COV-HIE
Technical Infrastructure

Draft 2 – September 25, 2009

Version 5

DRAFT

COV-HIE Technical Infrastructure

Table of Contents

Introduction.....Page 5

Current State .....Page 6

Proposed Project Summary .....Page 7

HITSP Interoperability Standards .....Page 7

Privacy & Security .....Page 8

Patient Identification .....Page 10

Network .....Page 10

Architectural Models .....Page 13

Barriers .....Page 14

Coded Healthcare Vocabularies .....Page 14

Exhibits .....Page 15

A: 2009 PQRI .....Page 17

B: Summary of HITSP Capabilities.....Page 23

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

DRAFT

COV-HIE Technical Infrastructure Domain

I. Introduction:

This draft white paper is designed to highlight possible standards for adoption during the planning phase for the COV-HIE's Technical Infrastructure HIE funding proposal. The green text is excerpts from Dr. Ruffin's early guidance to HITSAC. The blue text is copied from the grant announcement as a framework: 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. Using the grant format as a framework will facilitate and expedite subsequent incorporations as appropriate into the funding proposal. This white paper does not address the reasons/benefits of an HIE. Of the five domains noted in the grant announcement, this white paper addresses one domain, Technical Infrastructure and does not address the other four domains of Governance, Finance, Business and Technical Operations, and Legal/policy.

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

- 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

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.

II. Current State:

- Discuss and determine the current status of the state's progress in achieving statewide HIE among healthcare 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 healthcare convened by the Virginia Association of Health Plans (VHAP), the Virginia Hospital and Healthcare 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. _____
  - Electronic public health reporting (immunizations, notifiable laboratory results). The COV utilizes a system known as the Virginia Immunization Information System (VIIS) to track immunizations. This application 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 xx current initiatives underway to provide Health Information Exchange. These include the VIIS immunization registry, VHEN for financial administrative transactions, Carespark, Med Virginia, and vendor enabled health information exchanges such as Epic.

DRAFT

III. 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 healthcare 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 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 Healthcare Vocabularies

HITSP needs to develop a crosswalk/roadmap between the seven components above and the 26 Capabilities.

1. HITSAC Recommends the adoption of HITSP Interoperability Standards for the COV-HIE

The Commonwealth recognizes the multiple stakeholders who would participate and receive benefit from a state wide HIE which connects to healthcare 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 grant.

1. Electronic eligibility and claims transactions: adherence to HITSP Capability 140 (communicate benefits and eligibility) and as well as x12 transaction standards.
2. Electronic prescribing and refill requests: Utilize an established eprescribing vendor to implement HITSP prescription related Capabilities 117 & 118.
3. Prescription fill status and/or medication fill history - see #2 above.
4. Clinical summary exchange for care coordination and patient engagement: Establish Capabilities 119 and 120 as the basis for interoperability of patient documentation (structured and unstructured). An example is Capability 119 'Communicate structured document specification for (IHE's) emergency care summary document' described in the COV-HIE Technical Infrastructure white paper on page 3. The remaining capabilities will need to be specified so the exchange of patient information can be harmonized via the HIE among agencies as well as healthcare providers utilizing the HIE to demonstrate Meaningful Use.
5. Quality Reporting: Establish Capability 130.
6. Electronic public health reporting: Establish Interoperability Specification 11.
7. Electronic clinical laboratory ordering and results delivery: Establish Capabilities 126 & 127.

During implementation planning, performance measures will need to be identified to show the degree of provider, payer, public health, pharmacy, clinical laboratory, and other stake holder participation in the COV- HIE enabled state level technical services. For example, one measure would be the percent of pharmacies serving people within the state that are actively utilizing the electronic prescribing and refill requests. Need to figure out how to measure compliance.

2. HITSAC Recommends the adoption of Privacy and Security Standards for the COV-HIE

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 the incorporation of the privacy and security provisions of the following:

- 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)
- All applicable COV laws concerning security and privacy
- Grant application should mention VA's involvement in the The Health Information Security and Privacy Collaboration (HITSPC) 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 over time.

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
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.

In addition, HITSAC recommends that the COV-HIE accomplish the following:

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.

Another consideration is the enabling of how consumers/patients exert control over who may access their healthcare information and for what purpose. The standards to exchange access consent policies between an EHR and HIE are not yet mature. HITSP CAP 138 does address 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.

3. HITSAC recommendation for Patient Identification

Positive patient identification is a challenge for every healthcare 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 healthcare 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 that the COV-HIE create and maintain a Master Person Index (eMPI). This will serve to uniquely identify every person whose health care data and person data must be matched reliably between providers of care. Patients will have access to these utility services to obtain and review their own health care data from participating providers. The utility service for eMPI will centralize only identifying information about patients and the location of records. The clinical data themselves will remain on the computers of the providers and patients themselves.

Need to identify how within HITSP Capabilities patient identification is managed to verify it confirms this HL7 utilization : The widely accepted standard for exchanging information about patient IDs are the Patient Identity Cross-Reference (PIX) and the Patient Demographic Query (PDQ) profiles defined by Integrating the Healthcare Enterprise (IHE). HITSP has developed a new IS package – John Quinn to send link.

These profiles describe the use of HL7 messages (with supported variations for both HL7 version 2 and version 3) to provide the operations necessary to manage patient IDs across organizations. The operations defined by PIX and PDQ are:

- Patient Identity Feed: used to inform another entity about a patient identity
- PIX Update Notification: used to inform another entity about changes to a patient identity
- PIX Query: used to query another entity about Patient IDs that are linked (that is, assumed to be the same individual) as a given Patient ID
- Patient Demographics Query: used to query another entity about individuals who have the same or similar attributes (such as name, date of birth, gender or address) as the given attributes.

4. HITSAC recommendation for Network Standards and Architecture

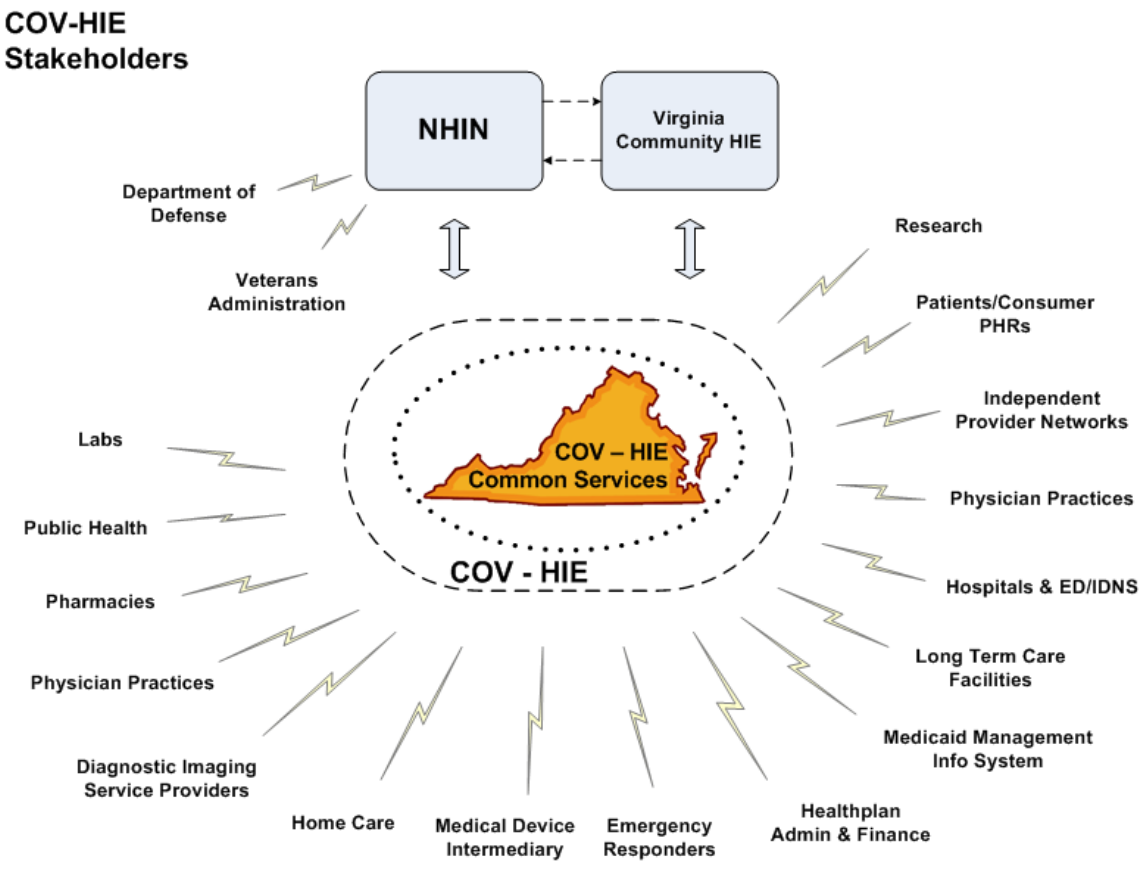
- The HIE grant application should reference the broadband initiatives in the Commonwealth.
- Recommendations for network standards and architecture should be vetted during the planning phase next year.

The first recommendation is that providers of health care services will maintain the patient clinical data for the COV-HIE on edge servers that are separate from, and updated daily by, the providers' electronic medical record transaction systems. 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.

The second recommendation is that the clinical data of patients, including demographic information such as name, address, age and birth date and medical information such as diagnosis codes, procedure codes, dates and times of service, medications, laboratory reports and textual content such as discharge summaries, radiology and pathology reports and operative reports, can be stored in HITSP and NHIN approved standard formats such as the Continuity of Care Document (CCD), which is an essential standard of the NHIN, and a Component of some HITSP Capabilities such as CAP 119. Providers' electronic medical record systems can update each patient's records in CCD format before transmitting those data, at the patient's request, to another provider of care.

The third recommendation is that the COV-HIE will require network connectivity to a variety of network "nodes". 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. 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.

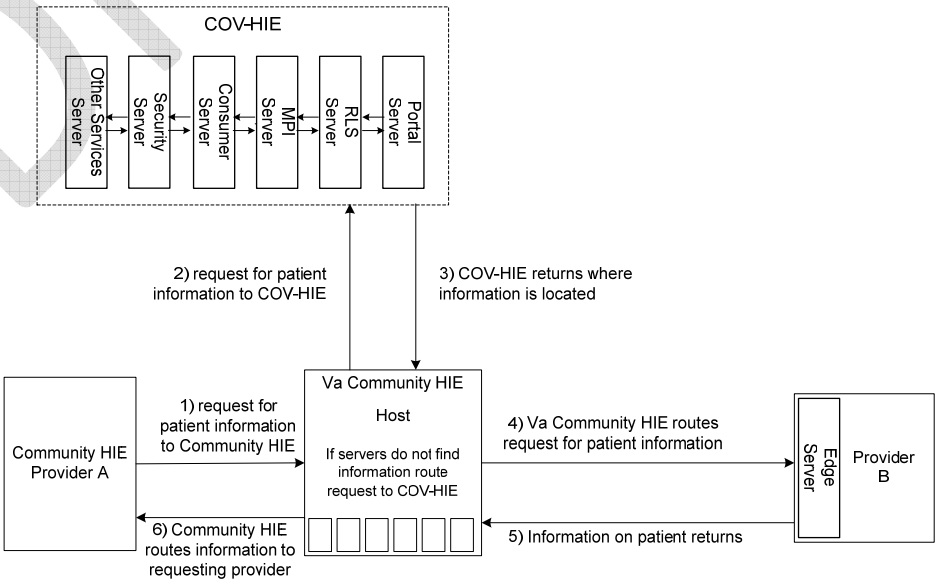
Large organizations of providers of health care services, such as the university medical centers, regional hospital systems and medical groups, share single electronic medical record systems now. These include VCUHS with Cerner, UVAHS soon to be with Epic, Inova Health System with General Electric, Carilion with Epic, Sentara with Epic, Bon Secours with Epic, Centra with McKesson, HCA with Meditech and federally qualified Community Health Centers with Eclinicalworks. These large systems will be able to extract clinical data in CCD format and store them on edge servers readily.

Community hospitals not part of a regional system, as they adopt electronic medical record systems that can produce data about their patients in CCD format, will invest in edge servers and populate them with CCD data. Medical and dental offices, as they adopt electronic medical record systems that can export data in CCD format, will populate their own edge servers with these data and connect them directly to the COV-HIE utility services (eMPI, RLS, eMPD) or they will connect through local or regional resource centers, operated by medical societies or regional hospital systems or entrepreneurial firms, that operate electronic medical record services as application services providers and maintain edge server banks for those providers.

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

A High Logical Flow

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



DRAFT

The fourth recommendation is that the COV-HIE will also provide an NHIN Gateway Function. If the Department of Health and Human Services Office of the National Coordinator for Healthcare IT (ONC) establishes standards that HIEs must meet to become and remain a Certified HIE, it will be the responsibility of the COV-HIE to conform to these standards. The VHIN would also provide the gateway for community HIE's to the NHIN as well as access from one community HIE to another. The Virginia recommended architecture and standards would need to be adopted by community HIE's in order to be a node on the VHIN.

One established standard from the NHIN Trial Implementation Framework has identified ten core service offerings[1]:

- Message Platform Service Interface Specification
- Authorization Framework Service Interface Specification
- Subject Discovery Service Interface Specification
- Query for Documents Service Interface Specification
- Document Retrieve Service Interface Specification
- Audit Log Query Service Interface Specification
- Consumer Preferences Service Interface Specification
- Health Information Event Messaging Service Interface Specification
- NHIE Service Registry Interface Specification
- Authorized Case Follow-Up Service Interface Specification

These services and others will be needed for a COV-HIE. Planning and implementation work would address and sequence all of the services needed.

[1] See NHIN Trial Implementations Service Interface Specifications (http://healthit.hhs.gov)

These core services support the fulfillment of the following use cases:

- Authorized Release of Information to a Trusted Entity Use Case
- Biosurveillance Use Case
- Consumer Preference Registration Med History
- EHR Lab Scenarios Use Case
- Emergency Responder Use Case
- Quality Use Case

HITSP has moved away from defining use cases and is focused on developing the 26 Capabilities. Use case terminology should not be mentioned in the grant application. The use cases above can be leveraged for testing the HIE.

5. Architectural Models for COV-HIE 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.

DRAFT

- 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 MPI (Master Patient Index) and RLS services as above. 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

HITSAC recommends a federated architecture for the COV HIE. The state will provide the Master Person Index (eMPI), a Master Provider Directory (eMPD) to identify uniquely every provider of health care services, and Record Locator Service (RLS)) to identify the locations of each person's clinical information among the electronic medical record systems of participating providers of care. Essentially, the COV-HIE would provide the "phone book" to provide an index for patients, providers, health plans, public health entities, research, etc. Entities which would utilize the State's central utility include both Hybrid community HIE's with centralized components e.g. VHEN for financial administrative data, and Federated/vendor solutions e.g. the State's Epic EMR Care Everywhere for State health system providers utilizing Epic. These architectures would work cooperatively through the adoption of interoperability industry standards to include standards from HL7, HITSP, 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 that the implemented solutions will enable synchronization of data from end user systems and the COV-HIE will be designed for high availability with redundancy and fail to achieve 24 by 7 by 365 service levels. Operational service level requirements must be addressed in the business and technical operations domain.

6. Barriers

a. Incomplete Broadband Access throughout the COV
b. Population identification and management
c. Lack of user tools to facilitate standards adoption
d. Lack of EHR automation within some stakeholders
e. Mapping of historical data to industry standard value sets
f. Lack of skilled/trained personnel to implement
g. Lack of funding
h. Training

7. Coded Healthcare Vocabularies

`

In addition to the standards needed to successfully implement an HIE, the HITSAC committee recommends coded healthcare vocabularies for statewide adoption. Data content standards, i.e., vocabularies and terminology standards include CDA2, SNOMED, ICD, X12, NCPDP, LOINC, Omaha

System, etc. The information content standards include the Reference Information Models (RIMs) standards.

Third party vendors today provide translation mappings for the healthcare vocabularies.

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

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

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

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. Healthcare 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, healthcare 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 healthcare 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

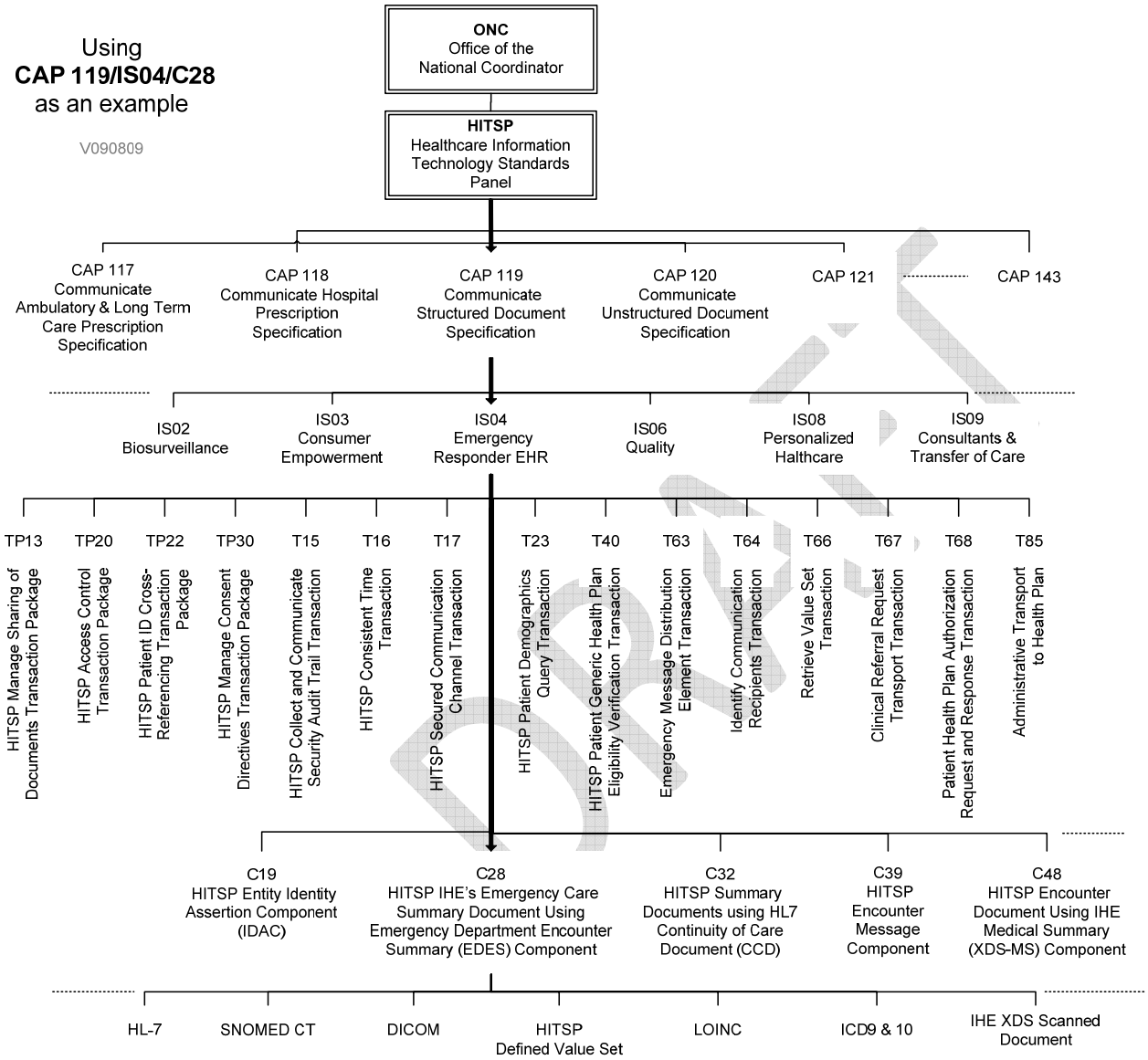
The following table shows the drill down of HITSP Capability 119. Capability 119 Communicate Structured Documentation is made up of several use cases or eleven Interoperability Specification. These are: IS 04 Emergency Responder Electronic Health Record; IS 08 Personalized Healthcare; IS 09 Consultations 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 healthcare interoperability is the variety and complexity of standards to implement. HITSP has mapped the standards for healthcare 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

Using
CAP 119/IS04/C28
as an example

V090809



CAPABILITIES

CONSTRUCTS

Interoperability Specifications

Messaging:
Transactions &
Transaction Packages

Components

CODED HEALTH CARE VOCABULARIES

DICOM Imaging not included CAP119, need to implement CAP128

Exhibit C - 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

DRAFT

- 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. 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.

DRAFT

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

DRAFT