Commonwealth of Virginia Health Information Exchange (COV-HIE)

Technical Infrastructure

November 19, 2009

Version 9

DRAFT

COV-HIE Technical Infrastructure

Table of Contents

Introduction.....Page 4

Summary of Recommendations.....Page 5

Key Accomplishments – Technical Infrastructure Domain .....Page 8

Technical Infrastructure Components.....Page 10

HITSP Interoperability Standards .....Page 11

Privacy & Security .....Page 12

Patient Identification .....Page 13

Network.....Page 14

Architectural Models for Data and Centralized Services .....Page 16

Coded Heath Care Vocabularies .....Page 17

Exhibits

A: 2009 PQRI .....Page 18

B: HITSP Capabilities.....Page 25

C: HITSP Capabilities Mapped to Interoperability Specifications.....Page 31

D: Summary of HITSP Capabilities (Drill Down Example) ..... Page 32

D: Privacy & Security References from funding opportunity .....Page 33

DRAFT

Commonwealth of Virginia - Health Information Exchange (COV-HIE)
Technical Infrastructure Domain

I. Introduction

In October 2009, the Commonwealth of Virginia responded to a federal funding opportunity announcement to develop a strategic and operational plan for a state Health Information Exchange (HIE). The Health Information Technology Standards Advisory Committee (HITSAC), which advises the Information Technology Investment Board (ITIB), created this white paper to serve two purposes:

- to assist the HIE Work Group in their application efforts and
- to begin summarizing the key technical infrastructure standards for a state HIE

The outline for this document follows the structure of the HIE funding opportunity announcement which 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 funding opportunity describes five domains:

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

This white paper focuses on the Technical Infrastructure domain.

The ***blue italic*** text in this white paper has been copied directly from the Funding Opportunity Announcement.

The red text highlights HITSAC recommendations and notes.

DRAFT

II. Summary of Recommendations

HITSAC recommends this initial set of standards for the Health Information Exchange (HIE) Technical Infrastructure Domain. Under the Technical Infrastructure Domain the standards have been grouped into four categories: Interoperability, Technical Infrastructure, Data and Privacy and Security.

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

The recommendations are as follows:

Standard	HITSAC Recommendation
Interoperability	1. The COV-HIE shall be congruent with the standards established by the Office of the National Coordinator (ONC) and be routinely certified by ONC. 2. The COV-HIE shall adopt the HITSP Interoperability Specifications and Capabilities recommended by ONC. The COV-HIE shall support the interoperability and data exchange functions of "meaningful use" of Electronic Health Records (EHR). 3. All Commonwealth of Virginia HIEs shall comply with the HITSP Interoperability Specifications and Capabilities. 4. The COV-HIE shall support, at a minimum, the following capabilities: ▪ Electronic eligibility and claims transactions: adherence to HITSP Capability 140 (communicate benefits and eligibility) and HIPAA standards. ▪ Electronic prescribing and refill requests: Utilize an established eprescribing vendor to adhere to HITSP Capabilities 117 and 118 (prescription). ▪ Prescription fill status and/or medication fill history: adherence to HITSP Capabilities 117and 118. ▪ Clinical summary exchange for care coordination and patient engagement: adherence to Capabilities 119 and 120 as the basis for interoperability of patient documentation (structured and unstructured). ▪ Quality Reporting: adherence to Capability 130. ▪ Electronic public health reporting: adherence to Interoperability Specification 11. ▪ Electronic clinical laboratory ordering and results delivery: adherence to Capabilities 126 and 127. 5. The COV-HIE shall adopt the HITSP Capabilities for patient identification, when issued by ONC.
Technical Infrastructure	1. The scope of technical infrastructure capabilities shall include all current and future requirements of HITSP Components for "meaningful use", as defined by ONC. 2. The COV-HIE shall support the connectivity requirements of the

DRAFT

	National Health Information Network (NHIN) and provide connectivity to the NHIN for providers and HIEs in the Commonwealth of Virginia. 3. The COV-HIE shall provide a NHIN Gateway Function. 4. The COV-HIE shall provide, at a minimum, Security Services, Patient Locator Services, Data/Document Locator Services, and Terminology Services as defined by HITSP. 5. 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 sentence describes the "hybrid" logical architecture. 6. Implemented solutions shall provide data synchronization from provider systems daily. 7. The COV-HIE shall provide high availability with redundancy and fail-over to achieve 24 by 7 by 365 service levels.
Data	1. Clinical patient data shall be stored on the edge servers in the Continuity of Care Document (CCD) format, as currently endorsed by HITSP. 2. The COV-HIE shall follow the HITSP interoperability specifications to determine the duration of data storage. 3. The COV-HIE shall adhere to the set of coded health care terminologies defined by the Federal Health Architecture (FHA).
Privacy and Security	1. The COV-HIE shall incorporate privacy and security provisions as specified in the federal HIE funding opportunity announcement. The privacy and security provisions are as follows: ▪ ARRA specific privacy and security provisions related to security breach restrictions and disclosures, sales of health information, consumer access, business associate obligations and agreements ▪ Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule for permitted uses and disclosures and individual rights related to protected health information. ▪ Health Insurance Portability and Accountability Act (HIPAA) Security Rule for administrative, technical, and physical security procedures, ▪ Confidentiality of Alcohol and Drug Abuse Patient Records Regulations for substance abuse treatment programs. ▪ 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. ▪ 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. ▪ The NHIN Cooperative Technical and Security Committee recommendations. 2. The COV-HIE shall adhere to all applicable Commonwealth of Virginia laws concerning security and privacy. 3. The COV-HIE shall adopt the HITSP specifications for privacy and security, when issued by ONC.

DRAFT

In addition, HITSAC suggests the Health Information Technology Advisory Commission (HITAC) chaired by the Commonwealth's Secretary of Health and Human Resources consider the following Governance recommendations.

Standard	HITSAC Recommendation
Governance	1. All providers and HIEs connect through the COV-HIE to the NHIN.
Governance & Operations	1. All institutions participating in the COV-HIE shall prove to the organization that governs the COV-HIE their ability to audit transactions and uphold policies ensuring data privacy and security. 2. The COV-HIE shall employ authentication and audit policies of the Health Information Security and Privacy Collaborative (HISPC).
Governance & Privacy and Security	1. Where two or more privacy and security standards conflict, the COV-HIE shall adopt the standards that are more protective of patient privacy.

DRAFT

III. Key Accomplishments – Technical Infrastructure Domain

According to the HIE Funding Opportunity Announcement key accomplishments for the Technical Infrastructure domain include:

Technical Infrastructure

- *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 Recommends:

- HITSAC recommends the scope of technical infrastructure capabilities include all current and future requirements of HITSP Components for "meaningful use", as defined by ONC.

HITSAC Notes:

- HITSAC notes that laboratory ordering, as stated in the funding opportunity announcement, is not currently a Health Information Technology Standards Panel (HITSP) defined Capability and should remain an independent solution for states; 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.*

The components of the Project Narrative counted as part of the 40 page limit include:

- *Current State*
- *Proposed Project Strategy*
- *Required Performance Measures*
- *Project Management*
- *Evaluation*
- *Organizational Capability Statement*

DRAFT

Listed below is HITSAC input on the Current State and Proposed Project Strategy components.

Current State

- *Discuss and determine the current status of the state's progress in achieving statewide HIE among health care providers and describe the progress and status of the state in its project planning and implementation, including:*
  - *Electronic eligibility and claims transactions –* The Virginia Health Exchange Network (VHEN) is a collaboration of Virginia health plans and health systems dedicated to lowering administrative costs in health care convened by the Virginia Association of Health Plans (VHAP), the Virginia Hospital and Health Care Association (VHHA) and the Governor's Office of Health IT.
  - *Electronic prescribing and refill requests –* A Surescripts vendor based pharmacy network exists in the state. The HIE should be capable of retrieving medication history and not duplicate the e-prescribing function a pharmacy network provides.
  - *Electronic clinical laboratory ordering and results delivery.* The State public health lab, known as the Division of Consolidated Services (DCLS), is actively engaged with CDC and the Association of Public Health Laboratories to develop an HL7 compliant message format for reporting nationally notifiable disease data to State health departments and CDC. This project uses nationally adopted data and technology standards for the submission of laboratory orders and reporting of results. This project has adopted HL7 version 2.5 and uses FIPS, CDC's PHIN_VADS, LOINC and SNOMED CT vocabularies. DCLS also receives daily electronic test orders from all local health departments through the VDH Webvision system. These orders are submitted using a non-standard messaging format and non-standard vocabularies. Currently results are delivered to VDH using paper-based reports because VDH systems are unable to consume and process an HL7 compliant message.
  - *Electronic public health reporting (immunizations, notifiable laboratory results).* The Commonwealth utilizes a system known as the Virginia Immunization Information System (VIIS) to track immunizations. VIIS was developed in Wisconsin under a CDC grant and is used in 20 states. The system utilizes SNOMED CT, NIP table values (National Immunization Program), CPT, CVX, LOINC, FIPS (Federal Information Processing Standard), and HL7 standards.
  - *Quality reporting capabilities.* Inpatient Hospitals report to CMS Physician Quality Reporting Initiative (PQRI) quality measures. The 2009 PQRI consists of 153 quality measures and is explained in Exhibit A. Health Systems are also surveyed and report core measures to the Joint Commission's ORYX quality initiative.
  - *Prescription fill status and/or medication fill history.* A Surescripts vendor based pharmacy network exists in the state. The HIE should be capable of retrieving medication history and not duplicate the e- prescribing function a pharmacy network provides.
  - *Clinical summary exchange for care coordination and patient engagement.* Providers that share the EPIC systems EMR will have this capability between them, but it will need to be extended to fully achieve the objectives of the state HIE. In addition, there are existing RHIO's and Community HIE's such as NOVA which will need to be included in the COV-HIE planning.

The Commonwealth of Virginia has several initiatives underway to provide health information exchange. These include the VIIS immunization registry, VHEN for financial administrative transactions, Carespark, Med Virginia, Public Health Laboratory Interoperability Project (PHLIP) with CDC and vendor enabled health information exchanges such as Epic.

DRAFT

Proposed Project Summary

Articulate the rationale for the overall approach to the project. Also note any major barriers anticipated to be encountered and how the project will be able to overcome those barriers. Include all portions required but applicants may frame their answers according to their current status (whether the state has an existing plan or intends to develop or finalize one using federal funds).

Domain Requirements

- ***Technical Infrastructure***
  - ***Standards and Certifications*** *– Describe efforts to become consistent with 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 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 Nationwide Health Information Network (NHIN), their plans must specify how they will be complaint with HHS adopted standards and implementation specifications. (http://healthit.hhs.gov/meaningfuluse)*

As stated in the Funding Opportunity Announcement, "widespread adoption and meaningful use of HIT is one of the foundational steps in improving the quality and efficiency of health care. The appropriate and secure electronic exchange and consequent use of health information to improve quality and coordination of care is a critical enabler of a high performance health care system. The overall purpose of this program, as authorized by Section 3013 of the PHSA, as added by ARRA, is to facilitate and expand the secure, electronic, movement and use of health information among organizations according to nationally recognized standards. The governance, policy and technical infrastructure supported through this program will enable standards-based HIE and a high performance health care system."

The Commonwealth of Virginia will develop a statewide clinical information service that will operate as a utility to serve the Virginia citizens' need to move clinical information in a reliable electronic format among the disparate electronic medical record systems of providers of health care services and among the personal health records of members of the public. This shared utility information service, COV-HIE, will be governed as a public-private partnership to protect the integrity and privacy of citizens' personal health information.

COV-HIE will increase the timeliness and reduce the costs of the movement of clinical data between providers of health care services for the benefit of their patients. COV-HIE will provide a common information exchange model for interoperability of electronic medical records consistent with national and international standards for health information exchange. Adherence to widely acknowledged health information standards will promote confidence in the adoption of electronic medical record (EMR) systems by providers of health care services in the Commonwealth of Virginia.

The COV-HIE approach will address the Technical Infrastructure for the following components.

1. HITSP Interoperability Standards
2. Privacy and Security
3. Patient Identification
4. Network
5. Architectural Models for Data and Centralized Services
6. Barriers and Possible Solutions
7. Coded Health Care Vocabularies

DRAFT

1. HITSP Interoperability Standards

HITSAC Recommends:

- HITSAC recommends the COV-HIE be congruent with the standards established by the Office of the National Coordinator (ONC) and be routinely certified by ONC.
- HITSAC recommends the COV-HIE adopt the HITSP Interoperability Specifications and Capabilities recommended by ONC. The COV-HIE shall support the interoperability and data exchange functions of "meaningful use" of Electronic Health Records (EHR).
- HITSAC recommends all Commonwealth of Virginia HIEs comply with the HITSP Interoperability Specifications and Capabilities.
- HITSAC recommends the COV-HIE adopt the HITSP Capabilities for patient identification, when issued by ONC.
- HITSAC recommends the COV-HIE 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.

HITSAC Governance Recommendations:

- HITSAC recommends all providers and HIEs connect through the COV-HIE to the NHIN.

HITSAC Notes:

- HITSAC recognizes that HITSP needs to develop a crosswalk/roadmap between the seven technical infrastructure components listed above and the 26 Capabilities.

The Commonwealth recognizes the multiple stakeholders who would participate and receive benefit from a state wide HIE which connects to health care related stakeholders, community HIE's, and the NHIN. To achieve a successful HIE, stakeholders HIT functions need to be sequenced, and relative industry standards need to be adopted as those functions are implemented. HITSP has been actively working to harmonize the relevant standards.

In July 2009, HITSP reorganized its work on 13 Interoperability Specifications (IS) and 60 related constructs into 26 Capabilities (CAP), to consolidate all information exchanges that involve an Electronic Health Record System. This work effort was organized around ARRA requirements in Title XIII (HITECH) Section 3000 Required Areas for Consideration; and Medicare and Medicaid Incentives defined in ARRA Title IV (Division B). A list of HITSP Capabilities and a drill down example is found in Exhibit B.

The following Capabilities are matched to the initial seven requirements which must be addressed as specified in the Funding Opportunity Announcement.

- HITSAC recommends the COV-HIE support, at a minimum, the following capabilities:
  - Electronic eligibility and claims transactions: adherence to HITSP Capability 140 (communicate benefits and eligibility) and HIPAA standards.
  - Electronic prescribing and refill requests: Utilize an established eprescribing vendor to adhere to HITSP Capabilities 117 and 118 (prescription).
  - Prescription fill status and/or medication fill history: adherence to HITSP Capabilities 117and 118.
  - Clinical summary exchange for care coordination and patient engagement: adherence to Capabilities 119 and 120 as the basis for interoperability of patient documentation (structured and unstructured).

DRAFT

- Quality Reporting: adherence to Capability 130.
- Electronic public health reporting: adherence to Interoperability Specification 11.
- Electronic clinical laboratory ordering and results delivery: adherence to Capabilities 126 and 127.

2. Privacy and Security

As stated in the Funding Opportunity Announcement, *"Privacy and security of health information, including confidentiality, integrity and availability of information, are integral to fostering health information exchange."*

HITSAC Recommends:
HITSAC recommends the COV-HIE incorporate privacy and security provisions as specified in the federal HIE funding opportunity announcement. The privacy and security provisions are as follows: (Listed below in blue italic).

- *ARRA specific privacy and security provisions related to security breach restrictions and disclosures, sales of health information, consumer access, business associate obligations and agreements*
- *HIPAA Privacy Rule for permitted uses and disclosures and individual rights related to protected health information.*
- *HIPAA Security Rule for administrative, technical, and physical security procedures,*
- *Confidentiality of Alcohol and Drug Abuse Patient Records Regulations for substance abuse treatment programs.*
- *HHS Privacy and Security Framework for a single consistent approach to address the privacy and security challenges related to electronic health information exchange.*
- *various 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.*
- *The NHIN Cooperative Technical and Security Committee recommendations (example provided below)*
- HITSAC recommends the COV-HIE adhere to all applicable Commonwealth of Virginia laws concerning security and privacy.
- The Commonwealth's funding opportunity should specify Virginia's involvement in the The Health Information Security and Privacy Collaboration (HISPC). Link to HISPC information - http://healthit.hhs.gov/portal/server.pt?open=512&objID=1240&parentname=CommunityPage&parentid=2&mode=2

Exhibit C from the funding opportunity announcement provides the links and references for these provisions. The COV-HIE will provide services for user identity management, user authentication and authorization, access control based on user role as well as individual patient permissions, credential services and access levels for all users connected directly and through other HIEs to the COV-HIE, audit logging of all services, digital certificates and certificate revocation, and comply with data integrity and availability standards. Security and Privacy standards will be monitored for ongoing requirements as these provisions continue to evolve.

As an example, for the NHIN, the NHIN Cooperative Technical and Security Committee has defined a common security header for all transactions on the NHIN. This security header, as defined in the NHIN Trial Implementations Authorization Framework specification, requires the use of the Secure Access Markup Language (SAML) version 2. This specification requires inclusion of information about the user that is originating the transaction. The following identity attributes about the requester must be present:

1. User ID

DRAFT

2. The method by which the user was authenticated
3. The time of the user authentication
4. The user's name in plain text (for audit purposes)
5. The user's organization in plain text (for audit purposes)
6. The role that the user is assuming when making the request, using a coded vocabulary defined in the specification
7. The purpose of the request, using a coded vocabulary defined in the specification

These assertions about the originating user are included in the security header, and digitally signed using an X.509 certificate from an authority designated by the NHIN. This digital certificate from a trusted authority provides a "chain of trust" that allows the receiving HIE to trust that the originating user is the user described in the security header. The receiving HIE can then apply certain types of security, such as role-based access control and auditing of transactions, even though the HIE was not previously aware of the user.

HITSAC Recommends:

- HITSAC recommends the COV-HIE adopt the HITSP specifications for privacy and security, when issued by ONC.

HITSAC Governance Recommendations:

- HITSAC recommends all institutions participating in the COV-HIE prove to the organization that governs the COV-HIE their ability to audit transactions and uphold policies ensuring data privacy and security.
- HITSAC recommends the COV-HIE employ authentication and audit policies of the Health Information Security and Privacy Collaborative (HISPC).
- HITSAC recommends where two or more privacy and security standards conflict, the COV-HIE adopt the standards that are more protective of patient privacy.

HITSAC expects HITSP specifications to address, at a minimum, the points listed below:

1. Establishment of one or more "identity providers" who are allowed to create user IDs and assign them to users.
2. The definition of identity attributes, including the user's name and the role or roles they are allowed to assume in the systems being connected.
3. User account management and provisioning, the processes by which user accounts are created and information about those accounts is sent to connected systems.
4. Establishment of a "chain of trust," enforced through digital certificates that describe the level of trust that organizations give each other when accepting user credentials from outside their own security domain.
5. HITSAC expects HITSP will create and extend specifications concerning how patients exert control over who can access their health care information and for what purpose. Current Capabilities include:
    a. HITSP CAP 138 addresses interoperability requirements to support 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.
    b. HITSP CAP 143 addresses managing Consumer Preference and Consents. Another consideration is the enabling of how consumers/patients exert control over who may access their health care information and for what purpose.

3. Patient Identification

DRAFT

Positive patient identification is a challenge for every health care organization, and will be a key success factor for the COV-HIE. Patients must be identified uniquely using given characteristics such as name, date of birth, driver's license number, etc. Non health care industries utilize extensive probabilistic methods to determine user identification. Analysis of how these techniques could be used in health care needs to occur.

HITSAC Recommends:

- HITSAC recommends the COV-HIE adopt the HITSP Capabilities for patient identification when issued by ONC.

HITSAC Notes:

- HITSAC acknowledges there are widely accepted standards for exchanging information about patient IDs - the Patient Identity Cross-Reference (PIX) and the Patient Demographic Query (PDQ) profiles defined by Integrating the Health Care Enterprise (IHE).

4. Network

HITSAC Recommends:

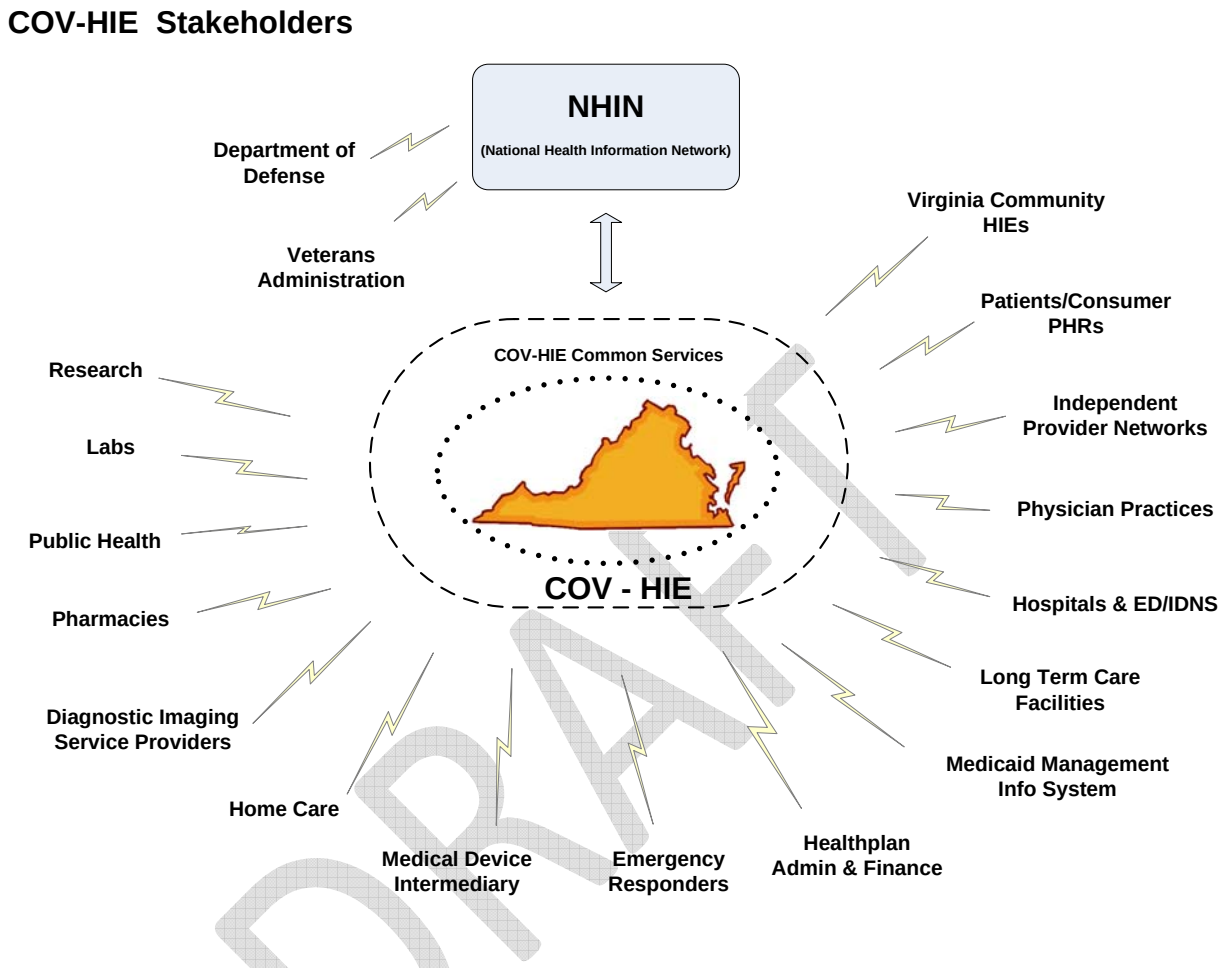
- HITSAC recommends clinical patient data be stored on the edge servers in the Continuity of Care Document (CCD) format, as currently endorsed by HITSP.
- HITSAC recommends the COV-HIE follow the HITSP interoperability specifications to determine the duration of data storage.

  In this way, the COV-HIE is independent of the proprietary designs of electronic medical record vendors and can still exchange pertinent data about patients among those various EMR systems used by providers. By copying data from a standard format to a separate edge server performance (speed) can be better assured since external inquiries are not competing for computing processors on the providers host system.

- HITSAC recommends the COV-HIE provide a NHIN Gateway Function.

DRAFT

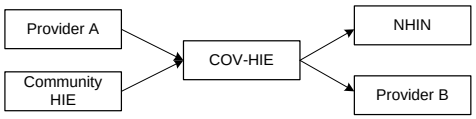
The following diagram provides a high level overview of the required connectivity.



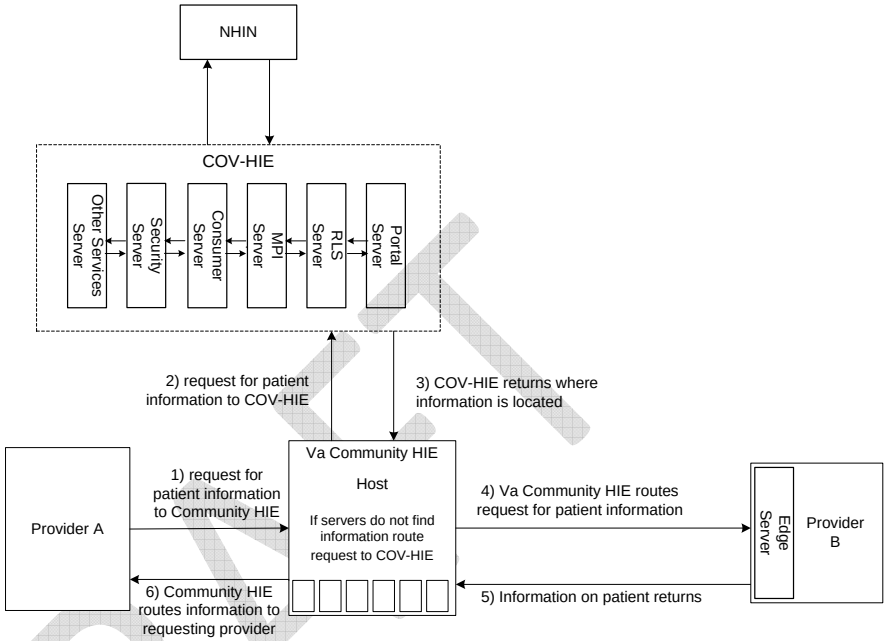
Nodes directly managed by the COV include the COV-HIE, the Medicaid Management Information System, and various public health entities. Center for Medicare and Medicaid Services (CMS) is currently designing a set of architectures (business, information and technical) for the future Medicaid Management Information Systems (MMIS). The overriding architecture for these systems is called MITA (Medicaid Information Technology Architecture). The MITA initiative envisions moving from traditional MMIS to web based, patient centric systems that are interoperable within and across all levels of government. CMS has been working on MITA for approximately 5 years, and is it estimated it will take another 5 to 10 years to arrive at a fully implemented and interoperable system.

There are many message flows that are possible between the COV-HIE nodes. The following table illustrates sample logical message flows in the node architecture.

A High Logical Flow



COV-HIE Sample Logical Message Flow
for Provider requests for clinical information routed through COV-HIE



5. Architectural Models for Data and Centralized Services

The COV-HIE will provide: Security Service, Patient Locator Service, Data/Document Locator Service, and Terminology Service. These technical services may be developed over time and according to standards and certification criteria adopted by HHS in effort to develop capacity for nationwide HIE.

There are three architectural models for data storage and services in an HIE. They are:

- Centralized – Population data would be intermingled on a single statewide HIE data storage center for query. The requestor must identify the patient, query the system for data on the patient, and assemble the returned information display.

- Federated – Population data would reside in individual health system databases and applications, and would be made available via real time queries. The requestor must identify the patient, query the state HIE for location of records on the patient (RLS), query the source systems for data on the patient, and assemble the returned information for display.

- Confederated or hybrid – The HIE provides a Patient Locator Service and a Record Locator Service. Population data would be hosted on participant's edge servers for real time data query. The requestor must identify the patient, query the state HIE for location of records on the patient (RLS), query the participants edge servers for data on the patient, and assemble the returned information for display.

DRAFT

HITSAC Recommends:

- HITSAC recommends the COV-HIE provide, at a minimum, Security Services, Patient Locator Services, Data/Document Locator Services, and Terminology Services, as defined by HITSP.
- HITSAC recommends the 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 sentence describes the "hybrid" logical architecture.

  This architecture would work cooperatively through the adoption of interoperability industry standards to include specifications from HITSP that use standards from HL7, ACR/NEMA(DICOM), ASTM, IEEE, NCPDP, ADA, etc. The utility services provided by the COV-HIE will be managed by the public-private partnership with the utmost security and privacy and made available to providers of health care services with permission of their patients.

- HITSAC recommends implemented solutions provide data synchronization from provider systems daily. The COV-HIE provides high availability with redundancy and fail-over to achieve 24 by 7 by 365 service levels.

- HITSAC will recommend operational service level requirements.

6. Coded Health Care Vocabularies

HITSAC Recommends:

- HITSAC recommends the COV-HIE adhere to the set of coded health care terminologies defined by the Federal Health Architecture (FHA).

DRAFT

Exhibit A - 2009 PQRI

Hospital Quality Alliance — Reporting Hospital Quality Data for Annual Payment Update

Inpatient Hospital Quality Measures
(Data Submission and Hospital Compare Details for Calendar Year 2009 Discharges)

The purpose of this document is to provide a reference guide on submission and Hospital Compare details for Quality Improvement Organizations (QIOs) and Providers for the National Quality Inpatient Measures.

All **measure sets** (AMI, PN, HF, SCIP, CAC and PR) contained in the *Specifications Manual for National Hospital Quality Inpatient Measures* are listed.

The first column contains the **Measure Identifier** followed by the **Measure Title.**

When required submission began — **Who data is collected for:** — **If/when measure is displayed on Hospital Compare Website:**

Inpatient Hospital Quality Measures		*Required Submission	Collected For:	**Hospital Compare Scheduled Release			
				Mar-09	Jun-09	Sep-09	Dec-09
Acute Myocardial Infarction (AMI)							
AMI-1	Aspirin at Arrival [1]	11/2003	CMS/TJC	✓	✓	✓	✓
AMI-2	Aspirin Prescribed at Discharge	11/2003	CMS/TJC	✓	✓	✓	✓
AMI-3	ACEI or ARB for LVSD [1]	11/2003	CMS/TJC	✓	✓	✓	✓
AMI-4	Adult Smoking Cessation Advice/Counseling [2]	3Q 2006	CMS/TJC	✓	✓	✓	✓
AMI-5	Beta-Blocker Prescribed at Discharge [1]	11/2003	CMS/TJC	✓	✓	✓	✓

A **footnote** has been added to designate when measures became part of the Reporting Hospital Quality Data for Annual Payment Update (RHQDAPU) program.
A table has been included at the bottom of the final page to further explain the footnotes.

Reporting Hospital Quality Data for Annual Payment Update (RHQDAPU) Measures
[1] Measure included in '10 measure starter set'
[2] Additional measure added to original '10 measure starter set' to make '21 measure expanded set' (CMS Reg. 1488-FC, posted 08/2006)
[3] Measure finalized in CY 2007 OPPS Final Rule (CMS Regulation 1506–FC, posted 11/2006)
[4] Measure finalized in FY 2008 IPPS Final Rule (CMS Regulation 1533-FC, posted 08/2007)
[5] Measure finalized in CY 2008 OPPS Final Rule (CMS Regulation 1392-FC, posted 11/2007)
[6] Measure finalized in CY 2009 IPPS Final Rule (CMS Regulation 1390-F, posted 8/2008)
[7] Measure finalized in CY 2009 OPPS Final Rule (CMS Regulation 1404-FC, posted 10/2008)

Revised 4/2/2009 — Page 1 of 6

Hospital Quality Alliance — Reporting Hospital Quality Data for Annual Payment Update

Inpatient Hospital Quality Measures

(Data Submission and Hospital Compare Details for Calendar Year 2009 Discharges)

Inpatient Hospital Quality Measures		*Required Submission	Collected For:	**Hospital Compare Scheduled Release			
				Mar-09	Jun-09	Sep-09	Dec-09
MEASURES REQUIRING ABSTRACTION AND/OR ACTION BY THE HOSPITAL							
Acute Myocardial Infarction (AMI)							
AMI-1	Aspirin at Arrival [1]	11/2003	CMS/TJC	✓	✓	✓	✓
AMI-2	Aspirin Prescribed at Discharge [1]	11/2003	CMS/TJC	✓	✓	✓	✓
AMI-3	ACEI or ARB for LVSD [1]	11/2003	CMS/TJC	✓	✓	✓	✓
AMI-4	Adult Smoking Cessation Advice/Counseling [2]	3Q 2006	CMS/TJC	✓	✓	✓	✓
AMI-5	Beta-Blocker Prescribed at Discharge [1]	11/2003	CMS/TJC	✓	✓	✓	✓
AMI-6	Beta-Blocker at Arrival [1] (Collection not required for CMS RHQDAPU participation beginning 2Q 2009 discharges, Measure will retire effective 2Q 2009 and will be rejected from QIO Clinical Warehouse if submitted.)	11/2003 Retired 2Q 2009	CMS/TJC				
AMI-7	Median Time to Fibrinolysis	N/A	CMS/TJC				
AMI-7a	Fibrinolytic Therapy Received Within 30 Minutes of Hospital Arrival [2]	3Q 2006	CMS/TJC	✓	✓	✓	✓
AMI-8	Median Time to Primary PCI	N/A	CMS/TJC				
AMI-8a	Primary PCI Received Within 90 Minutes of Hospital Arrival [2] [effective 1Q 2009 name changes to: Timing of Receipt of Primary Percutaneous Coronary Intervention (PCI)]	3Q 2006	CMS/TJC	✓	✓	✓	✓
AMI-9	Inpatient Mortality	N/A	TJC				
AMI-T1a	LDL Cholesterol Assessment **(OPTIONAL TEST MEASURE)**	N/A	CMS				
AMI-T2	Lipid Lowering Therapy at Discharge **(OPTIONAL TEST MEASURE)**	N/A	CMS				
Heart Failure (HF)							
HF-1	Discharge Instructions[2]	3Q 2006	CMS/TJC	✓	✓	✓	✓
HF-2	Evaluation of LVS Function[1]	11/2003	CMS/TJC	✓	✓	✓	✓
HF-3	ACEI or ARB for LVSD[1]	11/2003	CMS/TJC	✓	✓	✓	✓
HF-4	Adult Smoking Cessation Advice/Counseling[2]	3Q 2006	CMS/TJC	✓	✓	✓	✓
Pneumonia (PN)							
PN-1	Oxygenation Assessment[1, 6] (Collection not required for CMS RHQDAPU participation effective 1Q 2009, Measure will retire effective 2Q 2009 and will be rejected from QIO Clinical Warehouse if submitted)	11/2003 Retired 1Q 2009	CMS/TJC	✓	✓	✓	✓
PN-2	Pneumococcal Vaccination[1]	11/2003	CMS/TJC	✓	✓	✓	✓
PN-3a	Blood Cultures Performed Within 24 Hours Prior to or 24 Hours After Hospital Arrival for Patients Who Were Transferred or Admitted to the ICU Within 24 Hours of Hospital Arrival	N/A	CMS/TJC				

Revised 4/2/2009

Page 2 of 6

Hospital Quality Alliance — Reporting Hospital Quality Data for Annual Payment Update

Inpatient Hospital Quality Measures
(Data Submission and Hospital Compare Details for Calendar Year 2009 Discharges)

Inpatient Hospital Quality Measures		*Required Submission	Collected For:	**Hospital Compare Scheduled Release			
				Mar-09	Jun-09	Sep-09	Dec-09
Pneumonia (PN) continued							
PN-3b	Blood Cultures Performed in the Emergency Department Prior to Initial Antibiotic Received in Hospital[2]	3Q 2006	CMS/TJC	✓	✓	✓	✓
PN-4	Adult Smoking Cessation Advice/Counseling[2]	3Q 2006	CMS/TJC	✓	✓	✓	✓
PN-5	Antibiotic Timing (Median)	N/A	TJC				
PN-5b	Initial Antibiotic Received Within 4 Hours of Hospital Arrival[1, 6] (Submission required for RHQDAPU through 4Q 2008)	11/2003 Discontinued 1Q 2009	CMS/TJC				
PN-5c	Initial Antibiotic Received Within 6 Hours of Hospital Arrival[6] (Hospital Compare data displays PN-5c calculated from PN-5b data elements until 1Q 2009. The measure name changes to: Timing of Receipt of Initial Antibiotic Following Hospital Arrival)	1Q 2009	CMS/TJC	✓	✓	✓	✓
PN-6	Initial Antibiotic Selection for CAP in Immunocompetent Patients[2]	3Q 2006	CMS	✓	✓	✓	✓
PN-6a	Initial Antibiotic Selection for CAP in Immunocompetent – ICU Patients	N/A	TJC				
PN-6b	Initial Antibiotic Selection for CAP in Immunocompetent – Non–ICU Patients	N/A	TJC				
PN-7	Influenza Vaccination[2] **(NOTE: Reported by Flu Season ONLY)**	3Q 2006	CMS/TJC	✓	✓	✓	✓
Surgical Care Improvement Project (SCIP)							
SCIP-Inf-1	Prophylactic Antibiotic Received Within One Hour Prior to Surgical Incision[2]	3Q 2006	CMS/TJC	✓	✓	✓	✓
SCIP-Inf-2	Prophylactic Antibiotic Selection for Surgical Patients[3]	1Q 2007	CMS/TJC	✓	✓	✓	✓
SCIP-Inf-3	Prophylactic Antibiotics Discontinued Within 24 Hours After Surgery End Time[2]	3Q 2006	CMS/TJC	✓	✓	✓	✓
SCIP-Inf-4	Cardiac Surgery Patients With Controlled 6 A.M. Postoperative Blood Glucose[5]	1Q 2008	CMS/TJC	✓	✓	✓	✓
SCIP-Inf-6	Surgery Patients with Appropriate Hair Removal[5]	1Q 2008	CMS/TJC	✓	✓	✓	✓
SCIP-Inf-7	Colorectal Surgery Patients with Immediate Postoperative Normothermia (Data collection will be discontinued effective 4Q 2009)	N/A	CMS/TJC				
SCIP-Inf-9	Urinary Catheter Removed on Postoperative Day 1 (POD 1) or Postoperative Day 2 (POD 2) with Day of Surgery being Day Zero	N/A	CMS/TJC				
SCIP-Inf-10	Surgery Patients with Perioperative Temperature Management	N/A	CMS/TJC				
SCIP-VTE-1	Surgery Patients with Recommended Venous Thromboembolism Prophylaxis Ordered[3]	1Q 2007	CMS/TJC	✓	✓	✓	✓
SCIP-VTE-2	Surgery Patients Who Received Appropriate Venous Thromboembolism Prophylaxis Within 24 Hours Prior to Surgery to 24 Hours After Surgery[3]	1Q 2007	CMS/TJC	✓	✓	✓	✓
SCIP-Card-2	Surgery Patients on Beta-Blocker Therapy Prior to Arrival Who received a Beta-Blocker During the Perioperative Period[6]	1Q 2009	CMS/TJC				✓

Hospital Quality Alliance — Reporting Hospital Quality Data for Annual Payment Update

Inpatient Hospital Quality Measures
(Data Submission and Hospital Compare Details for Calendar Year 2009 Discharges)

Inpatient Hospital Quality Measures	*Required Submission	Collected For:	**Hospital Compare Scheduled Release			
			Mar-09	Jun-09	Sep-09	Dec-09
Children's Asthma Care (CAC)**						
CAC-1 Relievers for Inpatient Asthma	N/A	TJC	✓	✓	✓	✓
CAC-2 Systemic Corticosteroids for Inpatient Asthma	N/A	TJC	✓	✓	✓	✓
CAC-3 Home Management Plan of Care (HMPC) Document Given to Patient/Caregiver	N/A	TJC			✓	✓
Pregnancy and Related Conditions (PR)						
PR-1 VBAC	N/A	TJC				
PR-2 Inpatient Neonatal Mortality	N/A	TJC				
PR-3 Third or Fourth Degree Laceration	N/A	TJC				
Hospital Consumer Assessment of Healthcare Providers and System Survey (HCAHPS)**						
HCAHPS Hospital Consumer Assessment of Healthcare Providers and System Survey [3]	3Q 2007	CMS	✓	✓	✓	✓
Cardiac Surgery Measure						
Participation in a Systematic Database for Cardiac Surgery[6] (Provider must enter response on QualityNet)	7/1/2009 thru 8/15/2009	CMS				TBD
MEASURE INFORMATION OBTAINED FROM CLAIMS-BASED DATA						
30-Day Risk-Standardized Mortality Rates***						
MORT-30-AMI Acute Myocardial Infarction (AMI) 30-Day Mortality Rate [3]	N/A^	CMS	✓	✓	✓	✓
MORT-30-HF Heart Failure (HF) 30-Day Mortality Rate [3]	N/A^	CMS	✓	✓	✓	✓
MORT-30-PN Pneumonia (PN) 30-Day Mortality Rate [4]	N/A^	CMS	✓	✓	✓	✓
30-Day Risk-Standardized Readmission Rates***						
READM-30-AMI Acute Myocardial Infarction (AMI) 30-Day Readmission Rate [7]	N/A^	CMS		✓	✓	✓
READM-30-HF Heart Failure (HF) 30-Day Readmission Rate[6]	N/A^	CMS		✓	✓	✓
READM-30-PN Pneumonia (PN) 30-Day Readmission Rate[7]	N/A^	CMS		✓	✓	✓
Agency for Healthcare Research and Quality (AHRQ)Measures***						
Patient Safety Indicators						
PSI 4 Death Among Surgical Patients with Treatable Serious Complications[6]	N/A^	CMS				✓
PSI 6 Iatrogenic Pneumothorax, Adult[6]	N/A^	CMS				✓
PSI 14 Postoperative Wound Dehiscence[6]	N/A^	CMS				✓
PSI 15 Accidental Puncture or Laceration[6]	N/A^	CMS				✓
PSI Complication/Patient Safety for Selected Indicators (composite)[6]	N/A^	CMS				✓

Revised 4/2/2009

Page 4 of 6

Inpatient Hospital Quality Measures
(Data Submission and Hospital Compare Details for Calendar Year 2009 Discharges)

Inpatient Hospital Quality Measures	*Required Submission	Collected For:	**Hospital Compare Scheduled Release			
			Mar-09	Jun-09	Sep-09	Dec-09
Agency for Healthcare Research and Quality (AHRQ)Measures continued* **						
Inpatient Quality Indicators						
IQI 11 Abdominal Aortic Aneurysm (AAA) Mortality Rate[6]	N/A^	CMS				✓
IQI 19 Hip Fracture Morality Rate[6]	N/A^	CMS				✓
IQI Mortality for Selected Surgical Procedures (composite)[6]	N/A^	CMS				✓
IQI Mortality for Selected Medical Conditions (composite)[6]	N/A^	CMS				✓
Nursing Sensitive Measure* **						
NSC-1 Death Among Surgical Patients with Treatable Serious complications[6]	N/A^	CMS				TBD

LEGEND and FOOTNOTES:

All dates and quarters referenced refer to Calendar Year (CY) unless otherwise indicated (for example 1Q 2009 would represent discharges Jan-Mar 2009)

CMS = Centers for Medicare & Medicaid Services
IPPS = Inpatient Prospective Payment System
IQI = Inpatient Quality Indicator
OPPS = Outpatient Prospective Payment System
PSI = Patient Safety Indicator
TJC = The Joint Commission
TBD = To Be Determined
✓ = Displayed on 'Hospital Compare' website
▨ = Not applicable for the measure in that discharge timeframe

Reporting Hospital Quality Data for Annual Payment Update (RHQDAPU) Measures
[1] Measure included in '10 measure starter set'
[2] Additional measure added to original '10 measure starter set' to make '21 measure expanded set' (CMS Reg. 1488-FC, posted 08/2006)
[3] Measure finalized in CY 2007 OPPS Final Rule (CMS Regulation 1506–FC, posted 11/2006)
[4] Measure finalized in FY 2008 IPPS Final Rule (CMS Regulation 1533-FC, posted 08/2007)
[5] Measure finalized in CY 2008 OPPS Final Rule (CMS Regulation 1392-FC, posted 11/2007)
[6] Measure finalized in CY 2009 IPPS Final Rule (CMS Regulation 1390-F, posted 8/2008)
[7] Measure finalized in CY 2009 OPPS Final Rule (CMS Regulation 1404-FC, posted 10/2008)
^ CMS uses enrollment data as well as Part A and Part B claims for Medicare fee-for-service patients to calculate these measures. No hospital data submission is required to calculate these measure rates.

* Discharge (D/C) Quarter Required RHQDAPU Submission Started In Accordance with the Published Final Rule (IPPS and/or OPPS)

Revised 4/2/2009

Page 5 of 6

Reporting Hospital Quality Data for Annual Payment Update

Hospital Quality Alliance

Inpatient Hospital Quality Measures
(Data Submission and Hospital Compare Details for Calendar Year 2009 Discharges)

LEGEND and FOOTNOTES (continued):

** Clinical Process Measures, CAC Measures and HCAHPS Discharge Quarters Included in Hospital Compare Release (refreshed quarterly)
Mar-09: 3Q07, 4Q07, 1Q08 and 2Q08
Jun-09: 4Q07, 1Q08, 2Q08 and 3Q08
Sep-09: 1Q08, 2Q08, 3Q08 and 4Q08
Dec-09: 2Q08, 3Q08, 4Q08 and 1Q09

***Claims-based Measures (no data submission required) Refreshed annually on Hospital Compare
Mar-09: 3Q 2006 through 2Q 2007
Jun-09: 3Q 2005 through 2Q 2008
Sep-09: 3Q 2005 through 2Q 2008
Dec-09: 3Q 2005 through 2Q 2008 (Time span for AHRQ measures has not been determined)

This material was prepared by IFMC, the Quality Improvement Organization Support Contractor for the Hospital Reporting Program, under contract with the Centers for Medicare & Medicaid Services (CMS), an agency of the U.S. Department of Health and Human Services. 9SoW-IA-HRPQIOSC-03/09-005

Exhibit B - Summary of HITSP Capabilities

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.

DRAFT

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
Communicante 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.

DRAFT

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 3

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.

DRAFT

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.

DRAFT

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.

DRAFT

The following table shows the drill down of HITSP Capability 119. Capability 119 Communicate Structured Documentation is made up of several use cases or eleven Interoperability Specification. These are: 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.

One of the significant barriers to health care interoperability is the variety and complexity of standards to implement. HITSP has mapped the standards for health care interoperability to provide a "roadmap", but there is still a significant effort to understand, plan, and program EHR's for implementation. The lack of user friendly tools and trained informaticists could delay standards adoption.

DRAFT

Exhibit C: HITSP Capabilities Mapped to Interoperability Specifications HITSP has then taken the Capabilities, and Mapped them to the Interoperability Specifications. The following IS Table 5-1 from the HITSP EHR-Centric Interoperability Specification.

Table 5-1 HITSP Capabilities Mapped to Interoperability Specifications

HITSP Capabilities																											Supporting Components of the HITSP Interoperability Specifications IHE profiles shown when relevant to the specified HITSP component
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	
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				CLINICAL OPERATIONS (Care Delivery, Emergency Responder and Consumer Empowerment)												CLINICAL QUALITY AND PUBLIC HEALTH											
				Medication Management		Exchange of Clinical Data							Exchange of Laboratory and Imaging Data			Quality Management		Immunization			Case Reporting and Bio-surveillance				Emergency		
																											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

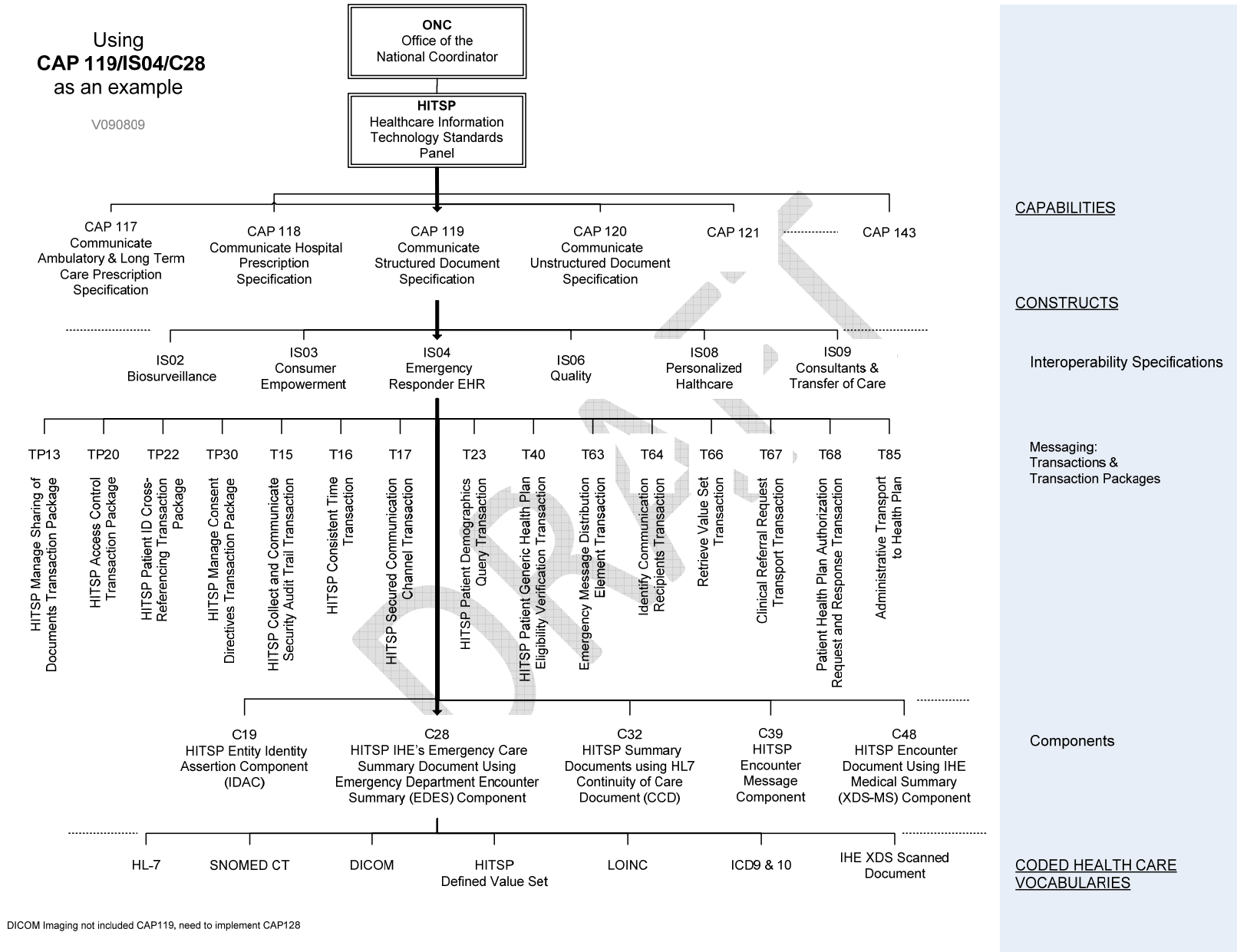

Using
CAP 119/IS04/C28
as an example
V090809
ONC
Office of the
National Coordinator
HITSP
Healthcare Information
Technology Standards
Panel
CAP 117
Communicate
Ambulatory & Long Term
Care Prescription
Specification
CAP 118
Communicate Hospital
Prescription
Specification
CAP 119
Communicate
Structured Document
Specification
CAP 120
Communicate
Unstructured Document
Specification
CAP 121
CAP 143
CAPABILITIES
CONSTRUCTS
IS02
Biosurveillance
IS03
Consumer
Empowerment
IS04
Emergency
Responder EHR
IS06
Quality
IS08
Personalized
Halthcare
IS09
Consultants &
Transfer of Care
Interoperability Specifications
TP13
HITSP Manage Sharing of Documents Transaction Package
TP20
HITSP Access Control Transaction Package
TP22
HITSP Patient ID Cross-Referencing Transaction Package
TP30
HITSP Manage Consent Directives Transaction Package
T15
HITSP Collect and Communicate Security Audit Trail Transaction
T16
HITSP Consistent Time Transaction
T17
HITSP Secured Communication Channel Transaction
T23
HITSP Patient Demographics Query Transaction
T40
HITSP Patient Generic Health Plan Eligibility Verification Transaction
T63
Emergency Message Distribution Element Transaction
T64
Identify Communication Recipients Transaction
T66
Retrieve Value Set Transaction
T67
Clinical Referral Request Transport Transaction
T68
Patient Health Plan Authorization Request and Response Transaction
T85
Administrative Transport to Health Plan
Messaging:
Transactions &
Transaction Packages
C19
HITSP Entity Identity
Assertion Component
(IDAC)
C28
HITSP IHE's Emergency Care
Summary Document Using
Emergency Department Encounter
Summary (EDES) Component
C32
HITSP Summary
Documents using HL7
Continuity of Care
Document (CCD)
C39
HITSP
Encounter
Message
Component
C48
HITSP Encounter
Document Using IHE
Medical Summary
(XDS-MS) Component
Components
HL-7
SNOMED CT
DICOM
HITSP
Defined Value Set
LOINC
ICD9 & 10
IHE XDS Scanned
Document
CODED HEALTH CARE
VOCABULARIES
DICOM Imaging not included CAP119, need to implement CAP128

Exhibit E - 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 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 assisted" 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

DRAFT

- 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. To read a full version of ARRA, click here.

Privacy Act of 1974

- 45.C.F.R. 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 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.

DRAFT

- 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, please visit healthit.hhs.gov and click on the Privacy and Security link for the Framework and its Principles.

DRAFT