eHealth Council

March 13, 2018
9:30 A.M. CT – 12:00 noon CT

1526 K Street, Lower Level, Training Room, Lincoln, NE
Desktop Videoconferencing Available by Request

Tentative Agenda

Meeting Materials

9:30	Roll Call Notice of Posting of Agenda Notice of Nebraska Open Meetings Act Posting *Approval of April 5, 2017 minutes** Approval of Oct. 12, 2017 minutes Public Comment
9:40	Updates - Nebraska Statewide Telehealth Network—Max Thacker - PDMP Update-Jenifer Roberts-Johnson and Kevin Borcher - NeHII Update—Deb Bass
10:00	- Trusted Exchange Framework and Common Agreement—Zoe Barber, Office of the National Coordinator for Health IT (confirmed) *Resource: Draft Trusted Exchange Framework—Jan. 5, 2018* *Resource: A User's Guide to Understanding the Draft Trusted Exchange Framework*
10:45	HIE and Data Governance Discussion-Deb Bass, NeHII; Kevin Conway, Nebraska Hospital Association; Dr. James McClay, UNMC
12:00	- Adjourn

* Indicates action items
Meeting notices were posted on the Public Meeting and NITC websites on Jan. 24, 2018. Meeting agenda posted on Jan. 24, 2018.

EHEALTH COUNCIL

April 5, 2017 1:30 P.M. CT – 3:30 P.M. CT
Administrative Services-Lower Level Training Room
1526 K Street, Lincoln, Nebraska
(Including Skype for Business Connections Upon Request)

Members Present:
Marsha Morien, Co-Chair
Kevin Borcher
Kevin Conway
Joel Dougherty
Marty Fattig
Cindy Kadavy
Rama Kolli (Video)
Jim McClay
Dave Palm
June Ryan
Brian Sterud (Video)
Robin Szwanek
Anna Turman (Video)
Heather Wood, Alt. for Linda Wittmuss
Bridget Young

Members Absent: Kathy Cook, Kimberly Galt, Dr. Shawn Murdock, Todd Searls, Max Thacker and Delane Wycoff

ROLL CALL NOTICE OF POSTING OF AGENDA NOTICE OF NEBRASKA OPEN MEETINGS ACT POSTING

Co-Chair, Marsha Morien, called the meeting to order at 1:31 p.m. Roll call was taken. There were 15 members present. A quorum was present to conduct official business. A copy of the Open Meetings Law was located on the back table. The meeting notices were posted on the Public Meeting and the NITC websites on March 28, 2017. The meeting agenda was posted on March 28, 2017.

APPROVAL OF OCTOBER 3, 2016 MINUTES*

Mr. Dougherty moved to approve the minutes as presented. Mr. Palm seconded. All were in favor. Motion carried.

PUBLIC COMMENT

There was no public comment.

Ms. Morien stressed the importance of the council to the NITC. The Council members are ambassadors of eHealth to the State of Nebraska. She also reminded members that they can designate alternates to serve in their absence at meetings.

Prescription Drug Monitoring Program (PDMP)UPDATE

Felicia Quintana-Zinn and Kevin Borcher

The Prescription Drug Monitoring Program (PDMP) went live as mandated on Jan.1, 2017, enabling dispensers to report all controlled substances dispensed as required. The Department of Health and Human Services received two grants which are supporting efforts to develop a PDMP and to prevent prescription drug overdoses.

The Harold Rogers- DOJ Bureau of Justice Assistance grant is supporting PMPD training and PDMP software enhancement. PDMP trainings are being conducted through live webinars, on-demand webinars (went live in March), in-person sessions and downloadable tutorials. Over 750 dispensers and prescribers have been trained since December. Training information is available on the PDMP website at www.dhhs.ne.gov/PDMP.

The Prescription Drug Overdose Prevention for States Grant (PDO-PfS) — CDC grant is supporting the following three strategies:

- **Develop and implement pain management guidelines.** The purpose of pain management guidelines is to promote consistent, safe, and effective pain management standards. The NDHHS Division of Public Health is collaborating with Division of Behavioral Health, Managed Long Term Care plans, Nebraska Medical Association, and physicians on the task force to develop the guidelines. The task force is using CDC and Oregon pain management guidelines as a resource. Task force members are identifying priority areas to include in the guidelines. The guidelines will be reviewed by content area experts and also presented to the professional boards. Once guidelines are approved, they will be disseminated with education provided.

- **Conduct needs assessment and educate on expanded access to naloxone.** Naloxone is an opioid antagonist that blocks or reversed the effects of opioid medication during an overdose event. The goal of the project is to decrease the rate of drug overdose deaths, including opioid and heroin deaths. A needs assessment was conducted with EMS, fire departments, law enforcement, physicians, pharmacists, and substance abuse treatment facilities. The results of the needs assessment will guide education on access and use of naloxone and the development of a media awareness campaign.

- **Enhance and maximize the NE PDMP system.** The PDMP team is working to increase access and use of the PDMP by medical professionals. As of 03/31/2017, 2,894 prescribers, 1,166 dispensers, and 36 designees had been registered to use the PDMP. As of 03/24/2017, 100% of total eligible Nebraska dispensers have registered to report to the PDMP or noted as an exempted pharmacy for the 2017 year. This includes community pharmacies, dispensing practitioners, and long-term care automated pharmacy dispensers. 79.7% of total eligible mail service pharmacies have registered to report to the PDMP or noted as an exempted pharmacy for the 2017 year. The grant is also supporting enhancements to utilize PDMP data for public health surveillance. The enhancements went live on Jan. 1, 2017. As of the end of February of this year, 497,382 dispensed records had been reported to the PDMP.

Ms. Quintana-Zinn and Mr. Borcher answered questions from members. Member questions included: How are consumers getting educated? Ms. Quintana-Zinn answered that the project has not officially started outreach for consumers yet, that is down the road. Information is available on the website. Amy Reynoldson is the contact for the educational portion of the grant. Members briefly discussed the status of LB 223. The bill is still in committee. Because it is Senator Howard's priority bill, it should make it to general file. Members also asked about how information on the PDMP is being incorporated into the medical curriculum. The team has received some calls to be guest speakers at Creighton and UNMC.

Ms. Byers commented that the project has been a team effort with support from the Legislature, DHHS, NeHII, DrFirst, work groups members, professional groups and other stakeholders.

ONC INTEROPERABLE HEALTH IT SERVICES TO SUPPORT HIE GRANT UPDATE
Anne Byers

Ms. Byers reviewed the "Lessons Learned" from the ONC grant.

- **Recruitment and Engagement of Long-Term Care and Post-Acute Care Facilities (LTPACs) and Critical Access Hospitals (CAHs).** It takes a lot of work to engage Critical Access Hospitals and long-term and post-acute care facilities.

- **Better Understanding the Needs of Long-Term and Post-Acute Care Facilities.** Work on the Integrated Community project has helped us better understand the needs of long-term and post-acute care facilities and the importance of including long-term care and post-acute care facilities and others providers in the health information exchange. Through the grant, the team has developed several use cases for exchanging health information with long-term and post-acute care facilities. Demonstrating the value of different use cases will facilitate efforts to engage long-term and post-acute care facilities.

- **Integration of Health Information Exchange into the Provider Workflow.** The process developed for the Integrated Communities Project is proving to be useful in engaging providers and helping them integrate health information exchange into their workflow. Having a facilitator to start the engagement process is a key component. It was also very helpful to have a project manager from NeHII as part of the team to provide technical assistance.

  Having all participating providers set up with both Direct and query-based exchange early in the process allows for the implementation of a greater number of use cases. Health information exchange isn't plug and play. It takes time and effort to integrate health information exchange into the provider workflow. For example, the NeHII Community Patient Profile (CPP) is easy to implement, but usage doesn't usually take off unless the CPP can be accessed with single sign on from the electronic health record. Direct has been touted as an easy first step for health information exchange, but in reality it takes time and effort to identify use cases and to work with other health care providers to begin exchanging information.

  Structured interviews were conducted with ADT subscribers to understand how ADT messaging was implemented and used and the impact and user satisfaction with the service.

Discussions from the meeting led to the recommendation to include the importance of a community champion as a lesson learned.

INTEGRATED COMMUNITY PROJECT AND TRAINING MODULES

Gary Cochran, PharmD, SM

With four months left in the grant, the team is in the final stages of the Integrated Community Project. The project identified two integrated communities which consisted of a hospital, clinic, long-term care facilities, and a pharmacy interested in exchanging health information. The team worked with the providers in each community to identify use cases and discuss current work processes/workarounds. NeHII matched available technology to the use cases. Facilities chose the use cases to be implemented. The team worked with the health care providers to integrate the use case into their regular workflow.

The team is also creating four training modules to provide background and direction for facilities considering the adoption of HIE and uses lessons learned from integrated communities. The four training modules focus on:

1. What is HIE and “why” do I care?
2. Is HIE right for me? Finding Value
3. HIE solutions
4. Integrating HIE into your facility

Ms. Bass commended Mr. Fattig for his efforts to contact and encourage facilities to participate in the project. It is beneficial to have champions promoting the benefits of electronic health records and integrated communities.

NEW NEHII PRICING STRUCTURE AND NEHII UPDATE
Deb Bass

With NeHII's migration to a new platform, the edge server pricing strategy based upon hospital bed size has ended. Participants were asking for a more tangible, customized method to determine participation fees. A workgroup was formed to develop pricing model and future value added services strategy. The pricing model was finalized in January 2017. Announcements letters were distributed in February and March 2017.

The new pricing module will create a more equitable manner to allocate costs based on a facility's potential use of the HIE. It is not intended as a method to increase revenue. Hospital license fees have remained unchanged since NeHII's go live in 2009. Large health systems paid a three year sustainability surcharge in 2013–2015. All other health systems paid a two year sustainability surcharge in 2014–2015. Five hospitals are paying slightly higher participation fees.

The new pricing module eliminates fees for licensed healthcare professionals to have access to the data. The cost of the exchange is shared evenly between payers and hospitals. The State of Nebraska is considered a payer. NeHII utilized the 2015 Medicare Cost Report and adjusted discharges as tangible numbers. A three-year phased implementation schedule will be used to allow for ease of transition:

- First year - 2017: 2/3s licensed bed model, 1/3 adjusted discharge
- Second year - 2018: 2/3s adjusted discharge, 1/3 licensed bed model
- Third year – 2019: full adjusted discharge

Licensed Healthcare Professionals pricing information:

- All will have free access to the data in the HIE
- If an ambulatory clinic becomes a data provider there will be a $500/month participation fee
- Eliminate site license model for hospitals
- Eliminate 1:3 ratio for allied professionals per provider
- Comparable to free access to the PDMP data
- Letter distributed February 20, 2017 (copy included in the meeting materials)

Hospitals and Health Systems pricing information:

- Based upon adjusted discharge rate
- $4.96 per discharge
- Three year phased implementation schedule
- Letters distributed March 7, 2017
- Calls made to all CEOs
- Limited number saw increases
- For CAH minimum fee of $500/month
- Use SHIP funding to offset HIE participation costs
- Reminder made of free access to all providers

Payers pricing information:

- $25,000 annual fee plus PMPM fee
- Sliding scale based upon number of covered lives
- Eight tiers in the scale
- Lowest tier:1 to 74,999 lives = 0.17 cents PMPM
- Highest tier: more than 450,000 lives = 0.10 cents PMPM
- Includes ADT event notification and other value add services

2016 Annual Report. The report was approved at the March board meeting. The full report is available at http://www.nehii.org/index.php?option=com_docman&view=list&slug=forms-documents&Itemid=54. A Town Hall Webinar will be hosted on May 4, 2017.

2017 Annual Meeting. Planning is in progress for the annual meeting to be held late July or early August. Kearney, Nebraska conference facilities are being considered for the location. Sponsorships are available. Suggestions for keynote speakers would be appreciated. It was suggested to have a panel of participants from the integrated communities, including Mr. Fattig.

OTHER UPDATES/REPORTS

US Government Accountability Office Report - Health Information Technology: HHS Should Assess the Effectiveness of Its Efforts to Enhance Patient Access to Use of Electronic Health Information

Ms. Byers wanted the council to be aware of this report. She was surprised that only 11% of patients access physician or hospital portals. Members agreed that when physicians recommend that patients use the portal and explain the benefits, patients are more likely to use portals. Some EHR vendors have more patient-friendly portals. The group also discussed the future of Meaningful Use Stage 3 and its possible impact on patient engagement.

Mr. Fattig shared that Nemaha County Hospital is working with NDHHS Division of Public Health to pilot Electronic Lab Reporting through NeHII.

POSSIBLE TOPICS FOR NEXT MEETING

Members made the following suggestions for topics for the next meeting:

- Public Health Data, Kathy Cook
- Population Health Analytics and Research
- Telehealth Network
- DHHS Behavioral Health CDS
- Medicaid Data Management and Architecture

ADJOURNMENT

With no further business, Ms. Morien adjourned the meeting at 3:22 p.m.

Meeting minutes were taken by Lori Lopez Urdiales and reviewed by Anne Byers, Office of the CIO/NITC.

EHEALTH COUNCIL
Nebraska Information Technology Commission
Oct. 12, 2017 9:30 A.M. CT – 11:30 P.M. CT
Varner Hall, Board Room, 3835 Holdrege St., Lincoln, NE
(Public Participation Video Connections Upon Request)

Members Present:
Marsha Morien, Co-Chair
Marty Fattig, Co-Chair
Jim McClay
Kevin Conway
Kathy Cook
Marty Fattig
Cindy Kadavy
Jenifer Roberts-Johnson
Brian Sterud

Public participation video connections (non-voting): Kevin Borcher, Max Thacker, Anna Turman (Video)

Members Absent: Joel Dougherty, Kimberly Galt, Rama Kolli, Dave Palm,Dr. Shawn Murdock, June Ryan, Todd Searls, Robin Szwanek; Linda Wittmuss, Delane Wycoff, and Bridget Young

ROLL CALL NOTICE OF POSTING OF AGENDA NOTICE OF NEBRASKA OPEN MEETINGS ACT POSTING

Co-Chair Marty Fattig called the meeting to order. Roll call was taken. There were 8 voting members present and three members at the public participation video connections who could participate but not vote. A quorum was not present to conduct official business.

Meeting notices were posted on the Public Meeting and NITC websites on September 19, 2017. The meeting agenda was posted on October 3, 2017.

APPROVAL OF APRIL 5, 2017 MINUTES*

The April meeting minutes were tabled until a quorum was present.

PUBLIC COMMENT

There was no public comment.

UPDATES

Nebraska Statewide Telehealth Network - Max Thacker

Mr. Thacker reported that the Nebraska Statewide Telehealth Network (NSTN) is in need of a major upgrade of its infrastructure and technical support. The network design has not been refreshed since 2004 with many of the rural hospitals still connecting to the network with T1 lines. Representatives of the Nebraska Statewide Telehealth Network have been in discussions with Ms. Byers and Mr. Rolfes to explore other options to support the network. Network Nebraska supports educational entities but could potentially be expanded to also support telehealth. For the telehealth network to become part of Network Nebraska, it will take a change in statute and there would need to be strong stakeholders support.

PDMP Update - Felicia Quintana-Zinn and Kevin Borcher

Ms. Quintana-Zinn shared important dates regarding the Nebraska Prescription Drug Overdose prevention efforts:

- January 1, 2017- Mandatory dispenser reporting of *dispensed controlled substances*
- January 1, 2018- Mandatory dispenser reporting of *all dispensed prescription drugs*
- July 1, 2018- Mandatory *veterinarian* reporting of *dispensed controlled substances*

The Harold Rogers, DOJ Bureau of Justice Assistance grant has been completed. The grant funded trainings PDMP trainings conducted through live webinars, on-demand webinars, and in-person sessions. Even though the grant has concluded, trainings are still be conducted. Training information is available on the PDMP website at www.dhhs.ne.gov/PDMP .

The Prescription Drug Overdose Prevention for States Grant (PDO-PfS) awarded by the CDC is still in progress. The purpose was to enhance and maximize the Nebraska PDMP system. Currently 3,987 prescibers (22.1% of those currently licensed in NE), 1514 dispensers(24.4% of those currently licensed in NE), and 120 designees (0.18% of those currently licensed/registered eligible individuals identified by the Uniform Credentialing Act in NE) are registered users of the PDMP. 100% of total eligible Nebraska Dispensers registered to report to the PDMP or noted as an exempted pharmacy for the 2017 year. A total of 2,040,451 dispensed records on 534,309 unique patients have been reported.

Two enhancements went live on Sept. 14, 2017: enhanced patient search and filter and sorting. In October through December 2017, three alerts will be implemented. The morphine milligram equivalents (MME) alert will place a notification alert banner on the patient's dispensed medication history page when a patient has received over 90 MME in the past 30 days. The 5/5/6 (Multiple Provider Episodes) Alert will place a notification alert banner on the patient's dispensed medication history page when a patient has dispensed opioid prescriptions from 5 or more prescribers and 5 or more dispensers over 6 month time period. The Overlapping Prescriptions Alert will place a notification alert banner on the patient's dispensed medication history page when a patient has overlapping dispensed opioids.

It is planned to have a public data dash board as well with different levels of information. DHHS has a grant to research mortality. The council suggested utilizing graduate research students to assist with the project's research and data trends. Council members were given an opportunity to ask questions.

ONC Grant Update - Anne Byers and Rachel Houseman

Ms. Byers reported that the ONC Advance Interoperable Health IT Services to Support HIE grant supported the adoption of health information exchange through NeHII in 47 facilities and health systems—including 21 Critical Access Hospitals (CAHs)—in 31 counties in Nebraska and in Montgomery County, Iowa. Through the grant, the number of hospitals and providers sharing data with NeHII increased from 28 to 53. Over 700 providers and clinical staff were added as users. New functionality implemented included population health analytics, the use of C-CDA exchange to provide information to NeHII, and an HIE to HIE gateway with the Missouri Health Exchange. Two Critical Access Hospitals were also successfully implemented to share syndromic surveillance data with the State's syndromic surveillance system. Council members were given an opportunity to ask questions.

NeHII Update - Rachel Houseman and Tony Troester

Mr. Troester just recently joined the NeHII team. He distributed a FAQ sheet regarding the Transforming Clinical Practice Initiative (TCPI), a federal contract by the Centers for Medicare and Medicaid Services

(CMS) to help clinicians achieve practice transformation and succeed in pay-for-performance funding models, providing better quality for more efficient costs. In October 2017, NeHII became the Nebraska state partner for TCPI services. Eligible clinicians for TCPI included: doctors-all specialties, podiatrists, optometrists, oral surgeons, dentist, chiropractors, physicians assistants, nurse practitioners, clinical nurse specialists, certified registered nurse anesthetists, anesthesiologist assistants, certified nurse midwives, clinical social workers, clinical psychologists, registered dieticians, nutrition professionals, audiologists, physical therapists, occupational therapists, and qualified speech-language therapists. The goal of the TCPI is to recruit 150,000 clinicians across the country. Council members were given an opportunity to ask questions.

PUBLIC HEALTH DATA - Kathy Cook

Public health is responsible for:

- Assessment and continuous monitoring of health status in communities served and convening the community to identify and prioritize issues/conditions that must be addressed
- Collaborating with stakeholders and partners to design and implement policies and programs to positively impact health of the community
- Continuing to assess and monitor health status to evaluate the impact of the policies and programs

None of this can be done without data about the community and the people who live in it. Almost any information about the population of the community or the environment of the community can be public health data.

Monitoring the health of the population is a core responsibility of public health – one of the three core functions of public health. All local health departments in Nebraska have or are completing a formal Community Health Assessment (CHA). The assessments are done every 3 to 5 years. Timely information is needed in order evaluate the effectiveness of the interventions/initiatives.

The advent of e-health data at the point of service, mechanisms for health data exchange, and creation of population health use cases for the use of aggregated data can potentially lead to:

- The opportunity to create measures that are more sensitive indicators of changes in overall community health.
- Significantly improved surveillance and early detection of diseases and events that threaten the health of the public.

Ms. Cook said that she is excited about the potential of NeHII to provide data in near real time to evaluate the effectiveness of interventions. Council members were given an opportunity to ask questions.

HIE AND PUBLIC HEALTH DISCUSSION

The Nebraska Department of Health and Human Services Division of Public Health is working with NeHII on several projects including the PDMP and syndromic surveillance. Other projects planned include a bidirectional interface with the immunization registry and electronic lab reporting through NeHII.

ACTION ITEMS FOR STATEWIDE TECHNOLOGY PLAN*

Suggestions made by the council included the following:

- Support efforts to modernize the Nebraska Statewide Telehealth Network
- Learn more about data governance and discuss follow-up steps including possibly forming a Data Governance Work Group

- Learn more about how health IT can support public health, including the priorities identified in the 2017-2021 Nebraska State Health Improvement Plan, and discuss follow-up steps.

Ms. Roberts-Johnson will send Ms. Byers the DHHS 5-year State Health Plan to share with members.

Ms. Byers will draft the action items and send to members for input.

ADJOURN

With no further business, Mr. Fattig adjourned the meeting at 11:28 a.m.

Meeting minutes were taken by Lori Lopez Urdiales and reviewed by Anne Byers of the Office of the CIO.

The Office of the National Coordinator for Health Information Technology

Understanding The Draft Trusted Exchange Framework

Zoe Barber, Special Assistant, Principal Deputy National Coordinator

March 13, 2018

What is the Draft Trusted Exchange Framework?

Format of the Draft Trusted Exchange Framework

Part A—Principles for Trusted Exchange

General principles that provide guardrails to engender trust between Health Information Networks (HINs). Six (6) categories:

- » **Principle 1 - Standardization:** *Adhere to industry and federally recognized standards, policies, best practices, and procedures.*
- » **Principle 2 - Transparency:** *Conduct all exchange openly and transparently.*
- » **Principle 3 - Cooperation and Non-Discrimination:** *Collaborate with stakeholders across the continuum of care to exchange electronic health information, even when a stakeholder may be a business competitor.*
- » **Principle 4 - Security and Patient Safety:** *Exchange electronic health information securely and in a manner that promotes patient safety and ensures data integrity.*
- » **Principle 5 - Access:** *Ensure that patients and their caregivers have easy access to their electronic health information.*
- » **Principle 6 - Data-driven Accountability:** *Exchange multiple records at one time to enable identification and trending of data to lower the cost of care and improve the health of the population.*

Part B—Minimum Required Terms and Conditions for Trusted Exchange

A minimum set of terms and conditions for the purpose of ensuring that common practices are in place and required of all participants who participate in the Trusted Exchange Framework, including:

- » Common authentication processes of trusted health information network participants;
- » A common set of rules for trusted exchange;
- » A minimum core set of organizational and operational policies to enable the exchange of electronic health information among networks.

Goals of the Draft Trusted Exchange Framework

GOAL 1

Build on and extend existing work done by the industry

The Draft Trusted Exchange Framework recognizes and builds upon the significant work done by the industry over the last few years to broaden the exchange of data, build trust frameworks, and develop participation agreements that enable providers to exchange data across organizational boundaries.

GOAL 2

Provide a single "on-ramp" to interoperability for all

The Draft Trusted Exchange Framework provides a single "on-ramp" to allow all types of healthcare stakeholders to join any health information network they choose and be able to participate in nationwide exchange regardless of what health IT developer they use, health information exchange or network they contract with, or where the patients' records are located.

GOAL 3

Be scalable to support the entire nation

The Draft Trusted Exchange Framework aims to scale interoperability nationwide both technologically and procedurally, by defining a floor, which will enable stakeholders to access, exchange, and use relevant electronic health information across disparate networks and sharing arrangements.

GOAL 4

Build a competitive market allowing all to compete on data services

Easing the flow of data will allow new and innovative technologies to enter the market and build competitive, invaluable services that make use of the data.

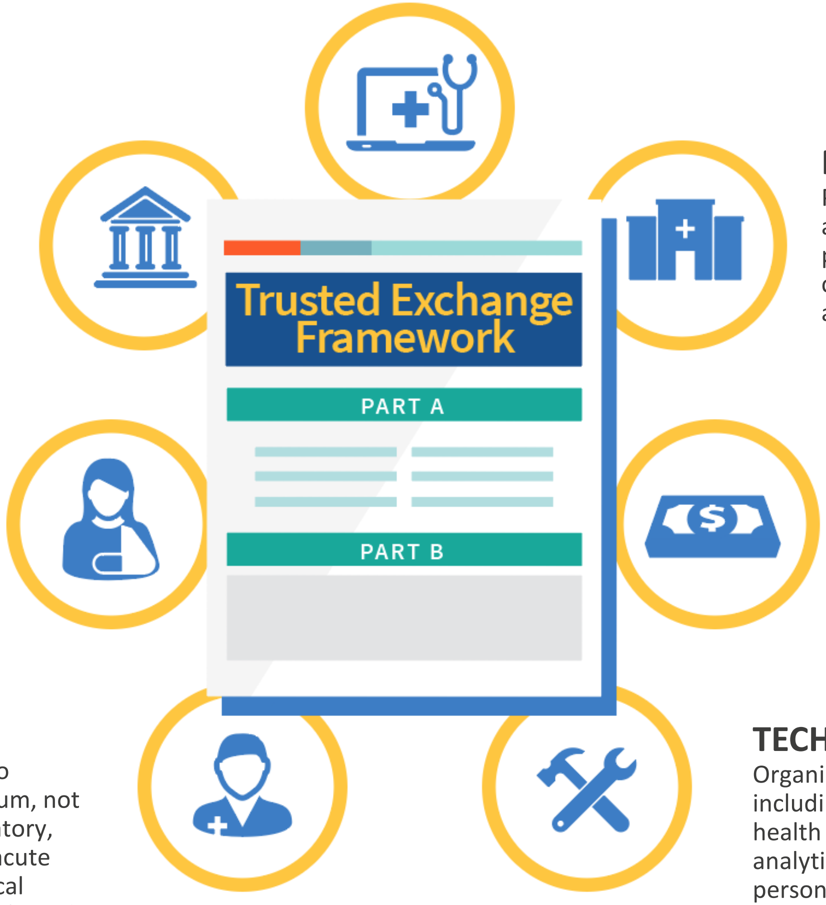
GOAL 5

Achieve long-term sustainability

By providing a single "on-ramp" to nationwide interoperability while also allowing for variation around a broader set of use cases, the Draft Trusted Exchange Framework ensures the long-term sustainability of its participants and end-users.

Stakeholders who can use the Trusted Exchange Framework

HEALTH INFORMATION NETWORKS



FEDERAL AGENCIES
Federal, state, tribal, and local governments

PUBLIC HEALTH
Public and private organizations and agencies working collectively to prevent, promote and protect the health of communities by supporting efforts around essential public health services

INDIVIDUALS
Patients, caregivers, authorized representatives, and family members serving in a non-professional role

PAYERS
Private payers, employers, and public payers that pay for programs like Medicare, Medicaid, and TRICARE

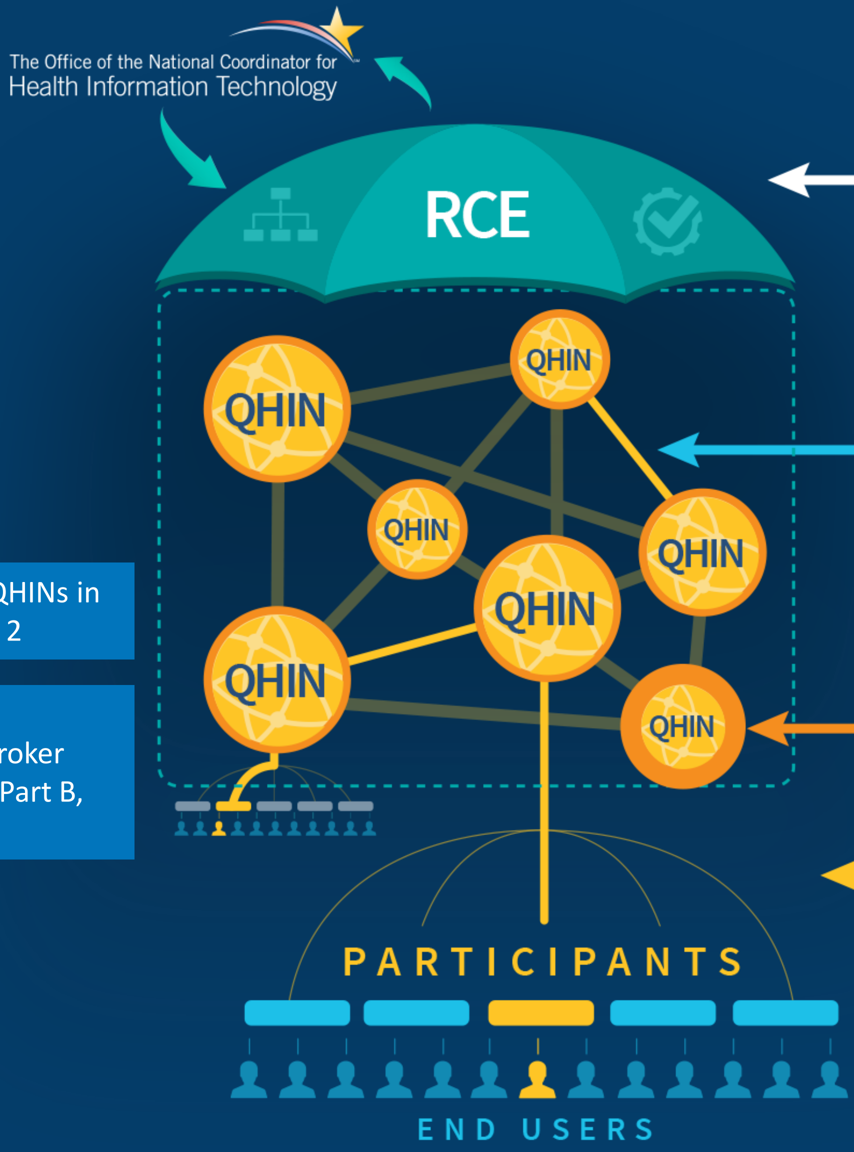
PROVIDERS
Professional care providers who deliver care across the continuum, not limited to but including ambulatory, inpatient, long-term and post-acute care (LTPAC), emergency medical services (EMS), behavioral health, and home and community based services

TECHNOLOGY DEVELOPERS
Organizations that provide health IT capabilities, including but not limited to electronic health records, health information exchange (HIE) technology, analytics products, laboratory information systems, personal health records, Qualified Clinical Data Registries (QCDRs), registries, pharmacy systems, mobile technology, and other technology that provides health IT capabilities and services

The Office of the National Coordinator for Health Information Technology

How will the Trusted Exchange Framework work?

How Will the Trusted Exchange Framework Work?


The Office of the National Coordinator for
Health Information Technology
RCE
QHIN
QHIN
QHIN
QHIN
QHIN
QHIN
QHIN
PARTICIPANTS
END USERS

READ MORE: QHINs in Part B, Section 2

READ MORE: Connectivity Broker Capabilities in Part B, Section 3

RCE provides oversight and governance for Qualified HINS.

Qualified HINs connect directly to each other to serve as the core for nationwide interoperability.

QHINs connect via connectivity brokers.

Each Qualified HIN represents a variety of networks and participants that they connect together, serving a wide range of end users.

Recognized Coordinating Entity (RCE)

Recognized Coordinating Entity

The RCE is the entity selected by ONC that will enter into agreements with HINs that qualify and elect to become Qualified HINs in order to impose, at a minimum, the requirements of the Common Agreement set forth herein on the Qualified HINs and administer such requirements on an ongoing basis as described herein.

The RCE will act as a governance body that will operationalize the Trusted Exchange Framework by incorporating it into a single, all-encompassing Common Agreement to which Qualified HINs will agree to abide. In its capacity as a governance body, the RCE will be expected to monitor Qualified HINs compliance with the final TEFCA and take actions to remediate non-conformity and non-compliance by Qualified HINs, up to and including the removal of a Qualified HIN from the final TEFCA and subsequent reporting of its removal to ONC.

The RCE will also be expected to work collaboratively with stakeholders from across the industry to build and implement new use cases that can use the final TEFCA as their foundation, and appropriately update the TEFCA over time to account for new technologies, policies, and use cases.

READ MORE: How Will it Work?

Recognized Coordinating Entity (RCE)

2018 Selection

Process for Recognizing Entity

ONC will release an open, competitive Funding Opportunity Announcement (FOA) in spring 2018 to award a single multi-year Cooperative Agreement to a private sector organization or entity. The RCE will need to have experience with building multi-stakeholder collaborations and implementing governance principles in order to be eligible to apply for the Cooperative Agreement.

Expectations for Entity

ONC will work with the RCE to incorporate the Trusted Exchange Framework into a single Common Agreement to which Qualified HINs and their participants voluntarily agree to adhere.

The RCE will **have oversight, enforcement, and governance responsibilities for each of the Qualified HINs** who voluntarily adopt the final TEFCA.

READ MORE: How Will it Work?

Defining Terms:
Who is the Trusted Exchange Framework applicable to?

The Trusted Exchange Framework aims to create a technical and governance infrastructure that connects

Health Information Networks

together through a core of

Qualified Health Information Networks.

The Office of the National Coordinator for
Health Information Technology

What is a Health Information Network?

Health Information Networks (HINs) are an Individual or Entity that:

1. Determines, oversees, or administers policies or agreements that define business, operational, technical, or other conditions or requirements for enabling or facilitating access, exchange, or use of electronic health information between or among two or more unaffiliated individuals or entities;

2. Provides, manages, or controls any technology or service that enables or facilitates the exchange of electronic health information between or among two or more unaffiliated individuals or entities; or

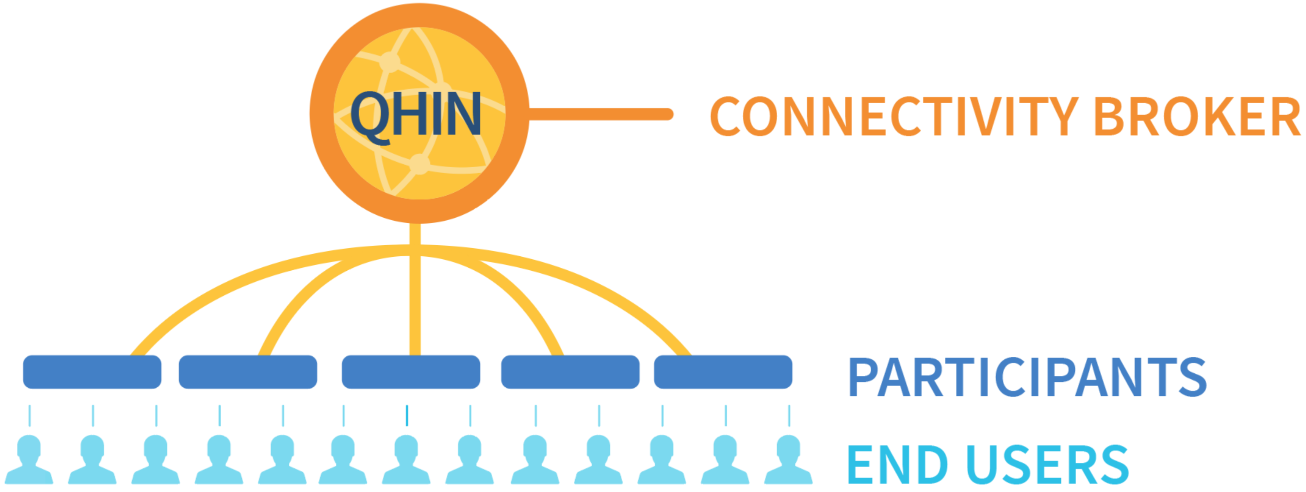
3. Exercises substantial influence or control with respect to the access, exchange, or use of electronic health information between or among two or more unaffiliated individuals or entities.

What is a Qualified Health Information Network?

A Qualified Health Information Network (Qualified HIN) must meet ALL of the requirements of a HIN. In addition, it must also:

- Be able to locate and transmit ePHI between multiple persons and/or entities electronically;
- Have mechanisms in place to impose Minimum Core Obligations and to audit Participants' compliance;
- Have controls and utilize a Connectivity Broker service;
- Be participant neutral; and
- Have Participants that are actively exchanging the data included in the USCDI in a live clinical environment.

Structure of a Qualified Health Information Network



READ MORE: QHINs in Part B, Section 2

READ MORE: Connectivity Broker Capabilities in Part B, Section 3

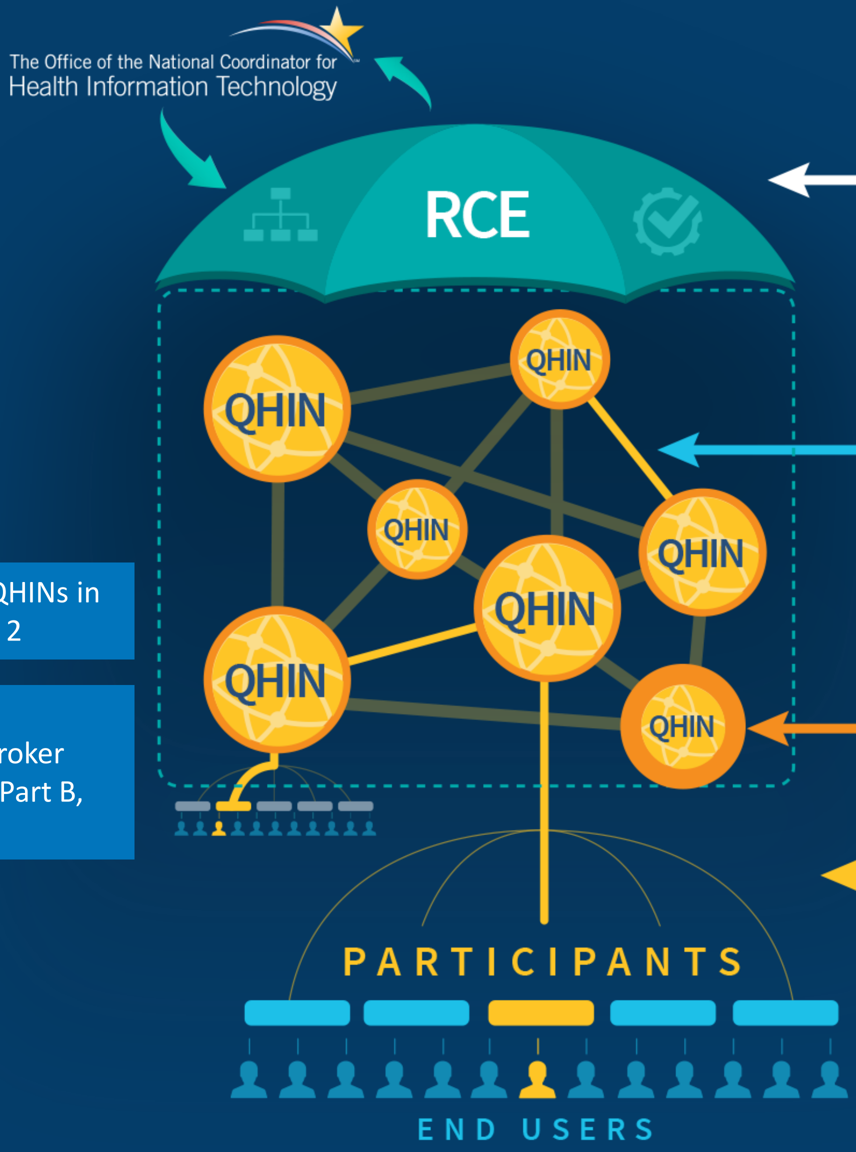
A Qualified HIN (QHIN) is a network of organizations working together to share data. QHINs will connect directly to each other to ensure interoperability between the networks they represent.

A Connectivity Broker is a service provided by a Qualified HIN that provides all of the following functions with respect to all Permitted Purposes: master patient index (federated or centralized); Record Locator Service; Broadcast and Directed Queries, and EHI return to an authorized requesting Qualified HIN.

A Participant is a person or entity that participates in the QHIN. Participants connect to each other through the QHIN, and they access organizations not included in their QHIN through QHIN-to-QHIN connectivity. Participants can be HINs, EHR vendors, and other types of organizations.

An End User is an individual or organization using the services of a Participant to send and/or receive electronic health info

How Will the Trusted Exchange Framework Work?


The Office of the National Coordinator for
Health Information Technology
RCE
QHIN
QHIN
QHIN
QHIN
QHIN
QHIN
QHIN
PARTICIPANTS
END USERS

READ MORE: QHINs in Part B, Section 2

READ MORE: Connectivity Broker Capabilities in Part B, Section 3

RCE provides oversight and governance for Qualified HINS.

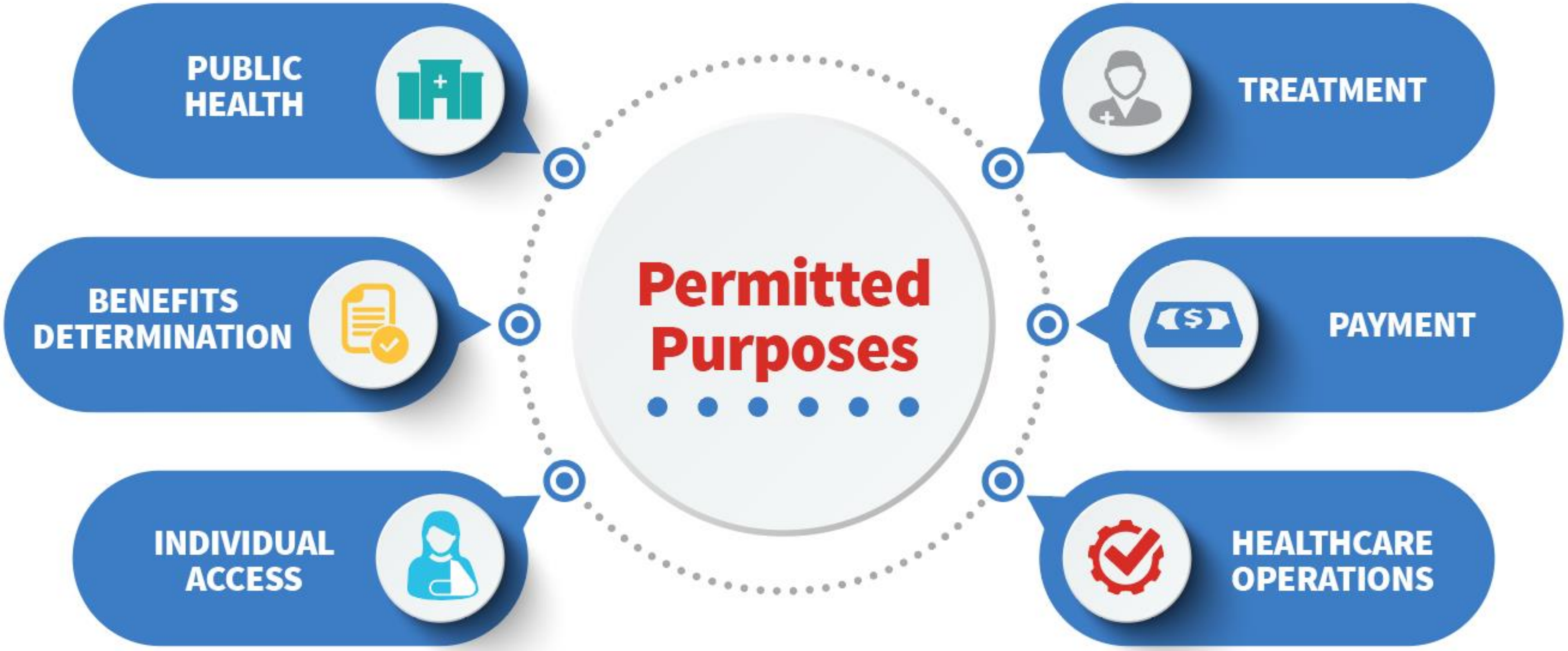
Qualified HINs connect directly to each other to serve as the core for nationwide interoperability.

QHINs connect via connectivity brokers.

Each Qualified HIN represents a variety of networks and participants that they connect together, serving a wide range of end users.

What use cases are covered under the Trusted Exchange Framework?

Permitted Purposes



READ MORE: Part B, Section 1

Use Cases

Broadcast Query

Sending a request for a patient’s Electronic Health Information (EHI) to all Qualified HINs to have data returned from all organizations who have it.

Supports situations where it is unknown who may have Electronic Health Information about a patient.

Directed Query

Sending a targeted request for a patient’s Electronic Health Information to a specific organization(s).

Supports situations where you want specific Electronic Health Information about a patient, for example data from a particular specialist.

READ MORE: Broadcast and Directed Queries- Part B, Section 5.4 and Section 3

READ MORE: Population level data- Part B, Section 8

Population Level Data

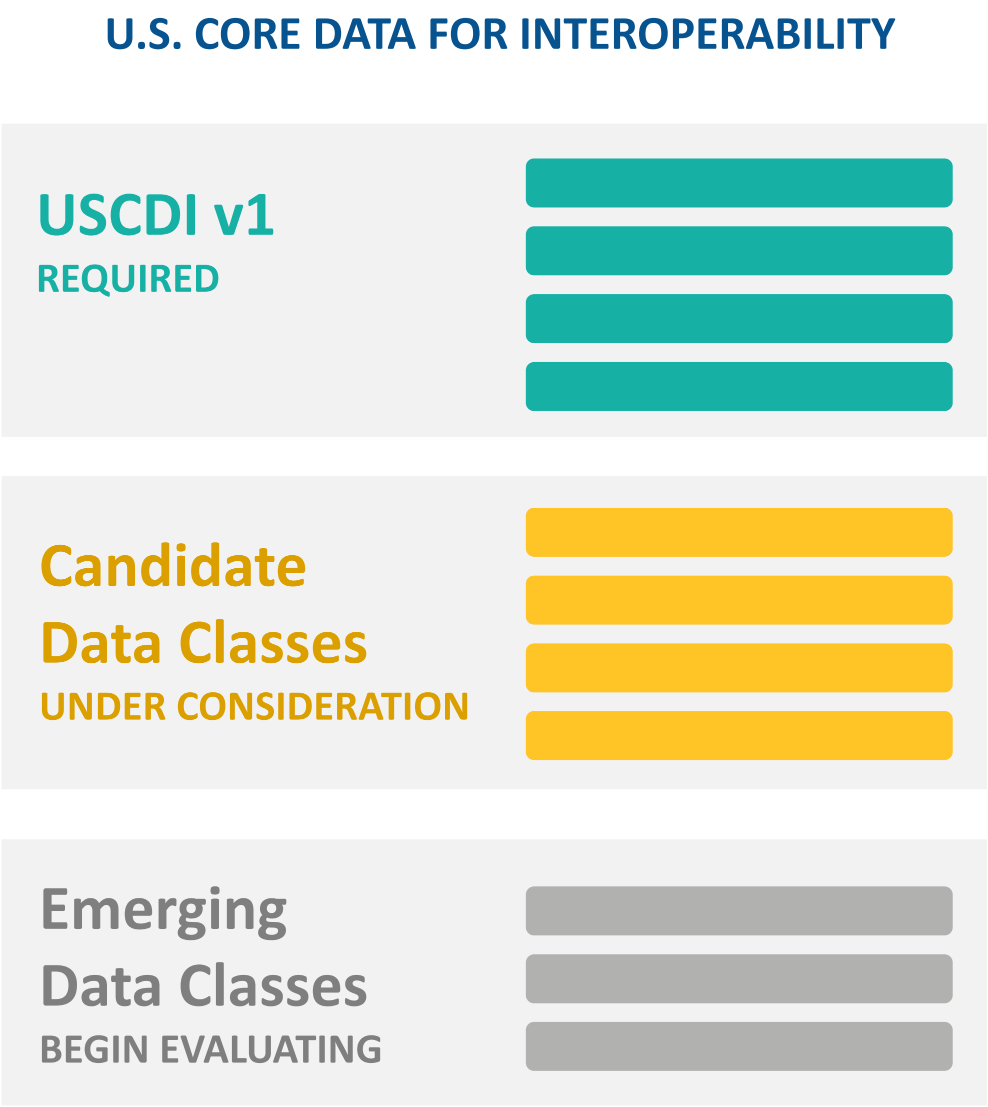
Querying and retrieving Electronic Health Information about multiple patients in a single query.

Supports population health services, such as quality measurement, risk analysis, and other analytics.

US Core Data for Interoperability (USCDI) Glide Path

The USCDI establishes a minimum set of data classes that are required to be interoperable nationwide and is designed to be expanded in an iterative and predictable way over time. Data classes listed in the USCDI are represented in a technically agnostic manner.

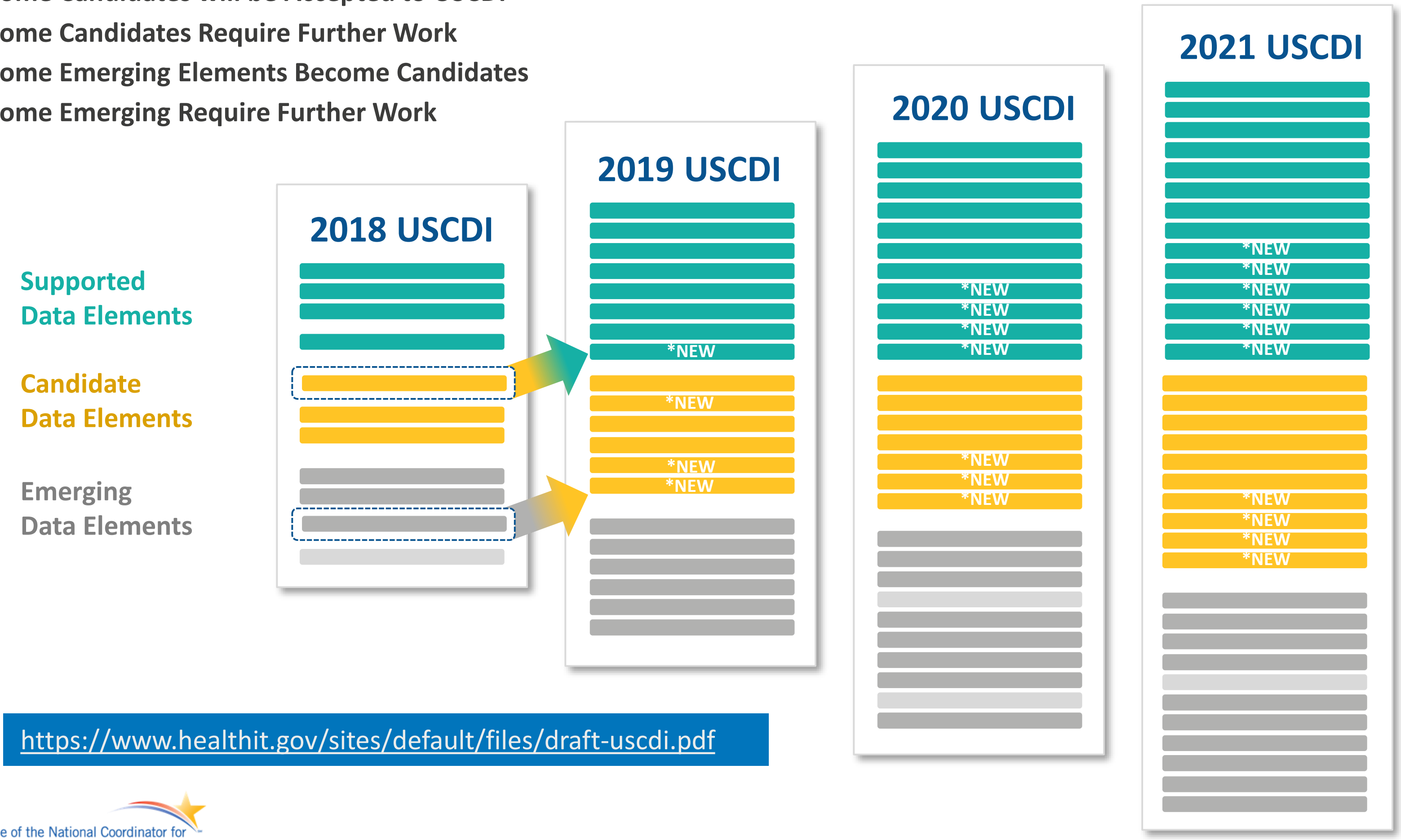
1. **USCDI v1— Required—CCDS plus Clinical Notes and Provenance**
2. **Candidate Data Classes—Under consideration for USCDI v2**
3. **Emerging Data Classes– Begin evaluating for candidate status**



Expansion of US Core Data for Interoperability (USCDI)

As the USCDI expands, Qualified HINs and their Participants will be required to upgrade their technology to support the data specified in the USCDI.

Some Candidates will be Accepted to USCDI
Some Candidates Require Further Work
Some Emerging Elements Become Candidates
Some Emerging Require Further Work



https://www.healthit.gov/sites/default/files/draft-uscdi.pdf

What privacy and security protections does the Trusted Exchange Framework guarantee?

Privacy/Security: Identity Proofing

Identity proofing is the process of verifying a person is who they claim to be. The Trusted Exchange Framework requires identity proofing (referred to as the Identity Assurance Level (IAL) in SP 800-63A).

End Users and Participants Each Qualified HIN shall require proof of identity for Participants and participating End Users at a minimum of IAL2 prior to issuance of credentials.

Individuals Each Qualified HIN shall require its End Users and Participants to proof the identity for Individuals at a minimum of IAL2 prior to issuance of credentials. Individuals must provide strong evidence of their identity.

IAL 2 REQUIREMENT	DESCRIPTION
Evidence	• One (1) piece of SUPERIOR or STRONG evidence; OR • Two (2) pieces of STRONG evidence; OR • One (1) piece of STRONG evidence plus two (2) pieces of ADEQUATE evidence
Validation	• Each piece of evidence must be validated with a process able to achieve the same strength as the evidence presented. • Validation against a third-party data service SHALL only be used for one piece of presented identity evidence.
Address Confirmation	• The Credential Service Provider (CSP) SHALL confirm address of record through validation of the address contained on any supplied, valid piece of identity evidence.

READ MORE: Part B, Section 6.2.4

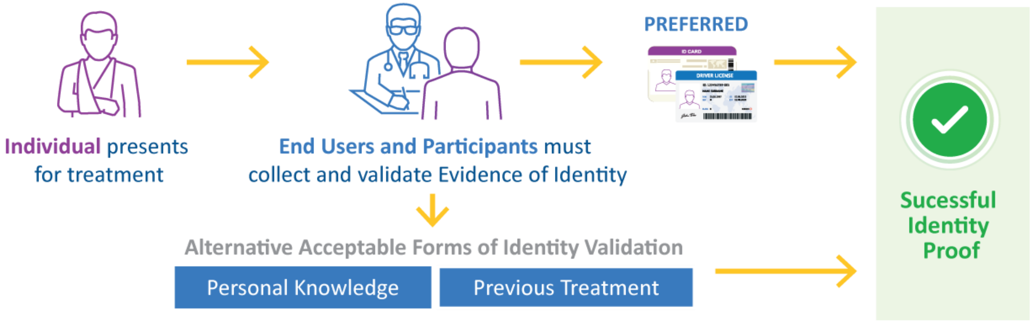
* Full IAL2 requirements can be found at www.nist.gov.

Privacy/Security: Identity Proofing - EXCEPTIONS

Qualified HINs, Participants, or End Users are responsible for proofing Individuals at the IAL2 level, HOWEVER:

Trusted Referee and Authoritative Source:
In instances where the individual enrolling cannot meet the identity evidence requirements specified, organization staff may act as a trusted referee, allowing them to use personal knowledge of the identity of patients when enrolling patients as subscribers to assist in identity proofing the enrollee.

Antecedent Event: Staff may also act as authoritative sources by using knowledge of the identity of the individuals (e.g., physical comparison to legal photographic identification cards such as driver's licenses or passports, or employee or school identification badges) collected during an antecedent, in-person registration event.



Individual presents for treatment

End Users and Participants must collect and validate Evidence of Identity

PREFERRED

Alternative Acceptable Forms of Identity Validation

Personal Knowledge

Previous Treatment

Sucessful Identity Proof

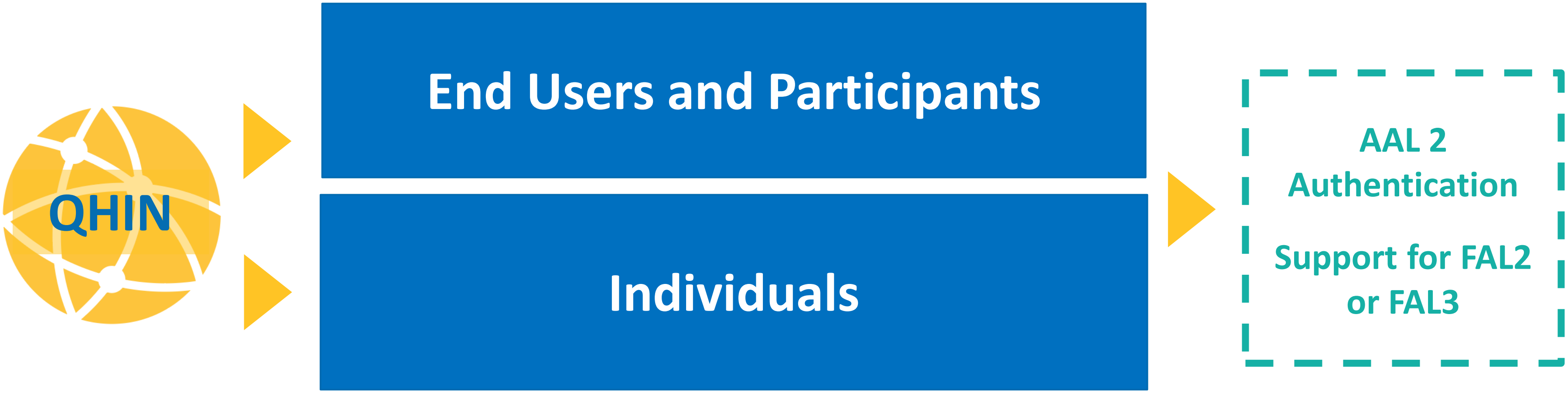
READ MORE: Part B, Section 6.2.4

For example, IAL2 identity proofing for an Individual can be accomplished by two of the following:

1. Physical comparison to legal photographic identification cards such as driver's licenses or passports, or employee or school identification badges,
2. Comparison to information from an insurance card that has been validated with the issuer, e.g., in an eligibility check within two days of the proofing event, and
3. Comparison to information from an electronic health record (EHR) containing information entered from prior encounters.

Privacy/Security: Authentication

Digital authentication is the process of establishing confidence in a remote user identity communicating electronically to an information system. NIST draft SP 800-63B refers to the level of assurance in authentication as the Authenticator Assurance Level (AAL). Federal Assurance Level (FAL) refers to the strength of an assertion in a federated environment, used to communicate authentication and attribute information (if applicable) to a relying party (RP).



QHIN

End Users and Participants

Individuals

AAL 2 Authentication

Support for FAL2 or FAL3

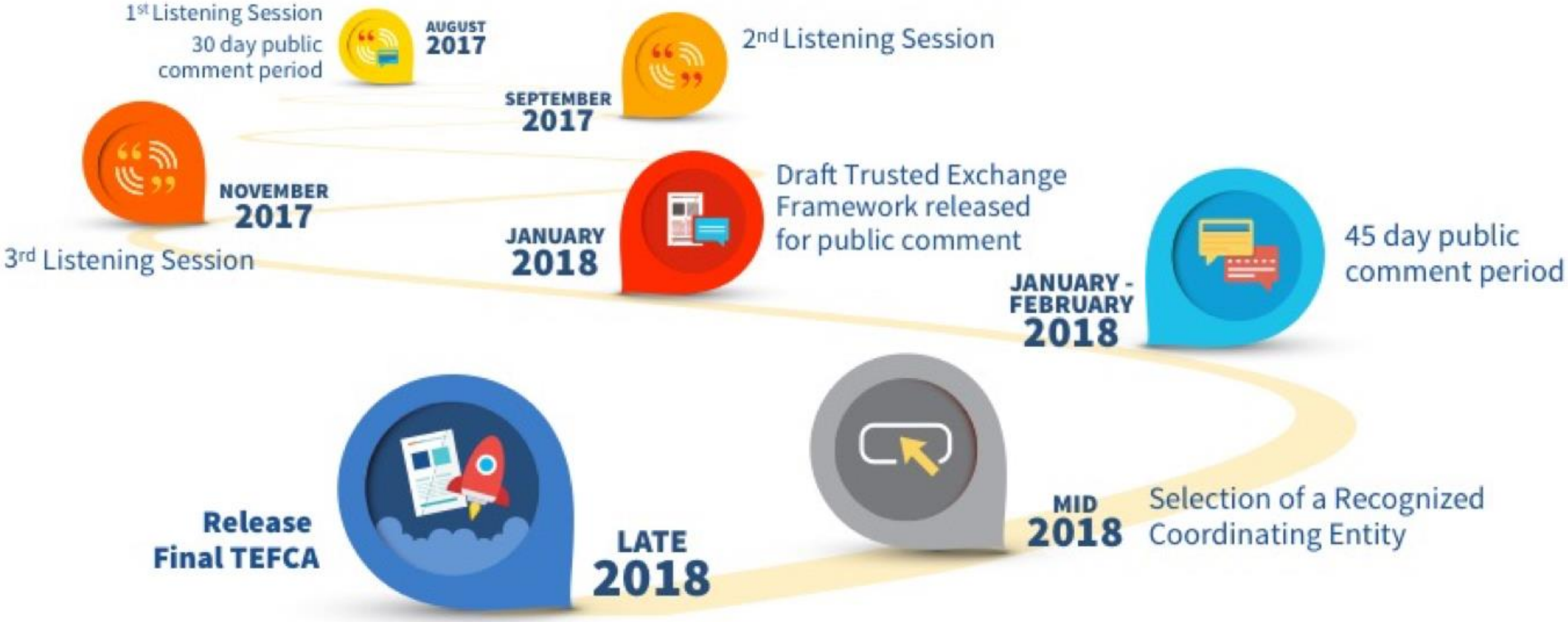
Each Qualified HIN shall authenticate End Users, Participants, and Individuals at a minimum of AAL2, and provide support for at least FAL2 or, alternatively, FAL3.

Connecting to a Qualified HIN or one of its Participant will require **two-factor authentication**. A list of acceptable second factors (in addition to a username and password) can be found at https://pages.nist.gov/800-63-3/sp800-63b/sec4_aal.html.

READ MORE: Part B, Section 6.2.5

When will the Trusted Exchange Framework be implemented?

Timeline


1st Listening Session
30 day public comment period
AUGUST 2017
SEPTEMBER 2017
2nd Listening Session
NOVEMBER 2017
3rd Listening Session
JANUARY 2018
Draft Trusted Exchange Framework released for public comment
JANUARY - FEBRUARY 2018
45 day public comment period
MID 2018
Selection of a Recognized Coordinating Entity
LATE 2018
Release Final TEFCA

INFORMATION GOVERNANCE
Principles for Healthcare (IGPHC)™

INFORMATION GOVERNANCE
Principles for Healthcare (IGPHC)™

PREAMBLE

Complete, current, and accurate *information* is essential for any organization in the healthcare industry to achieve its goals. Adoption of an information governance program underscores the organization's commitment to managing its information as a valued strategic asset. Governance of clinical and operational information:

- Improves quality of care and patient safety
- Improves population health
- Increases operational efficiency and effectiveness
- Reduces costs
- Reduces risk

Information governance helps manage and control information by supporting the organization's activities and ensuring compliance with its duties. Drawing from definitions of Gartner and ARMA International, AHIMA defines information governance as an organization-wide framework for managing information throughout its lifecycle and supporting the organization's strategy, operations, regulatory, legal, risk, and environmental requirements.

Information governance establishes policy, prioritizes investments, values and protects information assets, and determines accountabilities for managing information, making it an imperative for healthcare. It also promotes objectivity through robust, repeatable processes insulated from individual, organizational, political, or other biases, and then protects information with suitable controls. By following *information governance* principles, organizations conduct their operations effectively, while ensuring compliance with legal requirements and other duties and responsibilities.

Healthcare as a Unique Information Environment

Trust plays a critical role in healthcare delivery. Patients entrust their personal information to healthcare organizations, creating distinct requirements for confidentiality, privacy, and security. These organizations, regardless of their roles in healthcare, must earn the confidence of patients and society, through a firm commitment to ethical and responsible handling of personal information.

Embedded in trust is the expectation of information *integrity*, which depends on the completeness and correctness of data. Heightened focus on integrity to ensure confidence in information is demanded by the nature of healthcare, changes in care delivery and payment models, the increasing adoption of electronic systems, and the importance of reliable information exchange.

Healthcare organizations have an obligation to define uses of information and to define the policies and practices for governing use of the information. This includes protected health information, personally identifiable information, de-identified and anonymized information, aggregate and detailed information used to satisfy mandatory or voluntary reporting purposes, operational needs, secondary uses of data/information, and other uses based on the role and mission of the organization.

Research is fundamental to advancing the science of medicine. New guidelines, protocols, treatments, interventions and wellness insights, all developed through research, are essential to elevating population health. Research, whether focused on clinical care, delivery systems, or payment models, depends on trusted information.

> “Trust plays a critical role in healthcare delivery. Patients entrust their personal information to healthcare organizations, creating distinct requirements for confidentiality, privacy, and security. These organizations, regardless of their roles in healthcare, must earn the confidence of patients and society, through a firm commitment to ethical and responsible handling of personal information.”

Healthcare organizations must value and govern not only their clinical, but their nonclinical information, such as human resources, operational, financial, legal, and marketing information. Reliable information is essential to reducing healthcare delivery costs and improving operational efficiencies. For these reasons, establishing and implementing principles for the governance of clinical and nonclinical information, in all formats and on all media, increases in significance.

> “The adherence to information and technology standards across healthcare is compelled, as standards are crucial to information use and exchange given the imperatives of integrity, security and interoperability.”

The *healthcare ecosystem* consists of a variety of organizations and stakeholders, who share common goals. These organizations encompass healthcare *providers*, as well as *nonproviders*. Providers include all types and settings of healthcare service organizations. Nonproviders include organizations such as information exchanges, health plans, third party administrators, data clearinghouses, and other information intensive organizations. Indeed, an organization's entire *workforce*, including employed and contracted individuals, and where applicable all members of its nonemployed medical and professional staffs, are accountable for the responsible and ethical handling of information. The responsibility for practicing in accordance with organization's governance policies and procedures extends to outsourced services and their workforces, as well as to business partners and affiliates who use information or handle any aspect of information management for the organization.

Challenges facing the healthcare industry include:

- Expanding numbers of electronic systems/applications in use within and across organizations,
- Growing volume and variety of data and information,
- Expanding uses of healthcare information,
- Proliferation of medical devices creating data for which reliable integration into systems/applications is essential,
- State of interoperability across devices and systems, and
- Reliability of shared and exchanged information.

These challenges and complexities underscore the need for information governance, and the need for their due consideration in its adoption. The adherence to information and technology standards across healthcare is compelled, as standards are crucial to information use and exchange given the imperatives of integrity, security and *interoperability*.

- Despite the diversity in the healthcare industry, information across the various types of organizations can be governed using eight principles: accountability, transparency, integrity, protection, compliance, availability, retention, and disposition. These principles can be adopted in any organization within the healthcare industry.

Information Governance Principles for Healthcare

The principles of information governance, known as the *Information Governance Principles for Healthcare (IGPHC)*™, are comprehensive and written broadly. They do not set forth a legal rule for which strict adherence is required by every organization in every circumstance, but are intended to be interpreted and applied depending upon an organization's type, size, role, mission, sophistication, legal environment, and resources.

The *IGPHC*™ are based on practical experience, information theory, and legal doctrine within healthcare and further informed by other established practices and tenets from areas such as quality improvement, safety, risk management, compliance, data governance, information technology governance, privacy, and security. They are grounded in several common, yet essential, values embedded in healthcare—*accuracy, timeliness, accessibility*, and integrity. These values serve the best interests of the healthcare information consumer, from providers to nonproviders, from researchers to public health officials, from information exchanges to policymakers, from claims administrators to payers, and from patients to society.

AHIMA has convened healthcare industry stakeholders and leaders, as well as information governance experts from other industries to articulate the *IGPHC*™ through adaptation of ARMA International's Generally Accepted Recordkeeping Principles. Based on the general principles which apply to all industries, the *IGPHC*™ are specifically aimed at healthcare industry organizations. Therefore, the *IGPHC*™ apply not only to the governance of healthcare information, but also to the governance of information across all functions of organizations in the healthcare industry.

The adoption of these principles by an organization reflects a dedication to strengthen its information governance, and increase its effectiveness for the benefit of its patients, stakeholders, and society. These principles form the basis upon which every effective information governance program is built, measured, and eventually judged.

Therefore, it is in the best interest of patients, other consumers, society, and all organizations in the healthcare *ecosystem*, that there is full awareness of the *Information Governance Principles for Healthcare (IGPHC)*™ and that *information assets* be managed in accordance with them.

PRINCIPLE OF ACCOUNTABILITY

An *accountable member of senior leadership*, or a person of comparable authority, shall oversee the information governance program and delegate program responsibility for information management to appropriate individuals.

The governing body of the organization is ultimately accountable for the adoption of information governance practices and should require regular reporting by the designated member of senior leadership. The organization should adopt policies and procedures to guide its workforce and agents and ensure its program can be audited and continually improved to support the organization's goals.

An information governance program should:

- Establish an information governance structure for program development and implementation
- Designate a qualified accountable person to develop and implement the program
- Document and approve policies and procedures to guide its implementation
- Remediate identified issues
- Enable auditing as a means of demonstrating the organization is meeting its obligations to both internal and external parties

A basic premise of sound information governance is that within each organization a senior leader is formally designated as responsible for the overall program development and its implementation. The senior leader is accountable for ensuring the information governance program aligns with and supports the goals and strategies of the organization. The senior leader is also accountable for ensuring appropriate resources are allocated to support the program.

Governance should be established throughout the organization, utilizing a collaborative approach, with input of stakeholders, business process owners, and domain experts, assigning defined roles and responsibilities to workforce members. It should be clear where responsibilities reside and how the chain of command builds, implements, and updates the information governance program. For example, sub-committees can be designated to help build policies, define and implement technology, or improve the information governance program.

> "Governance should be established throughout the organization, utilizing a collaborative approach, with input of stakeholders, business process owners and domain experts, assigning defined roles and responsibilities to workforce members."

To assist the workforce in understanding how to implement information governance practices, it is essential that policies and procedures are documented, formally approved, and communicated. The workforce should be continuously trained in program policies and any relevant updates to standardize information governance practices across the organization and to reinforce compliance with and standardization of practices.

A senior leader at an appropriate level of authority shall oversee program compliance monitoring/audit and improvement. Audits should be performed to determine the following:

- The workforce demonstrates program awareness
- The workforce is trained in information governance practices, policies, and responsibilities
- Information is appropriately protected, accessed, stored, and released with a properly documented audit trail
- Information is available when and where it is needed
- Information is retained for the right amount of time and properly dispositioned when no longer required
- Policies are up-to-date, adopted, and cover all types of information in all media

An organization's information governance audit should be reported to its board of directors, trustees, audit committee, or other appropriate governing body, committee, or individual to show adherence in accordance with its program requirements and the organization's goals.

P PRINCIPLE OF TRANSPARENCY

An organization's processes and activities relating to information governance shall be documented in an open and verifiable manner. Documentation shall be available to the organization's workforce and other appropriate interested parties within any legal or regulatory limitations, and consistent with the organization's business needs.

> “The clearest and most durable evidence of the organization's operations, decisions, activities, and performance are its records and information.”

Transparency of the organization's governance practices must extend to definitions of appropriate information uses and the processes for ensuring compliance with policies on appropriate information use.

The clearest and most durable evidence of the organization's operations, decisions, activities, and performance are its records and information. An information governance program includes its information management and information control policies and procedures. To ensure the confidence of interested parties, records documenting the information governance program must themselves adhere to the fundamentals of information management. These records should:

- Document the principles and processes that govern the program
- Accurately and completely record the activities undertaken to implement the program
- Be available to legitimately interested parties in a timely and reasonable manner

The information documented in these records and the extent to which they are available to interested parties will vary depending upon the nature and circumstances of the organization. For example, healthcare organizations have a legitimate need to protect confidential and proprietary information. Therefore, procedures shall be put in place to control access to protected information, whether it relates to the confidentiality of information or the confidentiality of proprietary processes.

Various parties have a legitimate interest in understanding the information governance program activities and processes. In addition to the organization itself and its workforce, those parties include, but are not limited to, patients and consumers, government authorities, auditors and investigators, litigants, and for some organizations, the general public.

Complex and highly regulated records and information management systems may require extensive records documenting their governance. Simple systems may require only a few. In each case, however, the rationale and results should be clear to legitimately interested parties.

Each organization must therefore create and manage the records documenting its information governance program to ensure its structure, processes, and practices are apparent, understandable, and reasonably available to legitimately interested parties.

PRINCIPLE OF INTEGRITY

An information governance program shall be constructed so the information generated by, managed for, and provided to the organization has a reasonable and suitable guarantee of authenticity and reliability.

Integrity of information, which is expected by patients, consumers, stakeholders, and other interested parties such as investors and regulatory agencies, is directly related to the organization's ability to prove that information is *authentic, timely, accurate, and complete*. For the healthcare industry, these dimensions of integrity are essential to ensuring trust in information.

For safety, quality of care, and compliance with applicable voluntary, regulatory and legal requirements, integrity of information should include at least the following considerations:

- Adherence to the organization's policies and procedures
- Appropriate workforce training on information management and governance
- Reliability of information
- Admissibility of records for litigation purposes
- Acceptable audit trails
- Reliability of systems that control information

Information from External Sources

It is critical that organizations determine their responsibilities and processes for classifying and managing information received from other sources.

> "Information governance incorporates the *governance of data*. As data are the building blocks of information, information cannot be reliable if the data are not reliable."

A healthcare organization's information may contain patient or other business information that originated from another healthcare organization. For example, copies of selected patient reports are often sent by one healthcare provider to another where a patient is admitted. Information received from the previous provider is then incorporated into the patient's health record at the receiving organization. Organizations must comply with re-disclosure responsibilities under all relevant laws.

Information Governance Policies and Procedures

Adherence to information governance policies and procedures that have been approved by senior management is essential to an organization's ability to achieve legal and regulatory compliance, as well as consistently carrying out information governance practices. If adherence to policies and procedures is not substantiated, records may be at risk of not being accepted as having evidentiary value.

Appropriate Training on Information Management and Governance

The organization shall provide training to all workforce members, and outsourced or contracted individuals when appropriate, on the meaning and importance of compliance with its policies and procedures.

> “*Integrity* of information, which is expected by patients, consumers, stakeholders and other interested parties such as investors, and regulatory agencies, is directly related to the organization’s ability to prove that information is *authentic, timely, accurate, and complete.*”

Reliability of Information

Organizations should define and apply consistent information governance practices throughout the information lifecycle. This helps ensure information is managed in the usual and ordinary course of business, and in a manner which ensures integrity and compliance with accepted industry standards for quality. Given the variety, complexity, and risks associated with information assets, the lifecycle practices should incorporate a means of classifying and valuing information.

Reliability of information is of paramount importance in the delivery of healthcare services. Based on the nature and type of healthcare organization, measures to ensure reliability of data and information should be built in to processes and systems for creation and capture, processing, and other applicable stages of the information’s lifecycle. Such measures will promote quality of care, patient safety, and operational efficiency. Examples of such ongoing measures include field-specific data edits built into systems/applications; monitoring and correction of vendor identity errors and patient identity errors; monitoring and correction of documentation completeness and data accuracy; and ongoing data quality controls.

Information governance incorporates the *governance of data*. As data are the building blocks of information, information cannot be reliable if the data are not reliable. Data and information are inextricably linked, and the goals of information governance will not be achieved if practices do not ensure trustworthy data. In the governance of data, the organization should define expected *attributes of data quality*, and the practices and responsibilities for achieving those attributes.

Acceptable Audit Trails

Audit trails are essential in proving reliability of the information and in proving that practices to achieve quality attributes are in place. Therefore, acceptable audit and quality assurance processes should be in place and verifiable. These should be designed to audit and reinforce measures for ensuring the reliability and integrity of information.

Reliability of the Systems

The information systems must be reliable to ensure validity and integrity of the content. Therefore hardware, network infrastructure, software, storage, and other components should be monitored for reliability of performance, and prompt action taken to mitigate identified problems and risks. Formal *change control* processes should be part of maintaining a reliable information environment. These change control processes should require testing of functionality, and validation of data and all appropriate metadata. Given the number of disparate systems, applications, and medical devices in use within and across healthcare delivery organization, and the frequency with which data and information are exchanged, diligence around adherence to interoperability standards is critical to enabling information reliability.

PRINCIPLE OF PROTECTION

An information governance program must ensure the appropriate levels of protection from breach, corruption and loss are provided for information that is private, confidential, secret, classified, essential to business continuity, or otherwise requires protection.

> “Every system, electronic or manual, that generates, collects, stores, transmits, uses, archives, and dispositions data and information must be governed with protection in mind.”

These levels of protection must be applied to information, regardless of medium, from the moment it is created to the moment it reaches or exceeds its retention period and is appropriately dispositioned. Therefore, every system, electronic or manual, that generates, collects, stores, transmits, uses, archives, and dispositions data and information must be governed with protection in mind.

Information generated or managed by an organization requires varying degrees of protection, as mandated by laws, regulations, and/or organizational policies. An organization's governance should also mandate processes to ensure continued operation and continued protection, during and after periods of failure or disruption.

Information protection takes multiple forms. First, each system must enable management of security access controls. Only members of the workforce and other authorized parties with the appropriate levels of access or security clearance may access information relevant to their roles or duties. Reliably protecting electronic and physical assets requires use of tools such as user authentication, key card access restrictions, and other relevant measures. This also requires that as the workforce and other authorized parties transition in status or job function, respective level of access is changed immediately to a level appropriate to the new role and duties.

Second, protection requires preventing information, regardless of medium, from leaking outside the organization, either by physical or electronic means. This includes ensuring that electronic information cannot be inappropriately viewed, e-mailed, downloaded, uploaded, or otherwise proliferated—intentionally or inadvertently, even by individuals with legitimate access to the system. For example, a managed file transfer technology can reduce workforce contact with protected health information (PHI), personally identifiable information (PII) or other protected information, using automated file transfers. It is imperative that appropriate safeguards be clearly defined in organizational policy and that compliance be monitored. Measures to protect information must also include physical security of computing and access devices or any equipment containing private, secret, or confidential information or intellectual property of the organization.

Security, privacy and confidentiality requirements (rules, regulations, policies) should be observed when determining a method for the final disposition of information, regardless of source or media. Whether that disposition is archival, transfer to another organization, preservation for permanent storage, or destruction, appropriate protection must be considered in defining the process. For example, the workforce should:

- Implement reasonable safeguards to limit incidental disclosures of PHI and PII
- Receive training on disposal policies and procedures
- Not abandon or dispose of information, particularly PHI or PII or other private information in containers that are accessible by the public or other unauthorized persons
- Provide validation of disposal method, time, date, and accountable party

Finally, an organization's audit program should have a clear process to validate whether sensitive information is being handled in accordance with the organization's policies and procedures, and should be compliant with applicable laws and business practices.

PRINCIPLE OF COMPLIANCE

An information governance program shall be constructed to comply with applicable laws, regulations, standards, and organizational policies.

It is the duty of every organization to comply with applicable legal and regulatory requirements; those for maintaining and managing health information and those for managing other organizational information. Some healthcare requirements warrant special attention and consideration. For example, laws governing privacy and confidentiality, and fraud and abuse are particularly important to healthcare organizations. An organization's credibility and legal standing rest upon its ability to demonstrate that it conducts its activities in a lawful manner and manages information risks effectively. The absence of information, or poor quality of information required to demonstrate this damages an organization's credibility and may impair its standing in legal matters or jeopardize its ability to conduct business.

The duty of compliance affects systems and processes for information management and governance in two ways:

1. The information management systems and processes should contain information showing the organization's activities are conducted in an ethical and lawful manner.
2. The information management systems themselves are subject to legal and regulatory requirements, such as medical coding standards, security access controls, and transaction audit logs.

It follows from this that every organization should:

- Know what information should be entered into its records to demonstrate its activities are being conducted in a lawful manner.
- Enter that information into its records in a manner consistent with laws and regulations.
- Maintain its information in the manner and for the time prescribed by law or organizational policy.
- Develop internal controls to monitor adherence to rules, regulations, and program requirements, thus assessing and ensuring compliance.

> "An organization's credibility and legal standing rest upon its ability to demonstrate that it conducts its activities in a lawful manner and manages information risks effectively."

Organizations subject to codes of conduct, ethics rules, standards of practice, or other authorities are also subject to a duty to comply with them. To the extent that information management systems are required to demonstrate compliance, the organization's information must be maintained in accordance with these codes, rules, or authorities.

Policies are internal rules of conduct for the organization and the organization's own statement of what it deems as correct conduct. By its nature, a policy imposes a duty of compliance upon the organization and its workforce. To comply with legal and regulatory requirements, an organization should develop, adopt, monitor, and enforce suitable policies.

The precise manner and duties of compliance will vary among different types of healthcare organizations. Some organizations may be subject to multiple laws and regulatory requirements, as well as codes of ethics and accreditation standards. It may, in turn, require the organization to adopt, integrate, and enforce multiple policies for information governance.

Every organization should construct and enforce its policies and conduct its activities in an appropriate manner to ensure compliance with the totality of authorities applicable to it.

PRINCIPLE OF AVAILABILITY

An organization shall maintain information in a manner that ensures *timely, accurate, and efficient* retrieval.

Stakeholder trust in information and in the healthcare operations themselves is impacted by an organization's ability to ensure the timely, accurate, and efficiency of information availability.

A successful and responsible organization must have the ability to identify, locate, and retrieve the information required to support its ongoing activities. This information may be used by:

- The healthcare team, patients, and other caregivers
- Authorized members of the workforce and others authorized consistent with regulations
- Legal and compliance authorities for discovery and regulatory review purposes
- Internal and external reviewers for purposes including but not limited to: payer *audit*, financial audit, case management, and quality assurance.

Having the right information available at the right time for the right individual depends upon an organization's ability to address multiple demands. The organization must search for information in continually expanding volumes of information and multiple systems. For some organizations this includes multiple electronic and manual systems. Transactions are increasingly conducted across disparate electronic systems, both internal and external to the actual or virtual location(s) of the organization, complicating queries and access to data across those systems. Managing both vendor relationships and employee turnover can also challenge organizations to update their workforce and agents on the most current methods to access information.

To ensure critical information availability, organizations must determine levels of redundancy, failover, and contingencies needed based on risk of nonavailability of electronic systems and information.

Metadata

Efficient information availability, effective preservation and disposition, and effective database administration require assigning structural and descriptive characteristics to information. Metadata should be utilized in all applicable systems to facilitate information availability. *Metadata* are the structured information that describe, explain, locate, or otherwise make it easier to retrieve, use, audit, and manage information. Metadata consist of indexing terms and attributes; metadata are data about data. Metadata are typically categorized into groups including but not limited to: administrative, content, descriptive, preservation, and structural. For example, dates of creation, sending, receipt, last access, and last modified are examples of administrative metadata.

Backups, Conversion, Migration

To mitigate the effects of a disaster, system malfunction, or data corruption, information should be backed up routinely. Information created with legacy hardware and software systems should also be reviewed periodically to verify the information can be accessed with current systems. In case of impending system obsolescence, information with organizational value should be migrated to currently supported hardware and/or converted into a readable format.

> "Efficient information availability, effective preservation and disposition, and effective database administration require assigning structural and descriptive characteristics to information. Metadata should be utilized in all applicable systems to facilitate information availability."

> “Having the right information available at the right time for the right individual depends upon an organization’s ability to address multiple demands.”

Routine Disposition

To effectively manage the availability of its information assets at a reasonable cost, an organization should—in the normal course of business—regularly remove obsolete or redundant data and information. This will make the remaining information, which has ongoing value to the organization, more identifiable and accessible, enhance system performance, and reduce the maintenance costs of storage, backup, and migration.

However, removing unneeded information should occur in adherence with the organization’s information retention policies, which should also provide for suspending its disposition in the event of pending or ongoing legal process, audit, or, where appropriate, freedom of information requests.

Well-Designed Storage

An organization’s workforce is more likely to retrieve and use information for better decision making and more effective work if the organization has well-designed storage processes and access to understandable, retrievable, relevant, and consistent information. With properly structured information, personal productivity is improved, storage costs are minimized, and the reliability and speed of retrieval are optimized.

Accessibility through sufficient and readily available access points or devices is applicable to all types of stored information, including, but not limited to, clinical and nonclinical information regardless of storage medium.

Further, complete and accessible records and information in a well-managed environment minimize inconsistent and erroneous interpretation of the facts, simplify legal processes and regulatory investigations, and protect valuable information from being lost, corrupted, or stolen.

P PRINCIPLE OF RETENTION

An organization shall maintain its information for an appropriate time, taking into account its legal, regulatory, fiscal, operational, risk, and historical requirements.

Information documents an organization’s operations and is essential to effectively managing the organization. The ability to properly and consistently retain all relevant information is especially important, as organizations create and store large quantities—most of it in electronic form.

The ability to retrieve and access information should be maintained throughout its retention period. Accessibility through currently and readily available access points or devices is applicable to all types of stored information, including, but not limited to, clinical and nonclinical information regardless of storage medium.

To control information volume, an organization needs an information retention program that defines what information to retain, how long to maintain it and how to dispose of it when it is no longer required. This is based on the concept that information has a *lifecycle*, which begins at its creation and ends at its final disposition.

As part of its retention program, an organization must develop an information *retention schedule*, which specifies what information must be retained and for what length of time. Retention decisions are based on the type of information, and the organization’s legal, regulatory, fiscal, operational, clinical, role/mission, and historical requirements.

- **Legal and Regulatory**—Local, national, and international laws mandate the retention of information for a specified period of time—generally a minimum period—but may include a maximum period as well. To comply with these laws and regulations, an organization should conduct research in consultation with appropriate experts such as legal counsel to determine all retention requirements. Failure to comply may result in costly penalties and loss of legal rights.

- **Fiscal**—Information with financial or tax value should be retained to ensure the timely payment of obligations and the proper receipt of receivables, as well as to support the organization's financial audits and tax returns. Information related to the filing and support of governmental or payer reporting requirements should also be retained. In conjunction with legal counsel, workforce responsible for fiscal compliance should help determine fiscal retention requirements.
- **Operational**—An organization should determine how long information is needed to satisfy its operational needs. This is usually determined by interviewing the individuals most knowledgeable about the operational value of each information type.
- **Clinical**—As applicable, and based on the nature of care and/services services provided and its role, an organization should determine and how long information in the aggregate and by information type should be retained to satisfy clinical needs.
- **Role/Mission**—Based on the organization's role and/or mission in the healthcare industry, retention periods for all or specific types of information may be established outside time periods otherwise required. An example of such need is organizations conducting or participating in research.
- **Historical**—Information that depicts the history of an organization should be preserved and properly archived for the life of that organization. Examples of historical information include articles of incorporation, bylaws, charters, and boards of directors' minutes. Examples of historical clinical information include medical staff bylaws and minutes. Historical information normally constitutes a very small percentage of an organization's total retained information volume.

Information retention schedules should be reviewed periodically and revised regularly. Some internal changes in the organization such as mergers and acquisitions or lines of business changes, or types of records generated, as well as external events such as legal, regulatory, or fiscal changes, may require revisions. If a revision decreases a retention period for a particular records series, then that records series should be destroyed as soon as possible to comply with the revised information retention schedules.

Once the retention requirements listed above are determined, an organization should conduct a risk assessment to determine the appropriate retention period for each type of information. Retention decision makers should be aware the presence or absence of information can be either helpful or harmful to the organization. Therefore, to minimize risks and costs associated with retention, it is essential to immediately dispose of information after the retention period expires, in accordance with the organization's retention policy.

> “To control information volume, an organization needs an information retention program that defines what information to retain, how long to maintain it and how to dispose of it when it is no longer required. This is based on the concept that information has a *lifecycle*, which begins at its creation and ends at its final disposition.”

PRINCIPLE OF DISPOSITION

An organization shall provide secure and appropriate disposition for information no longer required to be maintained by applicable laws and the organization's policies.

At the completion of its retention period, an organization's information must be designated for disposition. This applies not only to patient health records and data, but many other types of information such as meeting minutes, credentialing files, agreements, financial records, human resource information, and privileged information such as that related to quality assurance.

Disposition includes not only destruction, but also any permanent change in custodianship of the information, such as when it is transferred to another party due to a merger or acquisition of another hospital, clinic, or physician practice or when a organization discontinues a practice, service, or other business.

In many cases, the appropriate disposition is the destruction of information, in which case the organization should ensure the information is transported and destroyed in a secure and environmentally responsible manner. The organization should document or certify that the information has been destroyed completely and irreversibly when required.

In some cases, healthcare organizations discontinuing their business may choose to transfer records of care to the patients or clients to whom they pertain. All such transfers are considered permanent disposition actions and should be documented.

If records and information are converted or migrated to new media, disposition of the previous media may also be warranted. In all instances, the organization should make a reasonable effort to ensure all versions and copies of the information are accounted for in the disposition. The organization should also document its disposition process.

"Disposition includes not only destruction, but also any permanent change in custodianship of the information, such as when it is transferred to another party due to a merger or acquisition of another hospital, clinic, or physician practice or when a organization discontinues a practice, service, or other business."

A duty to suspend disposition may arise in the event of pending or reasonably anticipated litigation or a regulatory action. The organization should designate information in consultation with counsel both as to scope and time to be held pending resolution of the litigation or audit and notify the affected workforce when a hold is issued as well as when the hold is released, so that the disposition process may be resumed.

IGPHC™ GLOSSARY OF SELECTED TERMS

The following terms appear in the IGPHC™ or are closely related to such terms. This set of definitions is not intended to be an exhaustive set of IG related terms and should be used in conjunction with relevant glossaries including AHIMA's Pocket Glossary of Health Information Management and Technology.

Definition sources are referenced as follows:

AHIMA—Pocket Glossary of Health Information Management and Technology

ARMA—Glossary of Records and Information Management Terms

M-W—Merriam-Webster Online Dictionary and Thesaurus

Task Force—definition developed by AHIMA IG Task Force

Accessibility: easily obtainable and legal to access with strong protections and controls built into the process (AHIMA)

Accountable Member of Senior Leadership: (examples include) CEO, C-Suite, President, Agency Director, Practice Partner, Administrator, Executive Director, Owner/Operator—(Task Force)

Accuracy: the extent to which the data are free of identifiable errors (AHIMA)

Audit, Auditing: the review of information-related activities to ensure that sufficient policies, procedures, and controls are in place and complied with to meet all operational, legal, and regulatory obligations and to identify where and how improvements should be made (ARMA)

Audit Trail: a record that allows a sequence of activities to be reconstructed, reviewed, and examined. (M-W). 1. A chronological set of computerized records that provides evidence of information system activity (log-ins, log-outs, file accesses) used to determine security violations. 2. A record that shows who has accessed a computer system, when it was accessed, and what operations were performed (AHIMA)

Authentic, Authenticity: the genuineness of a record, that it is what it purports to be; information is authentic if proven to be immune from tampering and corruption (AHIMA)

Availability: extent to which information is available, whenever and wherever it is needed (AHIMA). Definitions contextual to the Availability Principle: **(1)Timely:** (context of Availability) having the requested information available for the requestor before that requestor needs to make a decision for the next step in their workflow without an unreasonable wait (Task Force) **(2) Accurate:** verifying that the information retrieved matches the request for the correct item or person at the correct level of detail (Task Force) **(3) Efficient:** the sum of the organization's decisions to balance three competing imperatives: accuracy of the information retrieved, verifying that the requestor has rights to the information, and the speed in which the information is delivered to the requestor (Task Force)

Change Control: expected standard practice to ensure that changes software, hardware, firmware, or other components to technical infrastructure are introduced in a predefined, controlled manner. The practice should include testing of applicable aspects, including the impact or data and metadata integrity. Effective change control practices will minimize disruption and the need to fall-back on planned changes (Task Force)

Complete, Completeness: an element of a legally defensible health record. A (health, medical) record is not complete until all its parts are assembled and appropriate documents are authenticated according to medical staff bylaws. (AHIMA) Records and information comply with internal or external defined requirements for comprehensiveness, including clinical, business, and other operational needs (Task Force)

Data: basic facts and observations about people, processes, measurements, and conditions (e.g. dates, numbers, images, symbols, letters) (AHIMA)

Data Governance: the overall management of the availability, usability, integrity, and security of the data employed in an organization or enterprise (AHIMA)

Data Quality Attributes, Characteristics: accessibility, accuracy, comprehensiveness, consistency, currency, definition, granularity, precision, relevancy, timeliness. AHIMA includes Data Quality Characteristics in its "Data Quality Management Model (Updated)" available through the AHIMA Body of Knowledge (BOK). Data quality attributes includes but are not limited to:

- **Data Accuracy:** The extent to which the data are free of identifiable errors
- **Data Accessibility:** Data items that are easily obtainable and legal to access with strong protections and controls built into the process
- **Data Comprehensiveness:** All required data items are included—ensures that the entire scope of the data is collected with intentional limitations documented
- **Data Consistency:** The extent to which the healthcare data are reliable and the same across applications
- **Data Currency:** The extent to which data are up-to-date; a datum value is up-to-date if it is current for a specific point in time, and it is outdated if it was current at a preceding time but incorrect at a later time
- **Data Definition:** The specific meaning of a healthcare-related data element
- **Data Granularity:** The level of detail at which the attributes and values of healthcare data are defined
- **Data Precision:** Data values should be strictly stated to support the purpose
- **Data Relevancy:** The extent to which healthcare-related data are useful for the purposes for which they were collected
- **Data Timeliness:** Concept of data quality that involves whether the data are up-to-date and available within the expected time frame; timeliness is determined by manner and context in which the data are being used (AHIMA)

Ecosystem: everything that exists in a particular environment (M-W)

Healthcare Ecosystem: used in AHIMA's IGPHC ™ to reference the community of organizations, both healthcare provider and nonprovider, of all types, sizes, and settings, that are information intensive. Also referred to as in the IGPHC™ as healthcare industry and healthcare community (Task Force)

IGHPC™: the Information Governance Principles for Healthcare™. A set of governance principles adapted for use in provider and nonprovider organizations in the healthcare industry from ARMA International's Generally Accepted Recordkeeping Principles®. The IGPHC™ developed with multi-stakeholder and multi-discipline representation are the cornerstone of the AHIMA promulgated framework for the adoption and practice of information governance in healthcare. (Task Force)

Information Governance—AHIMA: an organization-wide framework for managing information throughout its lifecycle and supporting the organization's strategy, operations, regulatory, legal, risk, and environmental requirements

Information Governance—ARMA: a strategic framework composed of standards, processes, roles, and metrics that hold organizations and individuals accountable to create, organize, secure, maintain, use and dispose of information in ways that align with and contribute to the organization's goals

Information Governance—Gartner: the specification of decision rights and an accountability framework to ensure appropriate behavior in the valuation, creation, storage, use, archiving, and deletion of information

Information: data that have been collected, combined, analyzed, and/or interpreted to be used for a specific purpose or set of purposes. Data represent facts; information represents meaning (AHIMA)

Information Assets: information that has value for the organization. (AHIMA) The recognition that information must be recognized as a strategic asset by the organization is central to information governance principles (Task Force)

Information Lifecycle: the cycle of gathering, recording, processing, storing, sharing, transmitting, retrieving, and disposing of information (AHIMA)

Information Management: the generation, collection, organization, validation, analysis, storage, and integration of data as well as the dissemination, communication, presentation, utilization, transmission, and safeguarding of the information (AHIMA)

Interoperability: the ability of different systems to use and exchange information through a shared format (ARMA)

Integrity: 1. the state of being whole or unimpaired. 2. the ability of data to maintain its structure and attributes, including protection against modification or corruption during transmission, storage, or at rest. Maintenance of data integrity is a key aspect of data quality management and security. (AHIMA) *Integrity* of information is directly related to the organization's ability to prove that information is *authentic, timely, accurate, and complete*. (Task Force)

Metadata: descriptive data that characterize other data to create a clearer understanding of meaning, and to achieve greater reliability and quality of information. Metadata consist of indexing terms and attributes. Data about data. For example, dates of creation, sending, receipt, last access, last modified. (AHIMA). The structured information that describe, explain, locate, or otherwise make it easier to retrieve, use, or manage information resources. **Note:** Metadata are typically broken into broad types that include but are not limited to: administrative, content, descriptive, preservation, and structural. (ARMA)

Program: a plan of action to achieve a specified end (M-W)

Provider (of healthcare): physician, clinic, hospital, nursing home, or other healthcare entity that delivers healthcare services (AHIMA). Nonprovider: in context of the IGPHC™, means organizations within and service provider organizations or consumers that do not provide direct medical or health-care services (Task Force)

Record: any recorded information, regardless of medium or characteristics, made or received and retained by an organization in pursuance of legal obligations or in the transaction of business (ARMA)

- **Health Record:** information related to the physical or mental health or condition of an individual as made by or on behalf of a health professional in connection with the care ascribed that individual (AHIMA)
- **Legal Health Record:** documents and data elements that a healthcare provider may include in response to legally permissible requests for patient information (AHIMA)
- **Business Record:** a record that is made and kept in the usual course of business, at or near the time of the event recorded (AHIMA)

Reliability: (of information) information is managed in the usual and ordinary course of business, and in a manner which ensures integrity and compliance with accepted industry standards for quality (Task Force)

Retention: Mechanisms for storing records, providing for timely retrieval, and establishing the lengths of time that various records (and/or) information (sets) will be retained by the healthcare organization (AHIMA)

Retention Schedule: a time line for various records/information retention based on factors such as laws, statutes of limitation, age of patient, competency of patient, standards, AHIMA recommendations, operational needs, and role and mission of the organization (AHIMA, Taskforce)

Timely, Timeliness: the time between an event and the availability of data and/or information about the event. The completion of a business or health record within timelines established by external or internal requirements, medical and/or professional staff bylaws, or organization policy (Task Force)

Transparency: transparency of use of health information: open and transparent definition of uses and sharing of identified and de-identified, individual, or aggregate healthcare information (Task Force)

Workforce: human resources, employed, contracted, and where applicable, nonemployed members of medical and professional staff granted practice privileges. All members of the workforce of the healthcare organization are accountable for their responsible and ethical handling of information (Task Force)

Bibliography

American Health Information Management Association. *Pocket Glossary of Health Information Management and Technology*, 4th Edition. Chicago, IL AHIMA Press, 2014.

ARMA International. *Glossary of Records and Information Management Terms*, 4th Edition. Overland Park, KS. ARMA International. 2012

ARMA International. "Generally Accepted Recordkeeping Principles®." 2013 Overland Park, KS ARMA International. 2013

M-W–Merriam-Webster On-Line Dictionary and Thesaurus http://www.merriam-webster.com/ (terms searched 2014)

Suggested Reading:

Cohasset Associates and AHIMA. "A Call to Adopt Information Governance Practices." 2014 *Information Governance in Healthcare*. Minneapolis, MN. Cohasset Associates, 2014.

The Joint Commission. "Information Management (IM) Chapter", *Comprehensive Accreditation Manual for Hospitals*, 2014, Oakbrook Terrace, IL: The Joint Commission, 2014, pp.IM-1–IM-10.

The Information Governance Initiative. "The Information Governance Initiative Annual Report." 2014. New York, NY. www.IGinitiative.com

The Sedona Conference. "Commentary on Information Governance" The Sedona Conference® Working Group Series. A project of The Sedona Conference® Working Group on Electronic Document Retention and Production (WGI)

ACKNOWLEDGEMENTS

AHIMA acknowledges the following individuals and organizations for their valued contributions to the AHIMA Information Governance Principles for Healthcare (IGPHC)™.

Information Governance Taskforce

Deborah Bass, Chief Executive Director, Nebraska Health Information Exchange, AHIMA Practice Council Member on HIEs

Brent Bigelow, CISSP, Senior Security Architect, Cardinal Health

Galina Datskovsky, PhD, IGP-CRM, CRM, Consultant and Facilitator, CEO Covertix North America, VP Information Governance, HP Autonomy, Past President ARMA International

Sofia Empel, PhD, MLIS, **CRM, CDIA+**—InfoCentric Strategies

Deborah K. Green, MBA, RHIA, AHIMA. Executive Vice President and Chief Operating Officer, AHIMA EVP/COO, AHIMA National Visionary Award, 2000

Anupam Goel, MD, MBA, VP Clinical Information Advocate (ACO) UCSD, Beacon Communities, Malcolm Baldridge Examiner, Boarded in Informatics

Lee Hamilton, JD, MBA, RN, CPHQ, FNAHQ, PCMH CCE, International Executive and Consultant in Health Leadership, Policy and Quality/Risk. Past President of NAHQ

Melissa Martin, RHIA, CCS, CHTS-IM, Chief Privacy Officer and HIM Director at West Virginia University Hospitals, AHIMA Board, Third Year Director. Past President and Distinguished Member of WVHIMA

Gretchen Tegethoff, MS, CHCIO, CPHIMS, FHIMSS, FCHIME, CIO and CHIME Representative, CIO George Washington University, Athens Regional Health System

Mary G. Reeves, RHIA, Past AHIMA Chair EHRs Practice Council, Past Director AHIMA Board, AVP HIM Ops and CDI Regional HealthCare Partners. Former Admin HIM Director Vanderbilt

Lydia M. Washington, MPH, RHIA, CPHIMS, AHIMA Senior Director HIMPE, Former HIM Director MD Anderson

Sandra Wolfskill, CPA, FHFMA, HFMA, Director Revenue Cycle MAP

IG Expert Advisory Group

Bennett Borden, JD, Partner Commercial Litigation Practice Group-Co Chair IG and eDiscovery Group at Drinker Biddle and Reath, Sedona Conference, ARMA, Co-Founder IG Initiative, globally recognized authority on the legal, technology, and policy implications of digital information

Dee Cantrell, MS, RN, BSN, CP, Chief Information Officer, Emory Healthcare Associate Director for Enterprise Clinical Informatics for Emory's Center for Clinical Informatics and the Deputy CIO for the Office of Information Technology for Emory University

Todd Cooper, EVP, Center for Medical Interoperability, Principle Breakthrough Technologies Foundry, Chairman US Technical Advisory Group to ISO TC 215, Head of US Delegation ISO TC 215-Informatics, Board IHE, Co-Chair HL7 Medical Device, Chair IEEE

Ron Hale, PhD, CISM, Acting CEO and Chief Knowledge Officer for ISACA, Former Practice Director Enterprise Risk Management Division, Deloitte & Touche

Ronald J. Hedges, JD, Former US Magistrate Judge, Adjunct Professor Georgetown Law, eDiscovery Expert, Author, Sedona Conference, ARMA

Pamela Lane, MS, RHIA, CPHIMS, CA. DHHS, Deputy Section Health Information, Director Office of Health Information Integrity, Consulting and Hospital Ops Experience, US Navy Veteran

John Mache, **MS**, Chief Information Officer and Enterprise Security Officer, The Joint Commission

Fred Pulzello, MBA, CRM, IGP, President ARMA International

Don Rosen, MS, Director Policy and Enforcement, Officer of the Chief Records Officer, National Archives and Records Administration (NARA)

Sunil Sinha, MD, MBA, FACHE, FACP, Boarded: ABIM, ACPE, ABQUAR, Senior Malcolm Baldridge Examiner, Juror NQF National Quality Award, Johns Hopkins, Former Sr. Medical Officer CMS, Pfizer, Jencare Market Medical Director—Virginia

Rita Vann, RN, SVP Clinical Services Brookdale Senior Living, Long Term Care Nurse Executive Council

Charlotte Weaver, PhD, RN, Chief Clinical Officer and SVP Clinical Services Gentiva, VP & ED Nursing Research-Cerner, AMIA-Nursing Informatics Pioneer

Paul Wester, MA, MLS, Chief Records Officer, US Government National Archives and Records Administration (NARA)

AHIMA-Appointed IG Review Group

Kimberly A. Baldwin-Stried Reich, MBA, MJ, RHIA, PBCI, CPHQ, FAHIMA

Ellen Berkowitz, RHIT, CHDA, CPHQ

Patty Buttner, RHIA, CCS

Jill S. Clark, MBA, RHIA, CHDA, FAHIMA

Angie Comfort, RHIA, CDIP, CCS

Julie A. Dooling, RHIA, CHDA

Elizabeth A. Dunagan, RHIA

Melanie Endicott, MBA/HCM, RHIA, CDIP, CCS, CCS-P, FAHIMA

Louis Galterio, MBA, CHIME, CP, FHIMSS

Barb Glondys, RHIA

Pamela Heller, RHIA, CCS-P

Sandra A. Huyck, RHIT, CCS-P, CPC/H

Beth H. Just, MBA, RHIA, FAHIMA

Lesley R. Kadlec, MA, RHIA

Elisa Stamm Kogan, MS, MHA, CDIP, CCS-P

Susan Lucci, RHIA, CHPS, CHDS, AHDI-F

Katherine G. Lusk, MHSM, RHIA

Ann M. Meehan, RHIA

Deborah L. Neville, RHIA, CCS-P, PCS

Alice Noblin, PhD, RHIA, CCS

Brenda S. Olson, MEd, RHIA, CHP

Anna Orlova, PhD

Erik Pupo, MBA, CPHIMS, FHIMSS

Harry Rhodes, MBA, RHIA, CHPS, CDIP, CPHIMS, FAHIMA

Lisa A. Roat, RHIT, CCS, CCDS

Angela Rose, MHA, RHIA, CHPS, FAHIMA

Sharon K. Slivochka, RHIA

Patrice L. Spath, MA, RHIT, CHTS-IM

Diana Warner, MS, RHIA, CHPS, FAHIMA

Susan White, PhD, RHIA, CHDA

Lou Ann Wiedemann, MS, RHIA, CDIP, CHDA, CPEHR, FAHIMA

AHIMA Board of Directors 2014

Angela Kennedy, EdD, MBA, RHIA, President/Chair

Ann Chenoweth, MBA, RHIA

Cassi Birnbaum, MS, RHIA, CPHQ, FAHIMA, President/Chair-elect

Cindy Zak, MS, RHIA, PMP, FAHIMA

Colleen A. Goethals, MS, RHIA, FAHIMA

Dana C. McWay, JD, RHIA, Secretary

David Muntz, CHCIO, FCHIME, LCHIME, FHIMSS, Advisor

Dwayne M. Lewis, RHIT, CCS

Jennifer McManis, RHIT, Speaker of the House

Melissa M. Martin, RHIA, CCS, CHTS-IM, Treasurer

Lynne Thomas Gordon, MBA, RHIA, CAE, FACHE, FAHIMA, Chief Executive Officer

Virginia E. Evans, MBA, RHIA, FAHIMA

Susan J. Carey, RHIT, PMP

Zinethia L. Clemmons, MBA, MHA, RHIA, PMP

American Health Information Management Association
233 N. Michigan Ave., 21st Floor | Chicago, IL 60601
ahima.org | (800) 335-5535

AHIMA
American Health Information
Management Association®