manages and makes available a number of health terminology standards, including RxNorm, LOINC, and SNOMED.
http://www.nlm.nih.gov/

National Plan & Provider Enumeration System (NPPES)

The Centers for Medicare & Medicaid Services (CMS) has developed the National Plan and Provider Enumeration System (NPPES) to assign unique identifiers to health care providers. The National Provider Identifier (NPI) has been the standard identifier for health care providers since May 2007.
http://www.nber.org/data/npi.html

National Provider Identifier (NPI)

The National Provider Identifier (NPI) is a Health Insurance Portability and Accountability Act (HIPAA) Administrative Simplification Standard. The NPI is a unique identification number for covered health care providers. Covered health care providers and all health plans and health care clearinghouses must use the NPIs in the administrative and financial transactions adopted under HIPAA. The NPI is a 10-position, intelligence-free numeric identifier (10-digit number).
https://www.cms.gov/Regulations-and-Guidance/HIPAA-Administrative-Simplification/NationalProvIdentStand/index.html?redirect=/NationalProvIdentStand/

National Strategy for Trusted Identities in Cyberspace (NSTIC)

The National Strategy for Trusted Identities in Cyberspace (NSTIC, or Strategy) is a White House initiative to work collaboratively with the private sector, advocacy groups, public sector agencies and other organizations to improve the privacy, security and convenience of online transactions.
http://www.nist.gov/nstic/about-nstic.html

National Study of Long-Term Care Providers (NSLTCP)

The biennial National Study of Long-Term Care Providers (NSLTCP), sponsored by the U.S. Centers for Disease Control and Prevention's National Center for Health Statistics (NCHS), is a groundbreaking initiative to monitor trends in the major sectors of paid, regulated long-term care services providers.
http://www.cdc.gov/nchs/data/nsltcp/NSLTCP_FS.pdf

Nationwide Health Information Network (NwHIN)

The Nationwide Health Information Network is a set of standards, services and policies that enable the secure exchange of health information over the Internet.
http://www.healthit.gov/policy-researchers-implementers/nationwide-health-information-network-nwhin

Network Access Protection (NAP)

Network Access Protection (NAP) is a client health policy creation, enforcement and remediation technology that is included in Windows Vista® and Windows Server® 2008. With NAP, you can establish health policies that define such things as software requirements, security update requirements and required configuration settings for computers that connect to your network.
http://technet.microsoft.com/en-us/library/cc754378%28v=ws.10%29.aspx

OAUTH2

OAuth 2 is an authorization framework that enables applications to obtain limited access to user accounts on an HTTP service. It works by delegating user authentication to the service that hosts the user account and authorizing third-party

applications to access the user account. OAuth 2 provides authorization flows for web and desktop applications and mobile devices.
https://www.digitalocean.com/community/tutorials/an-introduction-to-oauth-2

Office for Civil Rights (OCR)

The Office for Civil Rights enforces the HIPAA Privacy Rule, which protects the privacy of individually identifiable health information; the HIPAA Security Rule, which sets national standards for the security of electronic protected health information; the HIPAA Breach Notification Rule, which requires covered entities and business associates to provide notification following a breach of unsecured protected health information; and the confidentiality provisions of the Patient Safety Rule, which protect identifiable information being used to analyze patient safety events and improve patient safety.
http://www.hhs.gov/ocr/office/about/index.html

Office of Consumer eHealth (OCeH)

OCEH works to empower patients and caregivers to be partners in their health care through the adoption and use of health IT.
http://www.ilhitrec.org/ilhitrec/pdf/ONCSummaryCongress_July2013.pdf

Office of the Assistant Secretary for Preparedness and Response (ASPR)

The Office of the Assistant Secretary for Preparedness and Response was created under the Pandemic and All Hazards Preparedness Act in the wake of Katrina to lead the nation in preventing, preparing for and responding to the adverse health effects of public health emergencies and disasters. ASPR focuses on preparedness planning and response, building federal emergency medical operational capabilities, countermeasures research, advance development and procurement, and providing grants to strengthen the capabilities of hospitals and health care systems in public health emergencies and medical disasters.
http://www.phe.gov/about/aspr/pages/default.aspx

Office of the National Coordinator for Health Information Technology (ONC)

The Office of the National Coordinator for Health Information Technology (ONC) is at the forefront of the administration's health IT efforts and is a resource to the entire health system to support the adoption of health information technology and the promotion of nationwide health information exchange to improve health care. ONC is organizationally located within the Office of the Secretary for the U.S. Department of Health and Human Services (HHS).
http://www.healthit.gov/newsroom/about-onc

OpenID Connect

OpenID, which was first created in 2005, allows web sites and authentication services to exchange security information in a standardized way. The goal of OpenID Connect is to allow an end user to log in once and access multiple,

disparate resources on and off the Web. The specification, which has the backing of numerous cloud providers, including Google and Microsoft, is expected to pave the way for companies to replace their on-premise identity and access management (IAM) systems with cloud offerings.
http://whatis.techtarget.com/definition/OpenID

Organization for the Advancement of Structured Information Standards (OASIS)

OASIS is a non-profit consortium that drives the development, convergence and adoption of open standards for the global information society, including many XML-based specifications and the specification for SOAP web services. OASIS promotes industry consensus and produces worldwide standards for security, Internet of Things, cloud computing, energy, content technologies, emergency management and other areas. OASIS open standards offer the potential to lower cost, stimulate innovation, grow global markets and protect the right of free choice of technology.
https://www.oasis-open.org/org

Persist or Persistence

The idea that a particular data element stays with the data as it flows downstream and is reprocessed and reused the permissions that may limit access to, use of, or disclosure of an individual's data must persist in the data to ensure proper privacy compliance. *Note: for this interoperability roadmap, the term is used as defined in this glossary.*

Personal Health Record (PHR)

A personal health record (PHR) is an electronic application used by patients to maintain and manage their health information in a private, secure and confidential environment.
http://www.healthit.gov/providers-professionals/faqs/what-personal-health-record

Person-Centered

ONC's vision for a person-centered learning health system: the power of each individual is developed and unleashed to be active in managing their health and partnering in their health care, enabled by information and technology. Health care is a partnership between the patient, their caregivers, the care team and supporting services.
http://www.healthit.gov/policy-researchers-implementers/person-center

Policy Decision Point (PDP)

The point where policy decisions are made. In the case of NAP, this is the NAP health policy server.
http://msdn.microsoft.com/en-us/library/ee380787.aspx

Policy Enforcement Point (PEP)

The point where the policy decisions are actually enforced.
http://msdn.microsoft.com/en-us/library/ee380787.aspx

Population Health

Population health is defined as the health outcomes of a group of individuals, including the distribution of such outcomes within the group.
http://www.improvingpopulationhealth.org/blog/what-is-population-health.html

Prescription Drug Monitoring Programs (PDMP)

Prescription drug monitoring programs (PDMPs) maintain statewide electronic databases of prescriptions dispensed for controlled substances (i.e., prescription drugs of abuse that are subject to stricter government regulation).
http://www.fas.org/sgp/crs/misc/R42593.pdf

President's Council of Advisors on Science and Technology (PCAST)

PCAST is an advisory group of the nation's leading scientists and engineers who directly advise the President and the Executive Office of the President. PCAST makes policy recommendations in the many areas where understanding of science, technology and innovation is key to strengthening our economy and forming policy that works for the American people.
http://www.whitehouse.gov/administration/eop/ostp/pcast/about

Probabilistic Matching Algorithm

Probabilistic Matching is a process whereby an estimate is made of the probability that two records are for the same person based on the degree to which certain fields in the two records match. Two thresholds are then set: all record pairs whose probability is above the higher threshold are considered to be matches; all record pairs whose probability is below the lower threshold are considered not to be matches. The disposition of record pairs whose probability falls in between the two thresholds is considered to be uncertain and they require additional review. An alternate method is Deterministic Matching Algorithm.
https://www.hln.com/assets/pdf/mpi_generic_final.pdf

Protected Health Information (PHI)

The HIPAA Privacy Rule defines PHI as individually identifiable health information, held or maintained by a covered entity or its business associates acting for the covered entity that is transmitted or maintained in any form or medium (including the individually identifiable health information of non-U.S. citizens).
http://privacyruleandresearch.nih.gov/pr_07.asp

Provider Enrollment, Chain and Ownership System (PECOS)

PECOS supports the Medicare Provider and Supplier enrollment process by allowing registered users to securely and electronically submit and manage Medicare enrollment information.
https://pecos.cms.hhs.gov/pecos/login.do

Public Health

Public health is the science of protecting and improving the health of families and communities through promotion of healthy lifestyles, research for disease and injury prevention and detection and control of infectious diseases. Overall, public health is concerned with protecting the health of entire populations. These populations can be as small as a local neighborhood, or as big as an entire country or region of the world.
http://www.cdcfoundation.org/content/what-public-health

Publish, Subscribe, Notification

Services allow participants to know if information is available for them to take action as they see fit, rather than having all of the information sent directly to them. Notification services can also support more automated processes that might rely on this information to feed other workflows or processes. Today, notification is handled in a variety of ways supported by a variety of technologies, including use of HL7 v2 Admit/Discharge/Transfer (ADT) messages passed between organizations and the Blue Button Toolkit, which includes the ability to subscribe to a resource and be notified as new information is available. *Note: for this interoperability roadmap, the term is used as defined in this glossary.*

Public Key Infrastructure (PKI)

A set of hardware, software, people, policies and procedures needed to create, manage, distribute, use, store and revoke digital certificates... (which are) electronic document(s) used to prove ownership of a public key. The certificate includes information about the key, information about its owner's identity and the digital signature of an entity that has verified the certificate's contents are correct. If the signature is valid and the person examining the certificate trusts the signer, then they know they can use that key to communicate with its owner.
http://en.wikipedia.org/wiki/Public_key_infrastructure
http://en.wikipedia.org/wiki/Public_key_certificate

Quality Reporting Data Architecture (QRDA)

QRDA is a document format that provides a standard structure with which to report quality measure data to organizations that will analyze and interpret the data.
http://www.hl7.org/implement/standards/product_brief.cfm?product_id=35

Query (pull)

Organizations and individuals will need to perform secure searches for health data from known or unknown sources. Information query (and its associated response by the other party) is a complex activity. Queries must be structured in a way that the recipient can – in an automated way – not only understand what is being requested, but identify whether the information is present and disclosure is authorized in response. Query/response transactions must be encrypted for security. They must be permitted under the laws and policies of all relevant jurisdictions (federal, state and local). A variety of technologies and standards are in use to support query, including IHE profiles, which have become the basis

for a variety of efforts (including the eHealth Exchange, EHRIHIE Work Group and the Care Connectivity Consortium). Web services are widely used with these and other standards to enable query/response transactions. *Note: for this interoperability roadmap, the term is used as defined in this glossary.*

Reference Information Model (RIM)

"The RIM is a large, pictorial representation of the HL7 clinical data (domains) and identifies the life cycle that a message or groups of related messages will carry. It is a shared model between all domains and, as such, is the model from which all domains create their messages."
http://www.hl7.org/implement/standards/rim.cfm

Representational State Transfer (RESTful)

RESTful (Representational State Transfer) is an architectural style and an approach to communications that is often used in the development of Web services. The use of REST is often preferred over SOAP (Simple Object Access Protocol). The primary popularity of REST is that it is simpler to configure and deploy than SOAP.
http://searchsoa.techtarget.com/definition/REST

RESTful API

A method of allowing communication between a Web-based client and server that employs representational state transfer (REST) constraints. A RESTful API is an application program interface (API) that uses HTTP requests to GET, PUT, POST and DELETE data. RESTful APIs break down a transaction to create a series of small modules, each of which addresses a particular underlying part of the transaction.
http://searchcloudstorage.techtarget.com/definition/RESTful-API

Rules of the Road

The set of basic rules that will provide the needed underpinning to support electronic health information exchange nationwide. *Note: for this interoperability roadmap, the term is used as defined in this glossary.*

RxNorm

RxNorm provides names and codes for clinical drugs and links those names and codes to the major commercial drug vocabularies commonly used in pharmacy management and drug interaction software. The goal of RxNorm is to allow computer systems to communicate drug-related information efficiently and unambiguously. RxNorm has been endorsed by ONC, CMS, National Council for Prescription Drug Programs (NCPDP, the major national Standards Development Organization for outpatient and long term care e-prescribing), among others. RxNorm data is updated weekly and monthly and is available for free without a license from National Library of Medicine, either as a download or through Application Programming Interfaces (APIs).
http://www.nlm.nih.gov/research/umls/rxnorm/overview.html

Secure File Transport Protocol (SFTP)

SFTP uses the Secure Shell protocol (SSH) to transfer files. Unlike FTP, it encrypts both commands and data, preventing passwords and sensitive information from being transmitted openly over the network.
http://en.wikipedia.org/wiki/File_Transfer_Protocol#Secure_FTP

Secure/Multipurpose Internet Mail Extensions (S/MIME)

S/MIME is a standard used to encode binary files for transfer via SMTP-based e-mail.
http://en.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol

Security Assertion Markup Language (SAML)

SAML, (pronounced sam-el) is an XML-based, open-standard data format for exchanging authentication and authorization data between parties, in particular, between an identity provider and a service provider. SAML is a product of the OASIS Security Services Technical Committee.
http://en.wikipedia.org/wiki/Security_Assertion_Markup_Language

Semantics

Terminology standards (or standardized nomenclature) define words permitting representatives of an industry or parties to a transaction to use a common, clearly understood language.
http://www.nist.gov/standardsgov/definestandards.cfm

Service/Service-oriented Architecture (SOA)

SOA is based on distinct pieces of software providing application functionality as services to other applications via a protocol. Depending on the service design approach taken, each SOA service is designed to perform one or more activities by implementing one or more service operations. As a result, each service is built as a discrete piece of code. This makes it possible to reuse the code in different ways throughout the application by changing only the way an individual service interoperates with other services that make up the application, versus making code changes to the service itself. SOA design principles are used during software development and integration.
http://en.wikipedia.org/wiki/Service-oriented_architecture

Simple Mail Transport Protocol (SMTP)

Simple Mail Transfer Protocol (SMTP) is an Internet standard for electronic mail (e-mail) transmission. SMTP defines message transport, not the message content.
http://en.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol

Simple Object Access Protocol (SOAP)-based Web Services/Web Services Description Language (WSDL)

SOAP is a protocol specification for exchanging structured information in the implementation of web services in computer networks. A Web service is a method of communication between two electronic devices over a network. The Web Services Description Language (WSDL pronounced wiz'-dul) is an XML-based interface definition language that is used for describing the functionality offered by a web service.

http://en.wikipedia.org/wiki/SOAP

http://en.wikipedia.org/wiki/Web_service

http://en.wikipedia.org/wiki/Web_Services_Description_Language

Standard

Common and repeated use of rules, conditions, guidelines or characteristics for products or related processes and production methods and related management systems practices. For types of standards see reference.

http://www.nist.gov/standardsgov/definestandards.cfm

Standards & Interoperability Framework (S&I Framework)

A collaborative community of participants from the public and private sectors who are focused on providing the tools, services and guidance to facilitate the functional exchange of health information.

http://www.siframework.org/whatis.html

Standards Development Organization (SDO)

SDOs are member-based organizations whose members set the priorities for which standards will be developed and refined. Each SDO has a very refined process for developing, balloting, piloting, finalizing and maintaining standards within its domain. *Note: for this interoperability roadmap, the term is used as defined in this glossary.*

State Innovation Models (SIM) Initiative

The State Innovation Models Initiative is providing support to states for the development and testing of state-based models for multi-payer payment and health care delivery system transformation with the aim of improving health system performance for residents of participating states.

http://innovation.cms.gov/initiatives/state-innovations

Statewide HIE Cooperative Agreement Program

HITECH Act program that funded states' efforts to rapidly build capacity for exchanging health information across the health care system both within and across states.

http://www.healthit.gov/policy-researchers-implementers/state-health-information-exchange

Structured Data Capture (SDC)

An initiative to develop and validate a standards-based data architecture so that a structured set of data can be accessed from EHRs and be stored for merger with comparable data for other relevant purposes like case reports and incident report.
http://wiki.siframework.org/Structured+Data+Capture+Initiative

Systematized Nomenclature of Medicine–Clinical Terms (SNOMED CT)

SNOMED CT is a comprehensive clinical terminology that was originally developed by the College of American Pathologists. In 2007, the International Health Terminology Standards Development Organisation (IHTSDO), an international SDO, took over SNOMED CT and currently owns, maintains and distributes the vocabulary. The National Library of Medicine (NLM) is the U.S. representative to IHTSDO and is therefore responsible for producing the US edition of SNOMED CT and distributing SNOMED CT in the U.S. It is one of a suite of designated standards for use in U.S. Federal Government systems for the electronic exchange of clinical health information. Meaningful use stage 2 requires that problems be captured and represented in SNOMED CT when exchanged in the C-CDA. NLM, CMS and other stakeholders are working to enhance the SNOMED CT terminology to include more codes to meet specific semantic needs.
http://www.nlm.nih.gov/research/umls/Snomed/snomed_main.html

Transition of Care (ToC)

The movement of a patient from one setting of care (hospital, ambulatory primary care practice, ambulatory specialty care practice, long-term care, home health, rehabilitation facility) to another.
http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/downloads/8_Transition_of_Care_Summary.pdf

Unified Code for Units of Measure (UCUM)

The Unified Code for Units of Measure is a code system intended to include all units of measures being contemporarily used in international science, engineering and business.
http://unitsofmeasure.org/trac/

Unique Ingredient Identifier (UNII)

The UNII is a non- proprietary, free, unique, unambiguous, non-semantic, alphanumeric identifier based on a substance's molecular structure and/or descriptive information.
http://www.fda.gov/ForIndustry/DataStandards/SubstanceRegistrationSystem-UniqueIngredientIdentifierUNII/

Universal Description Discovery and Integration (UDDI)

UDDI specifications form the necessary technical foundation for publication and discovery of Web services implementations both within and between enterprises.
https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=uddi-spec

Value Set Authority Center (VSAC)

The Value Set Authority Center (VSAC) is provided by the National Library of Medicine (NLM), in collaboration with the Office of the National Coordinator for Health Information Technology and the Centers for Medicare & Medicaid Services. The VSAC provides downloadable access to all official versions of vocabulary value sets contained in the 2014 Clinical Quality Measures (CQMs). Each value set consists of the numerical values (codes) and human-readable names (terms), drawn from standard vocabularies such as SNOMED CT®, RxNorm, LOINC and ICD-10-CM, which are used to define clinical concepts used in clinical quality measures (e.g., patients with diabetes, clinical visit). The content of the VSAC will gradually expand to incorporate value sets for other use cases, as well as for new measures and updates to existing measures.
https://vsac.nlm.nih.gov/

View Online, Download and Transmit (VDT)

One of the Stage 2 Meaningful Use Core Measures under the CMS EHR Incentive Programs is to, "provide patients the ability to view online, download and transmit their health information within four business days of the information being available to the eligible professional."
http://www.healthit.gov/providers-professionals/achieve-meaningful-use/core-measures-2/patient-ability-electronically-view-download-transmit-vdt-health-information

Virtual Private Networks (VPN)

A virtual private network (VPN) extends a private network across a public network, such as the Internet. It enables a computer or Wi-Fi-enabled device to send and receive data across shared or public networks as if it were directly connected to the private network, while benefiting from the functionality, security and management policies of the private network.
http://en.wikipedia.org/wiki/Virtual_private_network

World Health Organization (WHO)

The directing and coordinating authority for health within the United Nations system that also develops and maintains the International Classification of Diseases (ICD) terminology as the standard diagnostic tool for epidemiology, health management and clinical purposes.
http://www.who.int/classifications/icd/en/