Commonwealth of Virginia

Enterprise Technical Architecture (ETA)

Commonwealth of Virginia - Health Information Exchange (COV-HIE)

COV-HIE Topic Report
Information Domain

Virginia Information Technologies Agency (VITA)

Prepared by:
Information Technology Standards Advisory Committee

Health Information Technology Standards Advisory Committee (HITSAC)

Committee Members

Mr. Daniel Barchi, Senior Vice President and Chief Information Officer of Carilion Clinic (resigned 9/17/2010)
Mr. Geoff Brown, Senior Vice President and Chief Information Officer of Inova Health System
Dr. Alistair Erskine, Chief Medical Information Officer of VCU Health System (resigned 11/2/2010)
Mr. John Quinn, Chief Technology Officer of HL7, Inc.
Dr. Marshall Ruffin, Chief Technology and Health Information Officer UVA Health System

Virginia Information Technologies Agency (VITA) Support Staff for HITSAC

Nadine Hoffman, Data Manager (resigned 09/16/2010)
Susan McCleary, Lead Business Analyst

Reviews

- The Enterprise ~~Applications and Policy, Practice and~~ Architecture Division~~s~~ within the Virginia Information Technologies Agency (VITA) reviewed the COV-HIE Topic Report.
- Participation of all Executive Branch agencies was encouraged through a review and comment period via VITA's Online Review and Comment Application (ORCA).

This following table contains a history of revisions to this publication.

COV-HIE Architecture Report: Version History		
Version	**Date**	**Revision Description**
1.0	04-04-2011	Initial Document – includes revisions related to the submission of Commonwealth of Virginia's Health Information Exchange (COV-HIE) strategic and operational plan to the federal government on July 30, 2010.
1.1	*07-28-2016*	*Update necessitated by changes in the Code of Virginia and organizational changes in VITA. No substantive changes were made to this report.*

Table of Contents

Executive Summary

The Commonwealth of Virginia, led by the Health IT Advisory Commission (HITAC) and under the technical infrastructure guidance of the Health IT Standards Advisory Committee (HITSAC), developed a strategic and operational plan to implement a state wide health information exchange (HIE). The audience for this report includes business and technical leaders in state and local agencies that will connect to the National Health Information Network (NHIN) through the state HIE. HITAC submitted the COV-HIE strategic and operational plans to the Office of the National Coordinator for Health Information Technology (ONC) on July 30, 2010 for review and approval.

The standards presented in this report are the first set of technical infrastructure domain requirements for the Commonwealth of Virginia Health Information Exchange (COV-HIE). The COV-HIE is a network and a service, and ―exchange‖ within its name is both a noun and a verb. As a noun, it is a digital network allowing providers to exchange electronically and with semantic interoperability health care data about patients they share. As a verb, it is a collection of services that reliably communicate clinical data between providers by identifying patients and locating their digital medical records across various electronic medical record systems. The government of the Commonwealth of Virginia may choose to use the COV-HIE for other electronic communication among agencies and between agencies and citizens, to be determined.

The initial requirements are organized into four sub-topic areas:

- Interoperability
- Technical Infrastructure
- Data
- Privacy and Security

State agencies, within the Executive Branch, shall comply with these requirements in developing or connecting to the COV-HIE. The governance model for the COV-HIE will address broader compliance within the state.

In addition to defining requirements for the technical infrastructure domain, the HITAC working in conjunction with the Office of Health IT, within the Virginia Department of Health (VDH), defined requirements for the other four COV-HIE domains – governance, finance, business and technical operations, and legal/policy.

Background

The COV - HIE Topic Report is a subset of the Enterprise Technical Architecture (ETA) Information Domain Report. The ETA Information Domain describes technical topics such as business intelligence, reporting, data management, and knowledge management. The COV-HIE topic is a new addition to the domain report.

As a topic of the ETA Information Domain, this report expands on the principles, requirements and recommended practices presented in the ETA Information Domain report. Requirements and technology product standards introduced in this topic report will be incorporated into the COV Information Technology Resource Management (ITRM) Enterprise Architecture Standard.

Health Information Technology Standards Advisory Committee (HITSAC)

HITSAC was created by the Information Technology Investment Board (ITIB) on July 1, 2009. Five health information technology experts were selected to form the advisory committee. Dr. Marshall Ruffin, Chief Technology and Health Information Officer, University of Virginia Health System, was the chairman of the committee. The committee members were as follows: Mr. Daniel Barchi, Mr. Geoff Brown, Dr. Alistair Erskine and Mr. John Quinn.

During the 2010 legislative session, the ITIB was dissolved and replaced by the Information Technology Advisory Council (ITAC). On November 1, 2010, the ITAC appointed the following members to HITSAC: Mr. Geoff Brown, Dr. Alistair Erskine, Mr. John Quinn and Dr. Marshall Ruffin. Since this appointment, Dr. Alistair Erskine has resigned.

All HITSAC meetings are public. Materials can be found at: http://www.vita.virginia.gov/ITIB/default.aspx?id=9706.

The HITSAC Charter is as follows:

HITSAC will advise the Information Technology Advisory Council (ITAC) on the approval of nationally recognized technical and data standards for health information technology systems or software pursuant to subdivision 7 of § 2.2-2699 in the Code of Virginia.

HITSAC Guiding Principles

1. Define a utility and identify steps to create a Health Information Exchange
2. Focus on data requirements for both patient health purposes and public health purposes (research)
3. Ensure patient centric data are available within the Commonwealth
4. Recognize standards, like Electronic Medical Records (EMR) and Electronic Health Records (EHR) are a utility of health IT; not a competitive advantage
5. Focus on interoperability as a critical success factor
6. Be congruent with the guidance of the Federal ONC and achieve semantic interoperability with its work
7. Adopt national standards where they exist. In the absence of a national standard, adopt other standards to meet the Commonwealth's needs
8. Ensure standards have been validated prior to adoption

Health Information Technology Advisory Commission (HITAC)

In October 2009, Governor Kaine issued Executive Order 95 and established the Governor's Health Information Technology Advisory Commission (HITAC). In 2010, Governor McDonnell approved the continuation of the Executive Order. The Commission shall have the following responsibilities:

- Encourage public-private partnerships to increase adoption of electronic medical records for physicians in the Commonwealth
- Provide healthcare stakeholder input to build trust in and support for a statewide approach to HIE
- Ensure that an effective model for HIE governance and accountability is in place
- Examine and define an integrated approach with the Department of Medical Assistance Services and the Virginia Department of Health to enable information exchange and support monitoring of provider participation in HIE as required to qualify for Medicaid meaningful use incentives
- Develop and/or update privacy and security requirements for HIE within and across state borders
- Encourage and integrate the proliferation of telemedicine activities to support the Virginia healthcare improvement goals
- Monitor and support the activities of any Regional Extension Centers awarded in the Commonwealth
- Examine other health related issues as appropriate

The Secretary of Health and Human Resources will chair the Commission and will be responsible for convening the Commission. The Commission shall consist of members appointed by the chair in consultation with the Secretary of Technology and representing broad stakeholder engagement in health information technology and exchange. Four members of HITSAC were appointed as members of the Commission.

Office of Health IT

Executive Order 95 (2009) also directed the Virginia Department of Health (VDH) to serve as the Commonwealth's Health Information Technology Lead through an Office of Health IT. The Office consists of a director appointed by the Secretary of Health and Human Resources, in consultation with the Commissioner of Health and additional professionals as the Secretary shall determine.

The director shall have the following responsibilities:

- Serve as the Commonwealth's Health IT Lead to fulfill the responsibilities outlined in the American Recovery and Reinvestment Act of 2009 (ARRA)
- Support the work of the Governor's Health Information Technology Advisory Commission
- Facilitate collaboration between the Commission and all appropriate stakeholders
- Ensure broadband and telemedicine initiatives are integrated into the Commission's planning and implementation process
- Ensure VDH Health IT projects including the Advanced Directive Registry, the Immunization Registry, as well as any future Electronic Medical Record initiatives are appropriately aligned with the Commission's planning and aligned with ARRA-funded projects

Health Information Exchange – Federal Funding Opportunity Announcement

In October 2009, the Commonwealth of Virginia, through the Office of Health IT, responded to a federal funding opportunity announcement (FOA) to develop a strategic and operational plan for a state health information exchange (HIE).

> **An HIE is the electronic movement of health-related information among organizations according to nationally recognized standards.**

The HIE FOA is officially referred to as: American Recovery and Reinvestment Act of 2009, Title XIII - Health Information Technology, Subtitle B —Incentives for the Use of Health Information Technology, Section 3013, State Grants to Promote Health Information Technology, State Health Information Exchange Cooperative, Agreement Program, Funding Opportunity Announcement, Office of the National Coordinator for Health Information Technology Department of Health and Human Services 2009. The Virginia submission to the FOA can be viewed at the Health Information Technology Spotlight website - http://www.hits.virginia.gov/.

The FOA describes five domains required for the development of a state HIE:

1. Governance
2. Finance
3. Business and Technical Operations
4. Technical Infrastructure
5. Legal/Policy

This report is focused on the requirements for the Technical Infrastructure.

Key Accomplishments for the COV-HIE

According to the HIE FOA, the Technical Infrastructure domain should accomplish the following:

- Develop or facilitate the creation of a statewide technical infrastructure that supports statewide HIE. While states may prioritize among these HIE services according to its needs, HIE services to be developed include:

  - Electronic eligibility and claims transactions
  - Electronic prescribing and refill requests
  - Electronic clinical laboratory ordering and results delivery
  - Electronic public health reporting (i.e., immunizations, notifiable laboratory results)
  - Quality reporting
  - Prescription fill status and/or medication fill history
  - Clinical summary exchange for care coordination and patient engagement

  (HITSAC notes, that as of November 2009, laboratory ordering is not currently a Health Information Technology Standards Panel (HITSP) defined Capability and should remain an independent solution for Virginia; however HITSP has addressed laboratory results delivery through Capability 126 and 127.)

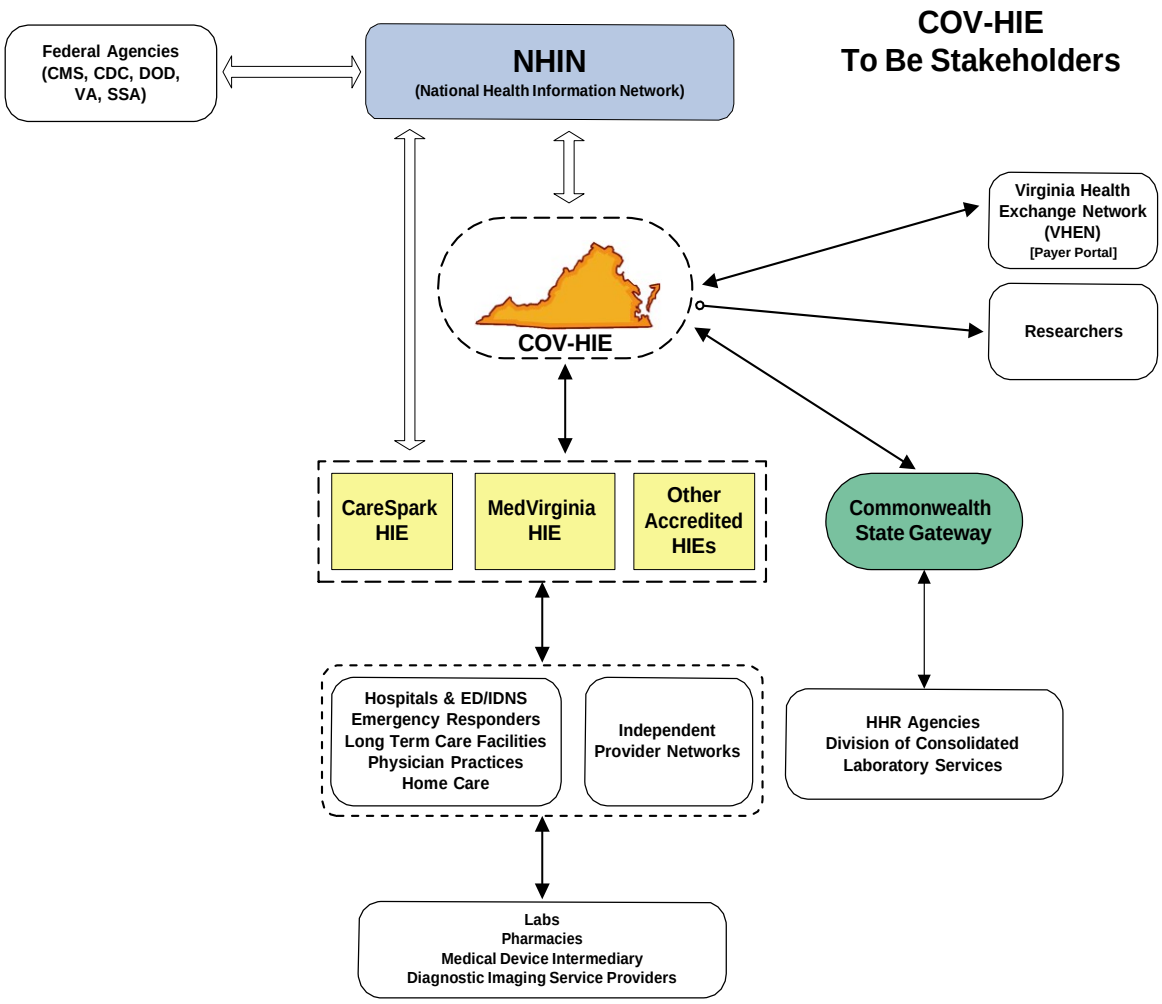
- Leverage existing regional and state level efforts and resources that can advance HIE, such as master patient indexes, health information organizations (HIOs), and the Medicaid Management Information System (MMIS)
- Develop or facilitate the creation and use of shared directories and technical services, as applicable for the state's approach for statewide HIE. Directories may include but are not limited to: Providers (e.g., with practice location(s), specialties, health plan participation, disciplinary actions, etc), Laboratory Service Providers, Radiology Service Providers, Health 13 Plans (e.g., with contact and claim submission information, required laboratory or diagnostic imaging service providers, etc.). Shared Services may include but are not limited to: Patient Matching, Provider Authentication, Consent Management, Secure Routing, Advance Directives and Messaging
- Technical Infrastructure

    - Standards and Certifications – Describe efforts to become consistent with Health and Human Services (HHS) adopted interoperability standards and any certification requirements, for projects
    - Technical Architecture – Requirements to ensure statewide availability of HIE among health care providers, public health and those offering service for patient engagement and data access.
    - Protection of health data – This needs to reflect the business and clinical requirements determined via the multi-stakeholder planning process. Specify how the architecture will align with National Health Information Network (NHIN) core services and specifications
    - Technology Deployment – Develop HIE capacity, enable meaningful use, indicate efforts for nationwide health information exchange. If a state plans to participate in the NHIN, their plans must specify how they will be complaint with HHS adopted standards and implementation specifications. Information on meaningful use can be viewed at (http://healthit.hhs.gov/meaningfuluse)

    During March 2010 – July 2010, the Technical Infrastructure Committee of the HITAC defined the technical infrastructure sections of the COV-HIE strategic and operational plan. The plans can be found here http://www.healthitcouncil.vi.virginia.gov/.

COV-HIE Stakeholders

The following groups have been identified as stakeholders for the COV-HIE:



Definition of Key Terms

All of the COV-HIE architecture requirements, considered to be critical components for implementing the Commonwealth's HIE, are included in this report.

Future versions of this report will include architecture guidance for agencies connecting to the COV-HIE and subsequently the NHIN.

Definitions

Requirements – mandatory enterprise architecture directions and activities that are considered strategic components of the Commonwealth's Enterprise Architecture. They are acceptable activities for current deployments and must be implemented and used for all future deployments.

Glossary

As appropriate, terms and definitions used in this document can be found in the COV ITRM IT Glossary. The COV ITRM IT Glossary may be referenced on the ITRM Policies, Standards and Guidelines web page at http://www.vita.virginia.gov/library/default.aspx?id=537.

Additional HIE specific terms are defined within the Glossary of HIE Terms section of this document.

Agency Exception Requests

Agencies that want to deviate from the requirements related to the COV-HIE Information Domain Topic or those requirements contained in the COV ITRM Enterprise Architecture Standard may request an exception using the *Enterprise Architecture Change/Exception Request Form* found here http://www.healthitcouncil.vi.virginia.gov/.

All exceptions must be approved prior to the agency pursuing procurements, deployments, or development activities related to technologies that are not compliant with the COV ITRM Enterprise Architecture Standard. The instructions for completing and submitting an exception request are contained in the current version of *COV ITRM Enterprise Architecture Policy.* HITSAC will advise the Chief Enterprise Architect and CIO on exception requests.

COV-HIE Architecture Scope

The mission of HITSAC is to define the health information technology data and technology standards for the Commonwealth. As part of this mission, HITSAC will define the technical infrastructure for the COV-HIE. This report presents HITSAC's initial architectural requirements for the COV-HIE.

State agencies, within the Executive Branch, shall comply with the requirements in connecting to the COV-HIE.

This architecture report will be revised, reviewed and reissued for ~~Secretary of Technology~~ *Chief Information Officer* approval as needed.

The current requirements are organized into four sub-topic areas:

1. Interoperability
2. Technical Infrastructure
3. Data
4. Privacy and Security

The audience for this report includes business and technical leaders in state and local agencies that will connect to the NHIN through the COV-HIE.

COV-HIE Requirements

For purposes of this document the term **Provider** is consistent with the HIPAA definition and refers to any person or organization that furnishes, bills or is paid for health care in the normal course of business.

COV-HIE Architecture - Interoperability Sub-Topic

Interoperability is defined by ONC as the ability of health information systems to work together within and across organizational boundaries in order to advance the effective delivery of health care for individuals and communities. The requirements for interoperability are as follows:

HIE-R-01: The COV-HIE shall be congruent with the standards established by the Office of the National Coordinator (ONC) and be routinely certified by ONC.

Rationale:

Interoperability across the Commonwealth and across the nation will not be achieved if there is not alignment to a standard set of Capabilities, Interoperability Specifications and Components.

HIE-R-02: The COV-HIE shall implement the HITSP Interoperability Specifications and Capabilities. The COV-HIE shall support the ONC interoperability and data exchange functions of —meaningful use‖ of Electronic Health Records (EHR).

Rationale:

ONC is the federal standards panel which assembles the standards for use by public and private organizations. Maintaining congruency with ONC is critical to achieving interoperability.

HIE-R-03: All HIEs within the Commonwealth that exchange data in electronic form with state agencies shall comply with the HITSP Interoperability Specifications and Capabilities.

Rationale:

The independent HIEs across the Commonwealth must be compliant with ONC's standards as well to achieve interoperability with Virginia providers and providers across the nation.

HIE-R-04: The COV-HIE shall support electronic eligibility and claims transactions: adherence to HITSP Capability 140 (communicate benefits and eligibility) and HIPAA standards.

HIE-R-05: The COV-HIE shall support electronic prescribing and refill requests: utilize an established eprescribing vendor to adhere to HITSP Capabilities 117 and 118 (prescription).

HIE-R-06: The COV-HIE shall support prescription fill status and/or medication fill history: adherence to HITSP Capabilities 117 and 118.

HIE-R-07: The COV-HIE shall support clinical summary exchange for care coordination and patient engagement: adherence to HITSP Capabilities 119 and 120 as the basis for interoperability of patient documentation (structured and unstructured).

HIE-R-08: The COV-HIE shall support quality reporting: adherence to HITSP Capability 130.

HIE-R-09: The COV-HIE shall support electronic public health reporting: adherence to Interoperability Specification 11.

HIE-R-10: The COV-HIE shall support electronic clinical laboratory ordering and results delivery: adherence to HITSP Capabilities 126 and 127.

HIE-R-11: The COV-HIE shall adopt the HITSP Capabilities for patient identification when issued.

Rationale:

By adhering to the capabilities listed in requirement HIE-R-05 through HIE-R-11, the COV-HIE will achieve the current definition of —meaningful usell.

Information on HITSP Capabilities is provided in Appendix B. A mapping of HITSP Capabilities to Interoperability Specifications is provided in Appendix C.

COV-HIE Architecture – Technical Infrastructure Sub-Topic

The requirements for technical infrastructure are as follows:

HIE-R-12: The COV-HIE shall support the data exchange functions for achieving meaningful use of certified Electronic Health Records (EHR) technologies.

HIE-R-13: The COV-HIE shall support the connectivity requirements of the National Health Information Network (NHIN) and provide connectivity to the NHIN for providers and HIEs in the Commonwealth of Virginia.

HIE-R-14: The COV-HIE shall provide a connection to the NHIN.

HIE-R-15: The COV-HIE shall provide Security Services, Patient Locator Services, Data/Document Locator Services, and Terminology Services as defined by HITSP Interoperability documents.

HIE-R-16: Providers of health care services shall maintain the patient clinical data for the COV-HIE on edge (staging) servers that are separate from, and updated regularly by, the providers' electronic medical record transaction systems.

This requirement describes the "hybrid" logical architecture.

HIE-R-17: Implemented solutions shall provide data synchronization from provider systems daily.

HIE-R-18: The COV-HIE shall provide high availability with redundancy and fail-over to achieve 24 by 7 service levels.

COV-HIE Architecture – Data Sub-Topic

The requirements for the management of data are as follows:

HIE-R-19: The COV-HIE will communicate with edge servers to provide data in structured or unstructured data formats as defined by ONC. Even though the federal government recognizes storing data in the Continuity of Care Document (CCD) and Continuity of Care Record (CCR) formats, the COV-HIE shall only require the data in the CCD format to ease the burden on the organizations generating the data to share.

HIE-R-20: The COV-HIE shall follow the ONC specifications for data storage.

HIE-R-21: The COV-HIE shall adhere to the set of coded health care terminologies defined by the Federal Health Architecture (FHA).

COV-HIE Architecture – Privacy and Security Sub-Topic

The requirements for privacy and security are as follows:

HIE-R-22: The COV-HIE shall incorporate ARRA privacy and security provisions related to security breach restrictions and disclosures, sales of health information, consumer access, business associate obligations and agreements.

HIE-R-23: The COV-HIE shall incorporate Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule for permitted uses and disclosures and individual rights related to protected health information.

HIE-R-24: The COV-HIE shall incorporate Health Insurance Portability and Accountability Act (HIPAA) Security Rule for administrative, technical, and physical security procedures,

HIE-R-25: The COV-HIE shall incorporate Confidentiality of Alcohol and Drug Abuse Patient Records Regulations for substance abuse treatment programs.

HIE-R-26: The COV-HIE shall incorporate Health and Human Services (HHS) Privacy and Security Framework for a single consistent approach to address the privacy and security challenges related to electronic health information exchange.

HIE-R-27: The COV-HIE shall incorporate federal requirements for protection of health data for federal health care delivery organizations such as the Department of Veterans Affairs and the Department of Defense.

HIE-R-28: The COV-HIE shall adopt the ONC specifications for privacy and security when issued.

HIE-R-29: The COV-HIE shall (as part of the onboarding process) issue a security certificate to the trusted entity.

Further information on privacy and security can be found in Appendix D.

Glossary of HIE Terms

Following are Glossary entries pertaining to the COV-HIE architecture. Additional HITSP terms can be found in Appendix B:

COV-HIE[1]	The COV-HIE is a network and a service, and —exchange‖ within its name is both a noun and a verb. As a noun, it is a digital network allowing providers to exchange electronically and with semantic interoperability health care data about patients they share. As a verb, it is a collection of services that reliably communicate clinical data between providers by identifying patients and locating their digital medical records across various electronic medical record systems.
Electronic Medical Record (EMR)[2]	An electronic record of health-related information on an individual that can be created, gathered, managed and consulted by authorized clinicians and staff within one health care organization.
Electronic Health Record (EHR)[2]	An electronic record of health-related information on an individual that conforms to nationally recognized interoperability standards and that can be created, gathered, managed and consulted by authorized clinicians and staff across more than one health care organization
Health Information Exchange (HIE)[2]	The electronic movement of health-related information among organizations according to nationally recognized standards.
Health Information Organization (HIO)[2]	An organization that oversees and governs the exchange of health-related information among organizations according to nationally recognized standards.
Interoperability[3]	Interoperability is the ability of health information system to work together within and across organizational boundaries, in order to advance the effective delivery of health care for individuals and communities.

[1] Definition created by Health Information Technology Standards Advisory Committee (HITSAC)
[2] National Alliance for Health Information Technology Report to Office of National Coordinator for Health Information Technology, April 28, 2008
[3] Health Information Technology Standards Panel (HITSP) Glossary version 2.0 dated July 2009

Appendix A: References and Links

State and Federal Sites:

Contributions, references, and insights were derived from the following web sites.

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

ONC is the principal Federal entity charged with coordination of nationwide efforts to implement and use the most advanced health information technology and the electronic exchange of health information. ONC is organizationally located within the Office of the Secretary for the U.S. Department of Health and Human Services (HHS): http://healthit.hhs.gov/portal/server.pt?open=512&objID=1200&parentname=CommunityPage&parentid=1&mode=2&in_hi_userid=10741&cached=true.

Healthcare Information Technology Standards Panel (HITSP)

HITSP is a cooperative partnership between the public and private sectors. The Panel was formed for the purpose of harmonizing and integrating standards that will meet clinical and business needs for sharing information among organizations and systems: http://www.hitsp.org/default.aspx.

Meaningful Use

http://healthit.hhs.gov/portal/server.pt?open=512&objID=1325&parentname=CommunityPage&parentid=1&mode=2.

Health IT Policy Committee

The Health IT Policy Committee will make recommendations to the National Coordinator for Health IT on a policy framework for the development and adoption of a nationwide health information infrastructure, including standards for the exchange of patient medical information: http://healthit.hhs.gov/portal/server.pt?open=512&objID=1269&parentname=CommunityPage&parentid=5&mode=2.

Federal Health Architecture (FHA)

http://healthit.hhs.gov/portal/server.pt?open=512&objID=1181&parentname=CommunityPage&parentid=1&mode=2&in_hi_userid=10741&cached=true.

Healthcare Information and Management Systems Society (HIMSS)

HIMSS is the healthcare industry's membership organization exclusively focused on providing global leadership for the optimal use of healthcare information technology (IT) and management systems for the betterment of healthcare: http://www.himss.org/ASP/index.asp.

HITECH Grant Programs

http://healthit.hhs.gov/portal/server.pt?open=512&objID=1310&parentname=CommunityPage&parentid=8&mode=2&in_hi_userid=11113&cached=true.

Funding Opportunity Announcement – State Health Information Exchange

http://healthit.hhs.gov/portal/server.pt?open=512&objID=1336&parentname=CommunityPage&parentid=47&mode=2&in_hi_userid=11113&cached=true#3.

Appendix B: HITSP Terms, Capabilities and Drill Down Example

Summary of HITSP Terms

The terms below have been defined by HITSP as follows:

Capabilities (CAP)

An implementable business service that specifies interoperable Information Exchanges using HITSP constructs. A Capability supports stakeholder requirements and business processes and includes workflow, information content, infrastructure, Security and Privacy.

Component

A component is a construct that defines the set of data elements, structures, relationships, constraints and terminology needed to support specific reusable information content. A Component may also express constraints on base or composite standards, examples include the Lab Result Message and Lab Result Context.

Constructs

A specification based on harmonized interoperability standards. HITSP defines Transaction, Transaction Package, Service Collaboration and Component constructs.

Interoperability Specifications (IS)

Interoperability Specifications are organized by scenarios, Capabilities, and integrates and constrains HITSP Constructs to specify the interoperability needs of one or more business processes.

Transaction (T)

A logical grouping of data exchanges and transport methods that must all succeed or fail as a group. Examples are the Query Lab Result or Send Lab Result.

Transaction Package (TP)

A logical grouping of two or more Transactions, Transaction Packages, and/or composite standards used to fulfill Information Exchange Requirements (IERs). A transaction package is not required to succeed or fail as a whole. Examples include the Record Locator Service and Entity Identification Service.

Classifications and Terminologies

Classifications and terminologies are used with code sets to define and classify individual health terms. They serve as a way to relate terms to one another so that they are easily and consistently understood by users. Classifications arrange related terms for easy retrieval, while vocabularies are sets of specialized terms that facilitate precise communication by eliminating ambiguity. Important classifications include: ICD-9-CM, ICD-10, ICD-10-CM/PCS, and ICF. Important terminologies include LOINC and SNOMED. There

are subtle differences between vocabularies, nomenclatures, terminologies and classifications. These have been addressed by the American Health Information Management Association (AHIMA).

Summary of HITSP Capabilities

HITSP has identified 26 capabilities from the original use cases. A high level summary of each capability is provided below:

HITSP/CAP117 Communicate Ambulatory and Long Term Care Prescription

This capability addresses interoperability requirements that support electronic prescribing in the ambulatory and long term care environment. The capability supports:

1. The transmittal of new or modified prescriptions
2. Transmittal of prescription refills and renewals
3. Communication of dispensing status
4. Access to formulary and benefit information

HITSP/CAP118 Communicate Hospital Prescription

This capability addresses interoperability requirements that support electronic prescribing for inpatient orders that can occur within an organization or between organizations. The capability supports the transmittal of a new or modified prescription from a Hospital to an internal or external pharmacy. It also includes the optionality to access formulary and benefit information.

HITSP/CAP119 Communicate Structured Document

This capability addresses interoperability requirements that support the communication of structured health data related to a patient in a context set by the source of the document who is attesting to its content. Several document content subsets, structured according to the HL7 CDA standard, are supported by this capability. The following are examples of the type of structured data that may be used:

1. Continuity of Care Document (CCD)
2. Emergency Department Encounter Summary
3. Discharge Summary (In-patient encounter and/or episodes of care)
4. Referral Summary Ambulatory (encounter and/or episodes of care)
5. Consultation Notes
6. History and Physical
7. Personal Health Device Monitoring Document
8. Health Care Associated Infection (HAI) Report Document. Document creators shall support a number of the HITSP specified coded terminologies as defined by specific content subsets specified in this capability

HITSP/CAP120 Communicate Unstructured Document

This capability addresses interoperability requirements that support the communication of a set of unstructured health data related to a patient in a context set by the source of the

document who is attesting to its content. Two types of specific unstructured content are supported, both with a structured CDA header:

1. PDF-A supporting long-term archival
2. UTF-8 text

HITSP/CAP121 Communicate Clinical Referral Request

This capability addresses interoperability requirements that support provider-to-provider (clinical) referral request interaction. It allows the bundling of the referral request document with other relevant clinical documents of interest by referencing such documents as shared by other capabilities such as: CAP119 Communicate Structured Document; CAP120 Communicate Unstructured Document; or CAP133 Communicate Immunization Summary.

HITSP/CAP122 Retrieve Medical Knowledge

This capability addresses the requirements to retrieve medical knowledge that is not patient-specific based on context parameters. The actual content delivered is not constrained by this capability; this capability focuses on providing the mechanism to ask for (query) and receive the medical knowledge.

HITSP/CAP123 Retrieve Existing Data

This capability supports queries for clinical data (e.g., common observations, vital signs, problems, medications, allergies, immunizations, diagnostic results, professional services, procedures and visit history).

HITSP/CAP124 Establish Secure Web Access

This capability is focused on providing a secured method to access information available from document repositories (e.g., Laboratory Report) in order to view them locally on a system. The chosen method for viewing the document content is through a web browser.

HITSP/CAP125 Retrieve Genomic Decision Support

This capability addresses interoperability requirements that support the communication of genetic and family history information and an assessment of genetic risk of disease for a patient.

HITSP/CAP126 Communicate Lab Results Message

This capability addresses interoperability requirements that support the sending of a set of laboratory test results. Ordering Providers of Care receive results as a laboratory results message. The communication of the order is out of scope for this capability. The content of these test results may be either or both: General Laboratory Test Results; Microbiology Test Results. This capability may use content anonymization.

HITSP/CAP127 Communicate Lab Results Document

This capability addresses interoperability requirements that support the communication of a set of structured laboratory results related to a patient in a context set by the source of the document who is attesting to its content. Non-ordering Providers of Care access historical

laboratory results as documents and "copy-to" Providers of Care may receive document availability notifications to retrieve such lab report documents. Lab Report content creators shall support HITSP specified coded terminologies as defined by specific content subsets specified in this Capability for: General Laboratory Test Results; Microbiology Test Results. This capability may use content anonymization.

HITSP/CAP128 Communicate Imaging Information

This capability addresses interoperability requirements that support the communication of a set of imaging results (i.e., reports, image series from imaging studies) related to a patient in a context set. This is done by an Imaging System acting as the information source attesting to its content. This capability may use content anonymization.

HITSP/CAP129 Communicate Quality Measure Data

This capability addresses interoperability to support hospital and clinician collection and communication of patient encounter data to support the analysis needed to identify a clinician or hospital's results relative to an EHR-compatible, standards-based quality measure. Quality measures may include:

1. Patient-level clinical detail from which to compute quality measures. Patient level clinical data is compiled from both the local systems and from longitudinal data available through other sources such as a Health Information Exchange (HIE)
2. Patient-level quality data based upon clinical detail. The —patient-level quality data reports‖ are exported from EHRs or quality-monitoring applications at the point of care. This capability may use content anonymization. Pseudonymization, if needed, is supported by the Capability 138 Retrieve Pseudonym. This capability may use Value Set Sharing

HITSP/CAP130 Communicate Quality Measure Specification

This capability addresses interoperability requirements for an EHR-compatible, standards-based quality measure. In the measure specification, needed patient encounter data elements are identified so they can be extracted from local systems and from longitudinal data available through other sources such as a Health Information Exchange (HIE). The measure specification also includes various sets of exclusion/inclusion criteria to identify which patients to include in calculation of the measure. This capability may use Value Set Sharing.

HITSP/CAP131 Update Immunization Registry

This capability addresses interoperability requirements that enable electronic communication of immunization data among clinicians, with patients, and with immunization registries as unsolicited structured patient immunization data. This capability may use content anonymization.

HITSP/CAP132 Retrieve Immunization Registry Information

This capability addresses interoperability requirements that support the query and retrieval of structured immunization data related to a patient's vaccination. The capability may use one of the following:

1. HL7V2 query with implicit Patient Identity resolution
2. HL7V2 query with explicitly Patient Identity resolution prior to query
3. HL7V3 Query for Existing Data The query for immunization documents from Capability 133 - Communicate Immunization Summary may also be used

HITSP/CAP133 Communicate Immunization Summary

This capability addresses interoperability requirements to support the communication of structured health data related to a patient's vaccination history. This immunization document contains a history of administered vaccines with details such as lot number, who administered it, as well as other information related to the patient's care such as medical history, medications, allergies, vital signs.

HITSP/CAP135 Retrieve and Populate Form

This capability addresses interoperability requirements to support the upload of specific captured data (e.g. public health surveillance reportable conditions, health care associated infection reporting) to Public Health Monitoring Systems and Quality Organizations Systems. The forms presented may be pre-populated by information provided by the clinical or laboratory information systems to avoid manual re-entry. A number of supplemental information variables may be captured from within the user's clinical information system to improve the workflow and timeliness of required reporting. One or more types of form content may be supported:

1. Pre-population for Public Health Case Reports from Structured Documents using CDA
2. Pre-population for Quality Data from Structured Documents using CDA
3. No pre-population content Systems may optionally support the means to retrieve request for clarifications

HITSP/CAP136 Communicate Emergency Alert

This capability addresses interoperability requirements to support multicast of non-patient specific notification messages about emergencies events, alerts concerning incidence of communicable diseases, alerts concerning population needs for vaccines and other generic alerts sent to an identified channel. The intended recipients are populations such as —all emergency departments in XXX county‖, —within a geographic area‖, etc. Note that this capability is not used to communicate patient-specific or identifiable data.

HITSP/CAP137 Communicate Encounter Information Message

This capability addresses interoperability requirements to send specific clinical encounter data among multiple systems. The content may be either or both:

1. Encounter Data Message
2. Radiology Results Message It may be used in conjunction with other capabilities such as those related to the communication of laboratory data. This capability includes optional anonymization of content

HITSP/CAP138 Retrieve Pseudonym

This capability addresses interoperability requirements to support a particular type of anonymization that both removes the association with a data subject, and adds an association between a particular set of characteristics relating to the data subject and one or more pseudonyms. This enables a process of supplying an alternative identifier, which permits a patient to be referred to by a key that suppresses his/her actual identification information. The purpose of this capability is to offer a pseudonymization framework for situations that require the use of specific data without disclosing the specific identity of patients or providers. Pseudo-identifiers are intended to allow accessibility to clinical information, while safeguarding any information that may compromise the privacy of the individual patient or provider. However, unlike anonymization, the alternative identifier key can be used to re-identify the individuals whose data was used.

HITSP/CAP139 Communicate Resource Utilization

This capability specifies the message and content necessary to report utilization and status of health provider resources to systems supporting emergency management officials at local, state or national levels who have a need to know the availability of hospital and other health care resources. The resource utilization information may be provided routinely or in response to a request.

HITSP/CAP140 Communicate Benefits and Eligibility

This capability addresses interoperability requirements that support electronic inquiry and response from a patient's eligibility for health insurance benefits. The information exchanged includes the following:

1. A patient's identification (i.e., name, date of birth, and the health plan's member identification number)
2. Communication of a member's status of coverage and benefit information and financial liability
3. Access to information about types of services, benefits and coverage for various medical care and medications. It provides clinicians with information about each member's health insurance coverage and benefits

HITSP/CAP141 Communicate Referral Authorization

This capability addresses interoperability requirements that support electronic inquiry and response to authorizing a patient (health plan member) to be referred for service by another provider or to receive a type of service or medication under the patient's health insurance benefits. The capability supports the transmittal of a patient's name and insurance identification number with the request for the type of service. It also includes the following optional requirements:

1. Identification of the type of service or medication requested for benefit coverage (does not guarantee payment by insurance provider)
2. Communication of a referral notification number or authorization number from the Payer System to the Provider System. It provides clinicians and pharmacists with information about each patient's medical insurance coverage and benefits. It may include information on referral or authorization permission

HITSP/CAP142 Retrieve Communications Recipient

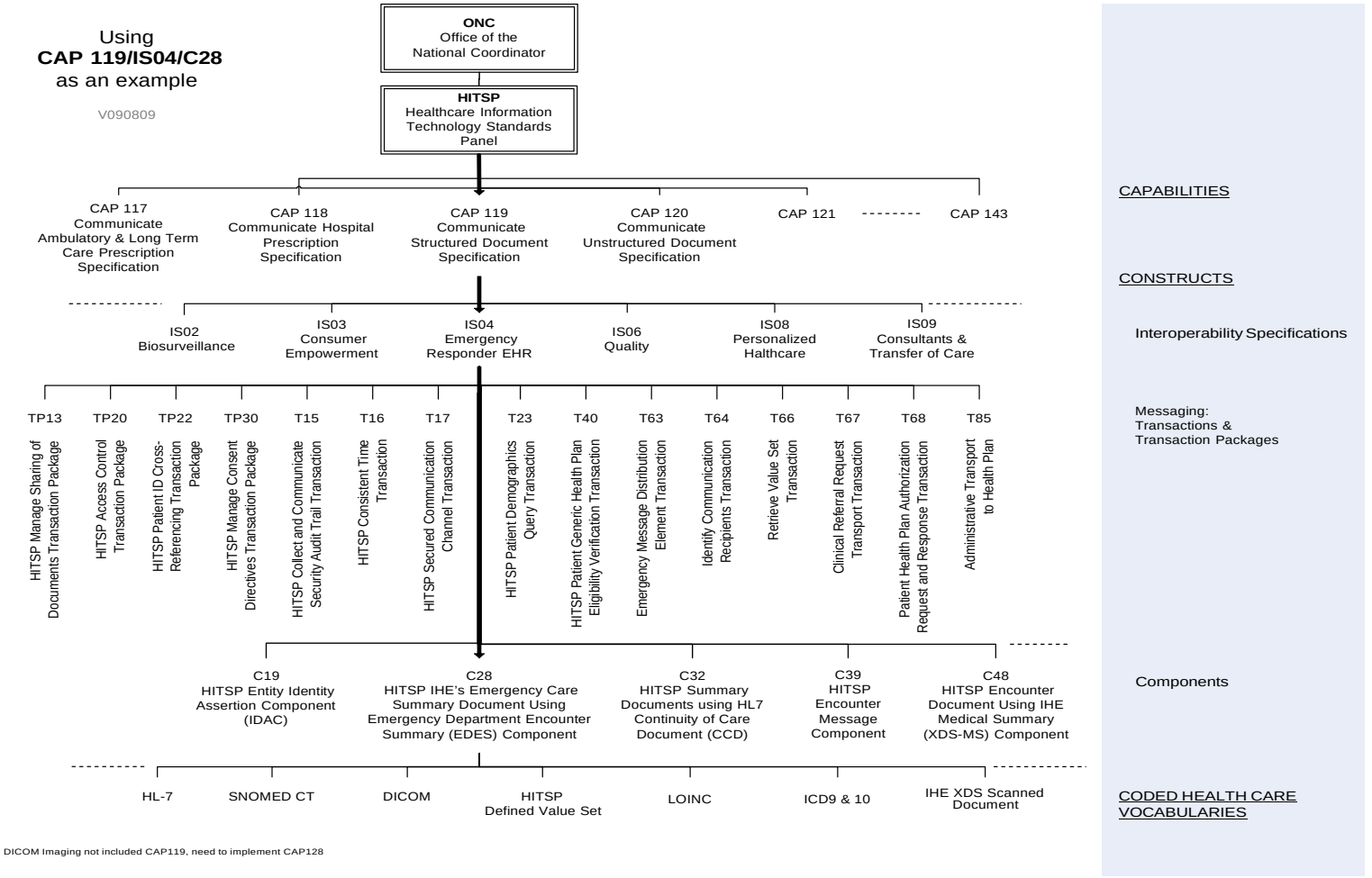
This capability addresses interoperability requirements that support access to a directory to identify one or more communication recipients in order to deliver alerts and bidirectional communications (e.g., public health agencies notifying a specific group of service providers about an event). The method and criteria by which individuals are added to a directory is a policy decision, which is out of scope for this construct.

HITSP/CAP143 Manage Consumer Preference and Consents

This capability addresses management of consumer preferences and consents as an acknowledgement of a privacy policy. This capability is used to capture a patient or consumer agreement to one or more privacy policies; where examples of a privacy policy may represent a consent, dissent, authorization for data use, authorization for organizational access, or authorization for a specific clinical trial. This capability also supports the recording of changes to prior privacy policies such as when a patient changes their level of participation or requests that data no-longer be made available because they have left the region.

Drill Down – Capability 119 Communicate Structured Documentation

Cap 119 is made up of eleven IS - IS 04 Emergency Responder Electronic Health Record; IS 08 Personalized Health Care; IS 09 Consultations and Transfers of Care; IS 02 Biosurveillance; IS 06 Quality; IS 10 Immunizations and Response Management; IS 11 Public Health Case Reporting; IS 03 Consumer Empowerment; IS 05 Consumer Empowerment and Access to Clinical Information via Media; IS 07 Medication Management; and IS 77 Remote Monitoring. This example drills down on transactions, components and vocabularies for IS 04.



Appendix C: HITSP Capabilities Mapped to Interoperability Specifications

The following IS Table 5-1 is from the HITSP EHR-Centric Interoperability Specification.

Table 5-1 HITSP Capabilities Mapped to Interoperability Specifications

HITSP Capabilities

Exchange Administrative Benefits/Eligibility transactions specification	Exchange Administrative Referral/Authorization Transactions Specifications	Retrieve Communications Recipient	Consumer Preferences and Consent Management	Communicate Ambulatory and Long Term Care Prescription Specification	Communicate Hospital Prescription Specification	Communicate Structured Document Specification	Communicate Unstructured Document Specification	Communicate Clinical Referral Request Specification	Retrieve medical Knowledge Specifications	Retrieve existing data Specifications	Establish Secure web access Specifications	Retrieve Genomic Decision Support Specifications	Communicate Lab Results Message Specifications	Communication of Lab Results Document Specifications	Communicate Imaging Information Specifications	Communicate Quality Measure Data Specifications	Communicate Quality Measure Specification Specifications	Immunization Registry update Specifications	Immunization Registry Query Specifications	Communication of Immunization Summary Specifications	Retrieve Pre-populated Form for Data Capture Specifications	Emergency Alerting Specifications	Send and Receive clinical data message Specifications	Assign pseudo-identity Specifications	Communicate Resource Utilization Specifications	Supporting Components of the HITSP Interoperability Specifications IHE profiles shown when relevant to the specified HITSP component
CAP 140	CAP 141	CAP 142	CAP 143	CAP 117	CAP 118	CAP 119	CAP 120	CAP 121	CAP 122	CAP 123	CAP 124	CAP 125	CAP 126	CAP 127	CAP 128	CAP 129	CAP 130	CAP 131	CAP 132	CAP 133	CAP 135	CAP 136	CAP 137	CAP 138	CAP 139	Original AHIC Use Cases
ADMINISTRATIVE and FINANCIAL				Medication Management		Exchange of Clinical Data							Exchange of Laboratory and Imaging Data			Quality Management		Immunization			Case Reporting and Bio-surveillance				Emergency	
				CLINICAL OPERATIONS (Care Delivery, Emergency Responder and Consumer Empowerment)												CLINICAL QUALITY AND PUBLIC HEALTH											
																										Provider Perspective
			•								•		•	•												IS 01 - Electronic Health Record (EHR) Laboratory Results Reporting
•	•	•	•			•	•	•						•								•	•		•	IS 04 - Emergency Responder Electronic Health Record (ER-EHR)
•	•	•	•			•	•		•			•	•	•												IS 08 - Personalized Healthcare
•	•	•	•			•	•	•					•	•	•								•			IS 09 - Consultations and Transfers of Care
																										Population Perspective
			•			•				•			•	•	•						•		•	•	•	IS 02 - Biosurveillance
			•			•				•						•	•									IS 06 - Quality
		•	•			•	•		•	•								•	•	•		•		•		IS 10 - Immunizations and Response Management
		•	•			•	•		•	•			•	•							•	•	•	•	•	IS 11 - Public Health Case Reporting
																										Consumer Perspective
			•			•	•		•					•												IS 03 - Consumer Empowerment
			•			•	•		•					•												IS 05 - Consumer Empowerment and Access to Clinical Information via I
•			•	•	•	•																				IS 07 - Medication Management
			•				•																			IS 12 - Patient – Provider Secure Messaging
•	•		•			•																				IS 77 - Remote Monitoring

Appendix D: Privacy and Security Resources

The ARRA includes specific privacy and security provisions related to security breach, restrictions and disclosures, sales of health information, consumer access, business associate obligations and agreements. Representative examples can be found in Funding Opportunity Announcement (FOA) Appendix F.

- The HIPAA Privacy Rule specifies permitted uses and disclosures and individual rights related to protected health information. These provisions are found at 45 CFR Part 160 and Part 164, Subparts A and E. For more details, please refer to: http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/adminsimpregtext.pdf
- The HIPAA Security Rule specifies a series of administrative, technical, and physical security procedures for covered entities to use to assure the confidentiality of electronic protected health information. These provisions are found at 45 CFR Part 160, and Part 164, Subparts A and C.C For more details, please refer to: http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/adminsimpregtext.pdf
- The Confidentiality of Alcohol and Drug Abuse Patient Records Regulation (42 CFR Part 2) specifies confidentiality requirements for substance abuse treatment programs as defined by 42 CFR § 2.11 that are —federally assistedll as defined by 42 CFR § 2.12(b)). For more details, please refer to: http://www.hipaa.samhsa.gov
- The HHS Privacy and Security Framework establishes a single, consistent approach to address the privacy and security challenges related to electronic health information exchange through a network for all persons, regardless of the legal framework that may apply to a particular organization. The goal of this effort is to establish a policy framework for electronic health information exchange that can help guide the Nation's adoption of health information technologies and help improve the availability of health information and health care quality. The principles have been designed to establish the roles of individuals and the responsibilities of those who hold and exchange electronic individually identifiable health information through a network. The principles are found in Funding Opportunity - Appendix F
- To the extent that states anticipate exchanging health information with federal health care delivery organizations, such as the Department of Veterans Affairs (VA), Department of Defense (DoD), and the Indian Health Service (IHS), it will be important for the state to meet various federal requirements for protection of health data as applicable
- As the program evolves over time, ONC plans to issue additional program guidance to further define the privacy and security requirements

American Reinvestment and ARRA References

ARRA Section D – Privacy describes improved privacy provisions and security provisions related to:

- Sec. 13402 - notification in the case of breach

- Sec. 13404 – application of privacy provisions and penalties to business associates of covered entities
- Sec. 13405 – restrictions on certain disclosures and sales of health information; accounting of certain protected health information disclosures; access to certain information in electronic format
- Sec. 13406 – conditions on certain contacts as part of health care operations
- Sec. 13407 – temporary breach notification requirement for vendors of personal health records and other non-HIPAA covered entities
- Sec. 13408 – business associate contracts required for certain entities

This list is provided to highlight examples of the ARRA privacy and security requirements. It is not intended to be comprehensive nor definitive program guidance to recipients regarding the ARRA requirements for privacy and security.

Privacy Act of 1974

- 45 CFR Part 5b. A link to the full Privacy Act can be found at: http://www.hhs.gov/foia/privacy/index.html

HIPAA Security Rule

- 45 CFR Parts 160, 162, and 164. A link to the HIPAA Security Rule can be found at: http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/adminsimpregtext.pdf

HIPAA Privacy Rule

- 45 CFR Part 160 and Subparts A and E of Part 164. For more details: http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/adminsimpregtext.pdf

Federal Information Security Management Act, 2002

- 45 CFR Parts 160, 162, and 164. A link to the full Act can be found at: http://aspe.hhs.gov/datacncl/Privacy/titleV.pdf

Confidentiality of Alcohol and Drug Abuse Patient Records

- 45 CFR Part 2. For more details: http://www.hipaa.samhsa.gov

The HHS Privacy and Security Framework Principles

- Individual Access - Individuals should be provided with a simple and timely means to access and obtain their individually identifiable health information in a readable form and format
- Correction- Individuals should be provided with a timely means to dispute the accuracy or integrity of their individually identifiable health information, and to have

erroneous information corrected or to have a dispute documented if their requests are denied

- Openness and Transparency - There should be openness and transparency about policies, procedures, and technologies that directly affect individuals and/or their individually identifiable health information
- Individual Choice - Individuals should be provided a reasonable opportunity and capability to make informed decisions about the collection, use, and disclosure of their individually identifiable health information
- Collection, Use and Disclosure Limitation - Individually identifiable health information should be collected, used, and/or disclosed only to the extent necessary to accomplish a specified purpose(s) and never to discriminate inappropriately
- Data Quality and Integrity - Persons and entities should take reasonable steps to ensure that individually identifiable health information is complete, accurate, and up-to-date to the extent necessary for the person's or entity's intended purposes and has not been altered or destroyed in an unauthorized manner
- Safeguards - Individually identifiable health information should be protected with reasonable administrative, technical, and physical safeguards to ensure its confidentiality, integrity, and availability and to prevent unauthorized or inappropriate access, use, or disclosure
- Accountability - These principles should be implemented, and adherence assured, through appropriate monitoring and other means and methods should be in place to report and mitigate non-adherence and breaches

For more information, visit http://healthit.hhs.gov and click on the Privacy and Security link for the Framework and its Principles.