California Health Information Exchange Operational Plan

March 31, 2010

Note: This document contains an *excerpt* of the complete CA HIE Strategic and Operational Plan. It is intended to highlight the Technical Infrastructure components of the plan. For a copy of the complete CA HIE Strategic and Operational Plan, as submitted to the Office of the National Coordinator, please see http://www.ehealth.ca.gov/eHealthPlan/tabid/72/Default.aspx (note that his is a large file that may take several minutes to load).

Table of Contents

1. Introduction

<Content omitted from this excerpted version>

2. Statewide HIE Planning

<Content omitted from this excerpted version>

3. Governance

<Content omitted from this excerpted version>

4. Landscape and Capacity Assessment

4.1 CA landscape: The Varied Characteristics of HIE Stakeholders and their Relationships

The basic EHR adoption rate among California providers ranks above the national estimate; yet the State has a long way to go before comprehensive adoption is realized.[1] A California Primary Care Association (CPCA) survey from August 2009 found that at least 20% of community clinics and health centers had and were actively using EHRs, another 10-20% was actively pursuing EHR adoption, and 30% intended to start pursuing an EHR when the incentive program begins. Similarly, among individual physicians, California physicians reported greater use of EHRs than the national average with 37% of physicians reporting EHR use in comparison to 28% nationally.[2] The majority of community clinics have some form of health IT in place, most commonly in the form of diabetes and immunization registries.

California's current HIE efforts fall broadly into two categories: (i) large health systems, affiliated providers and ancillary services implementing integrated EHRs, and (ii) community-driven efforts that aim to ensure ubiquitous availability of data within a region or across the State.

California's large, diverse health care delivery system is characterized by provider organizations of widely varying sizes, including very large (Kaiser-Permanente), large (Sharp Healthcare), medium-sized (Palo Alto Medical Foundation), and small (small and solo physician practices) providers. Outpatient providers in a community may be tightly integrated (e.g., via integrated delivery networks), loosely affiliated (e.g., in Integrated Practice Associations, or IPAs), or entirely independent. Hospitals may be part of regional, Statewide, or multi-State chains or they may be independent local facilities. Hospitals

[1] California Health Information Technology Study: Input to the California Health Data Exchange Roadmap, Accenture, January 2007. See http://www.hmohelp.ca.gov/library/reports/news/CA%20HIT%20Study%202007.pdf
[2] Ibid.

and community outpatient physicians may be tightly integrated in combined business entities (such as an Integrated Delivery Network, or IDN, like Kaiser-Permanente), or they may be related only by virtue of physician admitting privileges. Provider organizations that are part of larger commercial entities may be well-capitalized and capable of sophisticated infrastructure projects, whereas independent provider organizations or organizations treating underserved populations may be thinly capitalized and less able to develop and support complex infrastructures. In addition, the Veterans Administration, Department of Defense, and Indian Health Service also operate substantial facilities within the State.

With respect to ancillary services, large clinical laboratories with national data centers operate in California, as do smaller regional labs and local hospital labs. National pharmacy chains have facilities across the State, but small independent pharmacies also operate in their local communities. Imaging centers, urgent-care facilities, surgical centers, surgical hospitals, and dialysis centers are similarly diverse in their degree of "horizontal" integration (i.e., chains versus independents) and their degree of "vertical" integration (i.e., their business relationships with hospitals, community physicians, employer groups, and other entities).

Healthcare in California is funded through a similar mosaic of payment mechanisms. National, State-wide, and regional commercial insurers operate in California. State and local governments finance care for the underserved through a variety of mechanisms, including Medi-Cal (fee for service and managed care), Healthy Families, and the County Medical Service Program, as well as a separate mechanism for managing prisoner health. Medicare finances care for the elderly population. Insurance-payment models include network-based fee-for-service (Preferred Provider Organization, or PPO), network-based capitation (Health Maintenance Organization or HMO), and indemnity, as well as a wide variety of payments at facilities including percent of billed charges, case rates, per diem charges, and hospital capitation. Delegation of risk and other insurance functions via HMOs is more common in California than most other States. Medi-Cal and Medicare delegate risk and claims-payment functions to commercial insurance carriers through Medicare Advantage and other programs. Commercial insurers delegate risk and claims-payment functions to contracted IPAs or medical groups. IPAs delegate risk to their member providers.

A patient-centered health care system will necessitate HIE across all of these types of organizations, regardless of their sizes, relationships or existing HIT capabilities.

4.2 Gap Analysis for Achieving HIE in California: What's Currently Missing?

The relatively low penetration of EHRs in outpatient practices and hospitals is an obvious barrier to the achievement of HIE for meaningful use. However, in assessing the gaps in HIE capabilities required for meaningful use, the TAC and TWG anticipate that providers will be using certified EHRs or EHR modules, because otherwise they would not be eligible for meaningful use incentives.

The list below highlights some of the prominent gaps in HIE capabilities needed for meaningful use in 2011, as defined in the recently released NPRM and Interim Final Rule for Standards for Electronic Health Records (IFR):

- Between 50% and 60% of outpatient labs in California are performed by either LabCorp or Quest Diagnostics. The rest are performed by over 17,000 hospital, regional, public health and provider office labs, none of whom represent significant market share. Many of these hospital and regional labs are not prepared to send structured electronic lab results to outpatient physicians.

- There is no universally trusted framework for identity management and authentication of the principals participating in HIE transactions. Where trust relationships exist, they exist only (1) among principals within the same enterprise and (2) among principals in enterprises that have bi-lateral information-exchange agreements or (3) among principals in enterprises that participate in a regional HIO with a trusted identity-management framework.

- Many eligible professionals practicing in small provider organizations (including those with EHRs) lack the ability to provide patients' access to their health data through a "tethered" PHR (i.e., on that is tightly integrated with the organization's EHR).

- Many eligible professionals practicing in small provider organizations lack the ability to aggregate data sufficiently to generate patient lists or report ambulatory quality metrics from EHR to support the disease-management and quality measurement requirements of meaningful use.

- A majority of the state's immunization registries do not currently have the capacity to accept immunization data via HL7 messaging directly from EHRs.

- The California Department of Public Health's CalREDIE application for collecting reportable lab data (Electronic Laboratory Reporting) and reportable disease data (web-based Confidential Morbidity Reporting) is in pilot production and not yet operational statewide.

- Most provider organizations and ancillary organizations do not have technology in place on site or via external service providers or regional HIOs to generally participate in meaningful use.

- Some regions in the State continue to operate in an extremely competitive environment for healthcare services, limiting their ability or desire to cooperate in HIE activities.

4.2.1 Current HIE Capacity in California

California's existing infrastructure and available resources vary in stage of development achieved. In California, multiple uncoordinated HIE efforts have developed over the past 15 years as regional initiatives. Of these efforts, only three are exchanging clinical data today. The remaining efforts are focused primarily on organizing, fundraising, and piloting their solutions.

4.2.1.1 Regional HIOs

Currently, California has a small number of Health Information Organizations (HIOs) in several regions of the State (See Table 3). These efforts are at different stages of maturity and address various types of HIE goals. Although several are operational and provide valued services, none as yet encompass all of the health care organizations in its respective region, nor provides all of the HIE capabilities required to meet the meaningful use criteria. As these organizations further focus their efforts on supporting meaningful use goals, they will support HIE in their regions more extensively and perhaps expand as the demand for HIE across enterprises increases with the Medicare and Medi-Cal incentive programs. The technologies used in some of these HIOs may provide models or actual solutions for HIE, or these regional HIOs may need to change and evolve to comply with CalPSAB HIE guidelines and other evolving State and federal rules. For the time being, however, only a minority of eligible providers in California have access to HIE services through a regional HIO.

HIE	Year	Region	Org	Technology	Operational*	NHIN	Clinical Priorities	Financing to Date	Sustainability Model
Access El Dorado (ACCEL)	2004	El Dorado County	Unincorporated	Federated	Public health, mental health, 7 clinics, 2 hospitals	NA	Care coordination; public health, medical home	Grant, county, First 5, hospitals	In development
EKCITA	2004	Eastern Kern County	501(c)3 (2009)	Hybrid open source system	3 clinics; 2 private practices; 1 hospital	NA	Diabetes & Regional public health issues	Grant	Minimum volume of users
Health-e-LA	2004	Los Angeles County	Unincorporated	Federated	NA	NA	Safety net	Grant, private	In development
Long Beach Network for Health	2003	Long Beach	501(c)3 (2007)	Hybrid federated model	NA	Yes	ED & Patient safety	Grant	Minimum volume of users
OCPRHIO	2007	Orange County	Unincorporated	Federated	NA	NA	ED	Grant	In development
Redwood MedNet	2003	Mendocino, Sonoma, Lake Counties	501(c)3 (2005)	Federated with decentralized network	30 providers, 8 practices, 5k transactions/ month	Yes	Clinical data; Lab results, radiology, ePrescribing	Grant and private	Cooperative health data access service
Santa Cruz HIE	1995	Santa Cruz	IPA & hospital based	Push model; vendor outsourced	Local hospital; county clinics; IPA 90k transactions/ month	Yes	Clinical messaging; results delivery; eRx	IPA support	Hospital & IPA contributions

Table 3. Regional Health Information Organizations in California

4.2.1.2 In addition to classical RHIOs, there are numerous other initiatives and resources to exchange data across organizations that are important parts of the HIE infrastructure in CA. These resources are discussed below.

4.2.1.3 Other Existing HIE Infrastructure

4.2.1.3.1 Surescripts

The Surescripts prescribing network is potentially an important component of the HIE infrastructure for electronic prescribing in the outpatient setting. The network currently reaches approximately 75% of the retail pharmacies in California for electronic prescriptions and renewal requests. Coverage varies somewhat by metropolitan statistical area (range: 68% to 100%). The Surescripts network provides a way for retail pharmacies that are parts of large chains to connect, but offers significantly fewer connective services for independent pharmacies. Hence, areas with more independent pharmacies generally have less access to large e-prescribing networks. Notably, in the Los Angeles-Riverside-Orange County network, nearly a third of the 3,000 retail pharmacies are not yet connected to the Surescripts network. Depending on the geographical clustering of connected and excluded pharmacies, there may be areas in which eligible providers with EHRs are not yet able to submit prescriptions electronically via the Surescripts network.

The Surescripts network may also be an important facilitator of medication reconciliation, as medication dispensing and claims data from participating pharmacies and PBMs are aggregated within the network

and made available to authorized health care providers. This service provides a potential means for viewing outpatient medication histories across sites of care. As with e-prescribing, the effectiveness of this resource is affected by its degree of coverage among pharmacies and PBMs, which is not yet universal.

In addition to coverage gaps, the Surescripts network currently has a few technical limitations. These issues include difficulties in directing prescription-renewal requests to providers that practice at multiple sites and occasional challenges in matching patient identities when retrieving complete medication-history data.

The inclusion of Surescripts in this plan is not an endorsement by the State, but rather recognition of the value that this network may bring toward the successful implementation of this Operational Plan.

4.2.1.3.2 HIE Infrastructures of Large Provider Organizations

Certain provider organizations in California are already well integrated and achieve HIE within the scopes of their enterprises. Kaiser Permanente is the largest and best example of such provider integration. The Kaiser delivery system recently completed a large EHR infrastructure project that enables individual providers to share and exchange information with each other, as well as to prescribe electronically, receive test results electronically, and provide patients access to their own health data through a web portal. Within the Kaiser delivery system, therefore, much of the infrastructure necessary for meaningful use already exists.

A number of IDNs have also developed HIE capacities that allow their constituent physicians, hospitals, and ancillary service providers to exchange health information electronically today. Some systems engage in collective purchasing of EHR technology and have adequate capital budgets to integrate their EHRs with each other, with their hospital systems, with their ancillary services, and with other data sources. Although few of these IDNs achieve sufficient HIE to support all of the meaningful use goals, they are relatively well positioned to support HIE through their abilities to dictate standards within their organizations, build customized data interfaces, and operate internal infrastructures for authentication and access control.

A number of more loosely affiliated, community-based provider organizations in California, such as IPAs, have also developed some HIE capabilities. IPAs provide additional HIE resources, such as data interfaces to local hospitals, administrative web portals that facilitate eligibility checking (especially for capitated patients), and patient web portals that provide patients access to their health information and messaging with their providers. Although no specific patterns of integration exists across the many

different and diverse IPAs in California, many are providing some or all of these capabilities, with plans to expand these services as the meaningful use incentives create increased demand for HIE.

4.2.1.3.3 Commercial Infrastructure Components

Beyond the HIE infrastructure that provider organizations have built or purchased for their specific use, a number of commercial resources exist that can facilitate HIE required for meaningful use in the future. Several are listed below.

- *Untethered PHR systems (e.g., Google Health, HealthVault).* These systems may play a role in providing patients with access to their own medical information under the meaningful use requirements to the extent that providers' EHR systems can securely export such data to the accounts that patients maintain in these systems. Standards for specific activities and services enabled by PHRs will need to be developed before this is likely to occur on any large scale. This approach may be valuable for providers who do not have the capacity to operate their own patient web portals. Several provider organizations have implemented or are exploring this strategy today.

- *Insurance clearinghouses for Electronic Data Interchange (EDI) transactions (especially claims submission and electronic remittance advice).* These clearinghouses remain the prevailing mechanism for providers to electronically transmit claims to payers. They serve the purpose of aggregating claims submissions from many small provider organizations and forwarding them to payers, which obviates the need for payers to maintain direct connectivity with thousands of physician practices. At least a dozen clearinghouse vendors currently provide this service in California. One potential advantage of the expansion of EDI services to include clinical data is that these organizations have existing provider relationships and the payment for the financial transactions may be sufficient to cover some or all of the costs of the clinical transactions.

- *Payers' portals for web-based administrative transactions; specifically, eligibility inquiries.* All of the major payers in California, including Medi-Cal, provide web portals for submitting eligibility inquiries. These portals provide basic eligibility information regarding a member's enrollment status. Some of the portals provide more detailed information about eligibility, including specific covered benefits and/or patient-specific deductible balances. However, this infrastructure for electronic eligibility checking remains imperfect because (1) multiple discrete data elements are required to uniquely identify someone and avoid false positive

matches in the payer's enrollment database, and (2) many payers do not provide all of the needed eligibility and benefits information via their web portals.

4.2.1.3.4 Immunization Registries

[Note to editor: The changes in this section were suggested by Linette Scott of the DPH in her public comments.]

Over 100,000, or almost 20%, of two year-old children in California are not fully up-to-date with their immunizations. These children are at risk of severe or fatal illness from whooping cough, influenza, measles and other vaccine-preventable diseases. The complexity of the evolving immunization schedule, the migration of children among health care providers through childhood, and the constraints of traditional medical record systems make tracking children's immunizations difficult. These factors contribute to both the lack of immunizations and to over-immunization, which occurs when records cannot be found to verify prior vaccinations.

An immunization registry is a secure database of immunization records that addresses these problems. The registry providing a complete record for private and public health care providers, families, schools and child health, education and welfare agencies. Over the last 15 years, California has incrementally developed a collaborative, decentralized system of nine regional and one county web-based immunization registries collectively known as the California Immunization Registry (CAIR) (See Figure 1).

Figure 1 Immunization Registries in California

CAIR provides secure, electronic exchange of immunization records to support the elimination of vaccine preventable diseases. Within each region CAIR allows users to see patient demographic data, immunization history, immunization forecasting, contraindications, overdue immunizations, and other functions. CAIR provides users with copies of standard immunization record cards, usage reports, appointment remainders, and inventory management. There is no capacity to search across multiple registries at this time, thus limiting these benefits to both providers and patients on a region-to-region basis and more generally statewide.

Table 4. Systems and Interfaces for Immunization registries in California

Region	System Used	User Access
Bay Area Regional Immunization Registry (BARR)	CAIR	Web
Central Coast Immunization Registry (CCIR)	CAIR	Web
Central Valley Immunization Information System (CVIIS)	CAIR	Web
County Registries: Imperial County	County-Specific	Web
Contra Costa Automated Immunization Registry (CCAIR)	County-Specific	Client Server
Immunization Network of Northern California (INNC)	CAIR	Web
Los Angeles-Orange Immunization Network (LINK)	CAIR	Web
Regional Immunization Data Exchange (RIDE)	Region-Specific	Web
San Diego Regional Immunization Registry (SDIR)	Region-Specific	Web
Shots for Tots KIDS Regional Immunization Registry	CAIR	Web
VaxTrack Regional Immunization Registry	Region-Specific	Client Server

The majority of health information exchange between immunization registries and EHRs involves the transfer of updated immunization data, for which prompt, rather than immediate or real-time, exchange is usually sufficient. There are currently some EHR systems securely sharing data with CAIR, primarily through data exports in a standardized flat file format. Such exports are easy and inexpensive to implement, especially for providers who have limited IT resources and technical support. Nationally, flat files remain the predominant method by which immunization registries to obtain electronic data. The sharing of immunization records using HL7 messaging has been technically challenging to registries nationwide despite considerable, ongoing effort but is expected to accelerate through federal Health Information Exchange incentives to providers. With the exception of one county, California's regional immunization registries do not currently have the capacity to accept immunization data via HL7 messaging directly from EHRs.

4.2.1.3.5 Public Health Surveillance Resources

The California Department of Public Health is currently implementing the California Reportable Disease Information Exchange (CalREDIE) application. CalREDIE will support the electronic submission of lab results for reportable diseases via the Electronic Lab Reporting (ELR) system, as well as web-based Confidential Morbidity Reporting (CMR). Both ELR and CMR through CalREDIE specifically target the eighty (80) reportable diseases and conditions as cited under Title 17 of the California Code of Regulations.

The CalREDIE application begins a three-month, three-county pilot phase in January 2010. In pilot, ELR includes both a manual method to key enter lab results.

The CalREDIE application is scheduled for operation by the spring of 2011. Once fully implemented, ELR will provide for electronic data submissions from approximately 2,200 commercial labs (hospitals, reference, public health, etc.) and 15,000 licensed physician operated labs.

State legislation (AB 2658) requires labs to electronically transmit lab reports to the State of California. This requirement is referred to as "lab readiness" for which labs have already begun work to prepare and map lab tests and results to standard terminologies such as Logical Observation Identifiers Names and Codes (LOINC) and Systematized Nomenclature of Medicine (SNOMED) and subsequently construct standard Health Level 7 (HL7) messages for transmission.

At the local level, more than half of the 61 local public health jurisdictions are engaged or have previously engaged in syndromic surveillance data collection. Data sources vary widely, but predominantly include Emergency Department (ED) data from chief complaint or ICD-9 diagnosis. Other data sources include school absentees, sentinel providers, pharmacies, and labs. Some syndromic surveillance data are submitted electronically, but this varies widely by data source, jurisdiction, and surveillance platform or solution. For example, ED data often originates in billing systems, which tend to be automated more readily by large providers. CDC offers surveillance tools to analyze these data, including BioSense, ESSENCE, Real Time Outbreak Disease Surveillance (RODS), Early Aberration Reporting System (EARS.) Commercial offerings include SYRIS, FirstWatch, Reddinet, and EpiCenter.

4.2.1.3.6 Health Data Standards Infrastructure

The technical architecture for Statewide HIE services will use the following existing health data standards:

Lab Reporting: Although many versions of HL7 are used currently for reporting lab results to EHRs in California, an effort is underway to standardize lab reporting based on the EHR-Lab Interoperability and Connectivity Specification (ELINCS) implementation guide, which was developed by the California HealthCare Foundation and HL7. Although ELINCS is used in only approximately 50 lab interfaces today, its use continues to grow and it is supported in California by a number of lab service providers, including Quest Diagnostics and LabCorp. By the end of 2010, Quest Diagnostics will offer lab reporting based on the ELINCS standard to any of its clients in California, utilizing Quest's national result-reporting hub and web-services protocols.

Administrative Simplification: There is nearly universal support for the HIPAA X12 4010 administrative transactions among commercial payers in California. In particular, these payers support the 270/271 transaction for electronic eligibility checking and 837 transaction for claims submission, as required by the EHR-certification criteria for meaningful use. Although only 50% of the private payers currently support the Council on Affordable Quality Healthcare Committee on Operating Rules for Information Exchange (CAQH CORE) Phase-1 rules, which are also required for meaningful use, two-thirds have indicated that they are planning to support the Phase-1 rule within the next 12 months.

Clinical Summary: Many of the EHR vendors currently used by Eligible Providers in California are expected to be using certified EHRs which support the HL7 Continuity of Care Document (CCD) or the American Society for Testing and Materials Continuity of Care Record (ASTM CCR) document standards for exporting and importing clinical summaries. At least 80 ambulatory EHR products are now certified to this level. Fifteen products also support the CCR format for structured document exchange. Although the CCD and CCR standards are just starting points towards semantic interoperability of clinical summary data, they are sufficient to satisfy the meaningful use criteria and are already supported by many of the products likely to be used in California.

4.2.1.3.7 Network Infrastructure

According to the 2007 California Broadband Task Force study, 96% of California residences have access to residential commercial broadband services such as DSL and cable. Based on these findings, the TAC and TWG presume that roughly the same percentage of health care providers has access to broadband. Areas lacking coverage appear primarily in rural and isolated regions of the State, where population density is low. Even in these areas, however, T-1 grade network service is available, although at much higher and often prohibitive price.

With the goal of narrowing the urban/rural gap in residential broadband coverage, the California Telehealth Network is a Statewide initiative to bring network services sufficient for telehealth applications to all health care facilities. This project, which is largely subsidized through a 3-year Federal Communications Commission (FCC) grant, plans to build a private network with sufficient bandwidth (1.5 Mbps) and specialized capabilities to support real-time video-conferencing and other telehealth applications. A secondary goal of this project is to bring broadband-grade service to health care facilities in rural areas at a more cost-effective price than currently offered through the commercial marketplace.

5. Technical Infrastructure Background and Design Approach

To help define the requirements for the HIE architecture, members of the TAC completed a survey describing their current HIE capabilities, the technical resources they use to achieve these capabilities, and gaps in resources that impede or prevent their ability to achieve HIE. Although the TAC membership represents only a very small subset of the broader stakeholder community in California, the members of the group were able to share diverse views on HIE design.

The straw man architecture described here was defined by the TWG, based on general requirements proposed by the TAC and based on the TWG members' own knowledge of technical requirements for HIE. The design approach begins with proposing this high-level architecture and a number of specific architectural components as a starting point for further discussion. Hence, the design expressed in this draft document is by no means the only design or necessarily the best design for the future HIE architecture. Comments and input on this document and future versions of it will inform that ultimate design even as this operational plan is implemented.

5.1 Business and Technical Requirements

The HIE design was informed by a set of general principles and guidelines, as well as a set of specific requirements coming from the meaningful use requirements of the federal government. In addition, the design is intended to address gaps between existing infrastructure for HIE in California and the needs of stakeholders to achieve meaningful use and other healthcare improvement goals.

The near-term requirements of the HIE infrastructure in California should focus on those HIE capabilities needed to support the meaningful use criteria and related HER certification criteria. Only a subset of these criteria are related to HIE, which may be divided into two groups: Those criteria for which HIE is an *essential* element of the criterion and those criteria for which HIE is not the essence of the criterion but may be an important enabling capability. Table 1 and Table 2 below list the meaningful use criteria in

each of these categories, and the HIE capabilities related to each one. These HIE capabilities, therefore, comprise functional requirements integral to the HIE infrastructure in California.

The federal government has not yet specified the criteria required for meaningful use beyond 2011. However, given the effort and lead time required to build out the HIE infrastructure in California, it is also important to consider the HIE that will be needed to support future meaningful use criteria. The meaningful use NPRM provides some general guidance in this area:

> "For other objectives that are reliant on the electronic exchange of information, we are cognizant that in most areas of the country, the infrastructure necessary to support such exchange is not yet currently available. We anticipate raising the threshold for these objectives in future definitions of meaningful use as the capabilities of HIT infrastructure increases. *The intent and policy goal with raising this threshold is to ensure that meaningful use encourages patient-centric, interoperable health information exchange across provider organizations regardless of provider's business affiliation or EHR platform*."[3]

The emphasized sentence characterizes the general long-term goals of the HIE infrastructure in California, and should be a consideration in near-term planning and implementation decisions.

Table 1. Meaningful Use Criteria for which HIE is Essential

Meaningful Use Criterion	Relevant HIE Capability
1. Generate and transmit permissible prescriptions electronically	Infrastructure for an EHR or EHR module to correctly address and securely* transmit an electronic prescription to the desired dispensing pharmacy in the specified standard format. The transmission may occur directly or via a third party.
2. Incorporate clinical lab-test results into EHR as structured data	Infrastructure for labs to securely* transmit structured lab results to the EHR or EHR module of the appropriate provider(s) in the specified standard format. The transmissions may occur directly between labs and EHRs or via a third party.

[3] Notice of Proposed Rulemaking Medicare and Medicaid Programs: Electronic Health Record Incentive Program (Document ID CMS-2009-0117-0002)

Meaningful Use Criterion	Relevant HIE Capability
3. Check insurance eligibility electronically from public and private payers	Infrastructure to securely* query a payer, either manually via a web browser or automatically via Electronic Data Interchange (EDI), in the specified standard format and to receive an electronic response, either via a web browser or automatically via EDI, in the specified standard format. These transactions may occur directly between providers and payers or via a third party.
4. Submit claims electronically to public and private payers	Infrastructure to securely* transmit claims from a provider organization to a payer in the specified standard format. These transactions may occur directly between providers and payers or via a third party.
5. Provide patients with an electronic copy of their health information/discharge instructions upon request	HIE capability is required if the electronic copy is transmitted to the patient via a network, either directly (e.g. via secure email) or through a 3rd-party patient-authorized entity (e.g., a Personal Health Record). In these cases, the capability is required to correctly address and securely* transmit the information in an accepted format to the patient or the patient-authorized entity.
6. Capability to exchange key clinical information among providers of care and patient-authorized entities electronically	Infrastructure to correctly address and securely* transmit the specified types of information (problem list, medication list, etc.) in an acceptable data format from one provider to another, from a provider to a patient-authorized entity, or from a patient-authorized entity to a provider.
7. Provide patients with electronic access to their health information within 96 hours	HIE capability may simplify electronic access provided to patients via a 3rd-party patient-authorized entity, such as an "untethered" PHR. In this case, the same capability is required as for #6.

Meaningful Use Criterion	Relevant HIE Capability
8. Provide summary-of-care record for each transition of care and referral	HIE capability will simplify and promote the transition of care or referral made to a different organization, and most easily facilitate transfer of the summary-of-care record.
9. Capability to submit electronic data to immunization registries and actual submission where required and accepted	Infrastructure to securely* transmit immunization events from any hospital or outpatient facility to the appropriate immunization registry for the appropriate patient in a specified data format, and to allow immunization registries to securely* exchange data
10. Capability to provide electronic submission of reportable lab results to public health agencies and actual submission where it can be received	Infrastructure to securely* transmit lab results from any hospital laboratory to the appropriate public health agency in a specified standard format.
11. Capability to provide electronic syndromic surveillance data to public health agencies and actual transmission according to applicable law and practice	Infrastructure to securely* transmit relevant clinical data from any hospital or outpatient facility to the appropriate public health agency in a specified standard format, including de-identification of the data, if required.

** See section 5.1.1. for discussion of security requirements for meaningful use.*

Table 2. Meaningful Use Criteria That May be Facilitated by HIE

Meaningful Use Criterion	Relevant HIE Capability
12. Generate lists of patients by specific condition to use for quality improvement, reduction of disparities, and outreach	The required capability will enable secure* transmission of clinical data from the source organization to the aggregating organization and to resolve patient-identity discrepancies in the data at the time they are requested or received.

Meaningful Use Criterion	Relevant HIE Capability
13. Report ambulatory quality measures to CMS or States	Accurate generation of ambulatory quality measures may require the electronic aggregation of clinical data from multiple organizations (as above). In this case, the same HIE capability is required as for #12 above.
14. Perform medication reconciliation at relevant encounters and each transition of care	Accurate medication reconciliation may require the electronic aggregation of medication data from multiple organizations where care was received or medications dispensed, either via (1) an ongoing collection of data from various organizations into an EHR, disease registry or data warehouse, (2) a real-time distributed query to the various organizations holding the relevant patients' medication history data, or (3) a real-time query to a 3rd-party organization that aggregates patients' medication history data. In each case, an infrastructure is required to securely* transmit clinical data from the source organization to the aggregating organization and to resolve patient-identity discrepancies in the data at the time they are requested or received.

* See section 5.1.1 and 5.1.2 for discussion of security requirements for meaningful use.

5.1.1 General Principles and Guidelines

The following list represents high-level requirements that provide guidance for the conceptualization and design of an HIE infrastructure in California.

- The health information exchange capabilities that are needed to ensure compliance with the federal government's meaningful use criteria should inform prioritization of the functional requirements for the technical architecture and the shared services that will be developed. However, although priorities, the technical infrastructure and services should not be bounded by the meaningful use criteria, and services provided by the HIE should be self-sustaining and help offset the costs of building additional value-add services.

- The HIE services should support means for provider organizations of all sizes, in all locations, and serving all populations, including the vulnerable and underserved, to achieve meaningful use.

- The HIE services should complement and support, not impede, the core business and clinical processes of the intended providers and consumers of HIE services.

- The HIE services should facilitate HIE where existing HIE resources are lacking or insufficient to ensure that effective and affordable HIE services are available Statewide. Existing investments in HIE infrastructure should be leveraged, and HIE services should not disrupt or displace existing, effective HIE resources that are compliant with State and Federal requirements providing they comply fully with the State's HIE governance and technical requirements.

- The near-term adoption and use of these HIE services should be balanced against the requirement to have a robust long-term solution. The architecture should be flexible enough to enable a process of continuous improvement to address technology changes, new security threats, and developing technical specifications, requirements, and innovations.

- Patients and their families should be considered among the consumers and primary beneficiaries of HIE services and the meaningful use of HIT, and their needs should guide aspects of the design.

- The HIE infrastructure should be secure with respect to ensuring the identities of counterparties, transmitting health information such that it cannot be disclosed to unauthorized parties or modified in transit, and being in compliance with all applicable regulations and laws (including those CalPSAB guidelines that are ultimately adopted by CHHS).

- It is not sufficient for the HIE infrastructure to actually be secure. It must also be *perceived as secure* by California stakeholders, including health care providers and the general public. The HIE infrastructure must be paired with appropriate policy and procedure infrastructure to develop the trust required to be used by California stakeholders, including health care providers and the general public.

- The technical and security requirements of the HIE services must be consistent with and should support participating entities' compliance with privacy and security requirements.

- Use of the shared services developed under the State HIE Cooperative Agreement Program should be voluntary. Any stakeholder can choose to use the resources of their own enterprise, a regional HIO, or any other entity to achieve HIE.

- Use of the shared services developed under the State HIE Cooperative Agreement Program should be available to any healthcare participant, subject to the technology requirements, operating rules and fee requirements of the services, and restrictions or requirements of HIPAA and the HITECH provisions of ARRA.

- The design shall support interoperability with the NHIN as one emerges and with the HIE infrastructures of other States.

Security Requirements of Certified EHRs: The meaningful use criteria within the NPRM specify that eligible professionals and hospitals use certified EHR technology for HIE. The security requirements for EHR certification, as currently specified in the Interim Final Rule (IFR), include the following provisions:

1. Health information must be encrypted when in transit through the use (at a minimum) of transport-level security mechanisms, such as Transport Layer Security (TLS) or Internet Protocol Security (IPSec.)

2. It must be possible to verify that exchanged health information has not been altered in transit through the use of a secure hashing algorithm.

3. Transactions must contain sufficient identity information about the sending party (whether that party is providing health information or requesting health information) that the receiving party can make access control decisions and produce detailed and accurate security audit trails.

5.1.2 California Privacy and Security Requirements

CalPSAB has formulated a set of recommendations regarding privacy and security guidelines for exchanging health information under the State HIE Cooperative Agreement Program. The guidelines that are accepted by the Secretary will become binding requirements for all entities that exchange health information using resources of the State HIE, via execution of contracts and grant agreements between the GE and participants in HIE.

The recommended guidelines are currently in draft form, but it is expected that many will be accepted by the Secretary. In certain cases, these guidelines go well beyond the requirements for HIE set forth in the

meaningful use NPRM and in HIPAA, so it is important to consider them in planning an HIE infrastructure for California.

Notable guidelines proposed by CalPSAB include:

- *Allowable uses and disclosures of PHI via HIE*: Uses and disclosures of individual health information for transmitting through an electronic health information exchange initially are limited to (1) clinical treatment where a health care provider/individual relationship exists and (2) mandated public health reporting purposes. This guideline applies to an independent health information organization, as well as to two separate health care organizations who exchange individual health information without the use of a third party organization.

- *Patient Consent to transmission of their PHI via HIE*: An Opt In policy must be obtained to transmit individual health information through an electronic health information exchange for all other purposes before the information may be exchanged electronically. CalPSAB is reviewing opt-in policies subject to federal and State law and in consideration of the State HIE Cooperative Agreement Program with ONC, and the features of the opt-in policy may change.

- *User authentication within an entity*: An entity shall authenticate each authorized user's identity prior to providing access to individual health information. An entity shall authenticate each user to the level of authorized access that complies with the entity's level of trust agreement with the external exchange entity. An entity that authenticates users attempting to access individually identifiable health information remotely from an unsecured location or device, shall require National Institute of Standards and Technology (NIST) Level 3 authentication in which the data requester must establish two factors of authentication. For example, if Entity A requires two-factor authentication to allow disclosures of PHI to Entity B, Entity B will need to use two factor authenticate for its own users, at least when requesting information from Entity A.]

- *Entity authentication within a "trust network"*: If an entity is participating in a trust network health information exchange, the trust network shall manage entity authentication for those participating on the trust network, and an entity shall manage user authentication only for those entities participating on the trust network. If the user authentication process is across multiple systems or entities, an entity shall implement the agreed upon authentication process as specified by the requesting entity among the participants in the trust network.

- *Authorization and access control*: An entity shall use the following access control attributes to determine if a user is authorized to access requested information in a way that corresponds to, and is compliant with, the data use agreements governing such access and as it aligns with State requirements:

    a) Data Source;

    b) Entity of Requestor;

    c) Role of Requestor;

    d) Use of Data;

    e) Sensitivity of Data;

    g) Consent Directives of the Data Subject

An entity that acts as a data requestor shall execute the authorization process at the location agreed upon in the data use agreements governing that exchange. The data requestor shall pass the authentication and authorization to the data supplier as a single message if so designated by the data use agreement.

5.2 The Proposed Architecture

5.2.1 Definitions

The definitions below help to describe the elements of the proposed HIE architecture and how they may interact. These definitions are not necessarily authoritative across all contexts. Certain of the definitions are based on the consensus definitions of ONC[4] whereas others are *ad hoc* definitions intended specifically to explain the HIE architecture described in this document.

HIE: The electronic movement of health-related information between principals.

Principal (aka "actor"): The individual or entity that is the original sender or the intended recipient of exchanged health information. May be a person, an enterprise, a part of an enterprise (such as an emergency department), an application, or a data repository (such as an immunization registry). If denoting a person, a principal may be a health care professional or an administrative professional at a health care enterprise. Examples of principals are: a physician, a physician practice, a hospital, a care manager, a health plan, a pharmacy, an immunization registry. Operationally, principals are the entities

[4] See http://healthit.hhs.gov/defining_key_hit_terms.

that initiate HIE transactions or the entities to which HIE transactions are directed. Note that principals are not equivalent to the "nodes" or "end points" on a network. Principals use such nodes to send or receive information.

Counterparty (aka "data-trading partner"): The "other" principal with whom a specific HIE transaction is conducted. May be an individual or an entity.

Legal Entity: A business entity that assumes responsibility for safeguarding the patient health information under its control and for managing in a secure manner the exchanges of patient health information in which it participates. Legal entities may be physician practices, hospitals, pharmacies, health plans, health information organizations, etc. The responsibilities of legal entities include (1) ensuring that their users and applications (i.e., *principals*) are reliably authenticated when they request access to PHI that is controlled by other legal entities, and (2) reliably authorizing access to the PHI they control when requested by other legal entities. Note that legal entities may directly authenticate their principals or may use a trusted third-party identity provider.

Enterprise: A discrete business entity that controls in a "top-down" and centralized fashion the selection, purchase, and management of its H.I.T. resources, including the manner of interoperability among those resources Enterprises may be healthcare provider organizations, public health agencies, payers, etc. An enterprises is usually a *legal entity* (as defined above), although it could be a collection of multiple legal entities (e.g., an IPA that purchases and manages the information systems of its constituent practices) or just part of a legal entity (e.g., a hospital clinic that controls its own I.T. infrastructure). The key attribute of an enterprise is internal control over its I.T. resources, such that the enterprise can achieve *internal* HIE without necessarily having to agree on communication protocols, messaging formats, etc. with other business entities.

Health Network Node: An addressable network node that may be the source or the recipient of an HIE "transmission." Health network nodes may include EHRs, lab information systems, PHRs, , interface engines, etc. Health network nodes are not equivalent to principals or legal entities. For example, in the electronic delivery of a lab result, the principals are the laboratory and the physician, the legal entities are the hospital in which the lab resides and the medical group in which the physician practices, and the health network nodes are the hospital's interface engine and the physician's EHR.

Health Information Organization (HIO): An organization that oversees and governs the exchange of health-related information among principals. HIOs may include *regional* HIOs (see below), IPAs, or

other private non-profit, private for-profit, or government entities that oversee and govern HIE. HIOs often provide *HIE Services* (see below).

Regional Health Information Organization (Regional HIO): An HIO that brings together health care stakeholders within a defined geographic area and governs health information exchange among them for the purpose of improving health and health care in that community.

HIE Service: **Any information system** that facilitates HIE, along with its related standards, policies, and processes. HIE services may be provided by private non-profit, private for-profit, or government entities, including HIOs and commercial vendors.

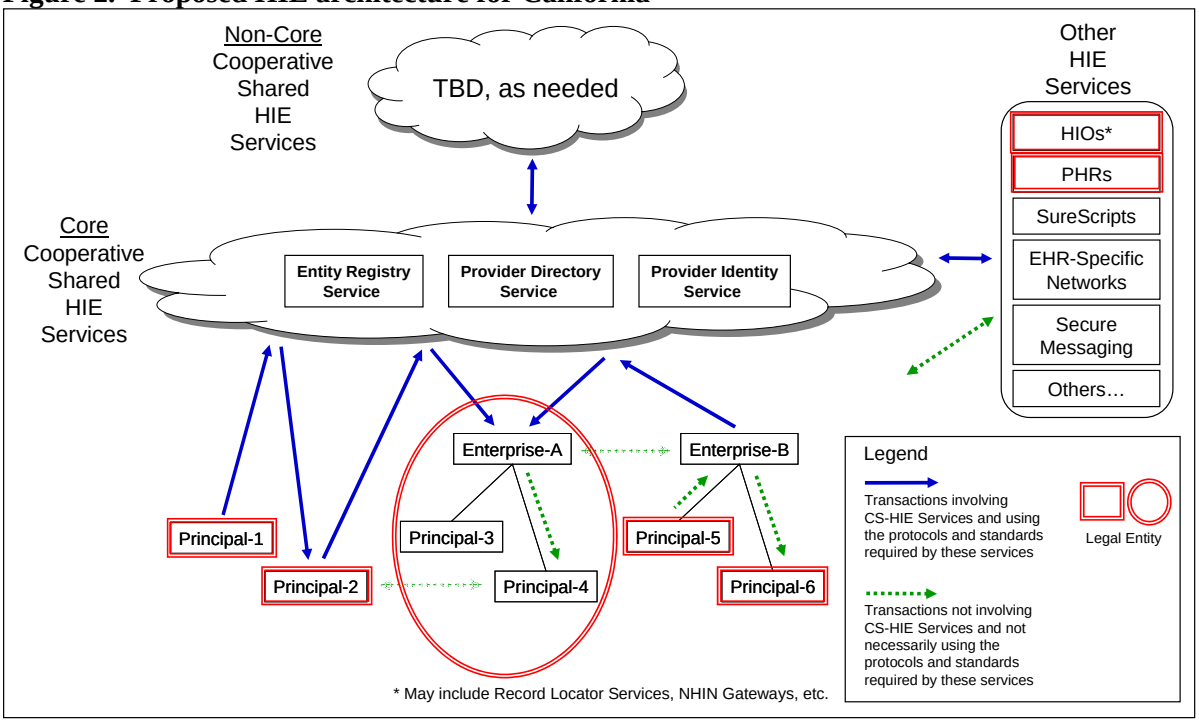
Cooperative Shared HIE Service (CS-HIE Service): An HIE Service that (1) is available to any eligible stakeholder in the CA health care system to enable HIE, (2) is managed, overseen, regulated, and/or financially supported to some extent by the GE under the State HIE Cooperative Agreement Program, and (3) is designated as a "Cooperative Shard HIE Service" by the GE.

HIE Infrastructure: The complete set of technical resources that enable HIE, including HIE Services, other HIE Services, and the agreed-upon protocols, standards, and policies for health information exchange.

HIE Architecture: The set of CS-HIE Services and the specified ways that eligible providers and other entities interact with these services to achieve HIE.

5.2.2 Architectural Components and their Relationships

Figure 2. Proposed HIE architecture for California



The elements of the architecture are briefly summarized below and further described in the following sections.

- Principals: The principals that engage in HIE may be part of larger enterprises (e.g., "Principal-6") or they may be "stand-alone, i.e., their own enterprise, such as a solo practitioner or an independent pharmacy (e.g., "Principal-1"). In any case, all principals that wish to use the CS-HIE services must be associated with a registered legal entity that can manage the principal's identity and attest to the principal's authentication.

- Enterprises: If principals are part of larger enterprises, they may use the resources of those enterprise as HIE Services to communicate with other principals in the same enterprise, or they may use the resources of those enterprises as HIE "gateways" to communicate with principals in other enterprises (including via an HIO). For example, a hospital ("Principal-5") in an IDN ("Enterprise-B") could use the HIE Services of the IDN to transmit a discharge summary to a physician ("Principal-6") in the same IDN, or it could use an HIE "gateway" provided by the IDN to locate and send the discharge summary to a physician ("Principal-4") who is not affiliated with the IDN.

- HIOs: Enterprises may be part of a regional HIO (if one is available) or they may be "stand-alone". If part of an HIO, enterprises may use the various resources of the HIO (such as a record locator service or a NHIN Gateway) as HIE Services to communicate with principals within the same HIO but outside of their enterprise, or they may use the resources of the HIO as a "gateway" to communicate with principals in other HIOs or in no HIO.

- E-Prescribing, PHRs, or other HIE services: There may exist HIE Services furnished by entities other than the enterprise or the HIO to which that a provider belongs. These "Other HIE Services" may include untethered PHRs, commercial prescription routing networks, or secure messaging systems. A principal may benefit from these other services by either interacting with them directly, by interacting with them via its enterprise, or by interacting with them via an HIO. For example, an HIO may provide a gateway for small physician practices to appropriately format and transmit electronic prescription to an e-prescribing network.

- Core Cooperative Shared HIE Services: In addition to the resources described above, there also exists a set of Core Cooperative Shared HIE (CS-HIE) Services that provide a federated identity management service and directory service. These services are intended to create a broadly trusted framework for identity-management, authentication, and electronic addressing to facilitate the HIE transactions otherwise undertaken by the principals, enterprises, HIOs, and Other HIE Services described above. Transactions that use the Core HIE Services must conform to the specific protocols and standards defined for these services (see Legend in Figure 2). For example, an independent hospital in one part of the State ("Principal-2") may wish to send a discharge summary to a physician ("Principal-4") that is part of a large IDN ("Enterprise-1") in another part of the State. The hospital would look up the physician's identity and electronic address via the Core HIE Services using the specified protocols, authenticate for purposes of the transaction using the Core HIE Services using the same protocols, and transmit the discharge summary to the physician's IDN. Upon receipt, the IDN would look up the hospital's electronic identity and verify its credentials using the Core HIE Services, and then deliver the document to the physician using its own internal communications protocols.

- Non-Core Cooperative Shared HIE Services: These shared services provide additional functionality to certain principals, enterprises, HIOs, and Other HIE Services for which the functionality would be otherwise unavailable. For example, the non-core HIE Services may

include an NHIN gateway for principals that are not part of a large enterprise, HIO, or other entity that could otherwise provide this service.

- Bi-Lateral Communications: Note that enterprises or principals may, in certain cases, choose to have dedicated bi-lateral communication channels with other enterprises or principals that involve neither an HIO nor the HIE Services. For example, an IDN ("Enterprise-A") may be part of an HIO, but may choose to use an existing lab-reporting interface it has developed to a national reference lab ("Enterprise-B"), rather than the lab-reporting service provided by the HIO.

The remainder of this section describes each of these components and their interactions in more and provides several HIE use cases to illustrate how the architectural components may be used to facilitate HIE.

5.2.3 Core HIE Services

The Core HIE Services are intended to create a foundation for organizations and participants to exchange health information across their organizational boundaries, such that two entities that have not necessarily exchanged information previously can find each other, positively identify each other in a manner they both trust, determine where and how to effectively exchange health information, exchange information in a secure manner that supports both authorization decisions and the appropriate logging of transactions, and reconcile the identity of the individual patient to whom the information pertains.

The Core HIE Services consist of an *Entity Registry Service*, a *Provider Directory Service*, and a *Provider Identity Service*. These services provide four primary functions:

1. A **trusted process for positively identifying persons and organizations** with which one intends to exchange health information. Positive identification is provided through entries in the Entity Registry Service, a designated electronic registry of legal entities that have been certified as authentic and reputable by a trusted third party. Certified entities, in turn, provide trusted identifying information about the specific persons, departments, and other "principals" within their spheres of control with which health information may be directly exchanged.

2. A **trusted registry of health network nodes** that can send or receive HIE transactions across organizations. The identities of these network nodes are also maintained as entries in the Registry Service and are certified as authentic and reputable by a trusted third party. The

entries allow the information systems that send and receive HIE transactions to verify each other's legitimacy, to mutually authenticate each other, and to protect health information in transit from disclosure or corruption. Each registered network node in the Registry Service must be associated with a single legal entity also registered there.

3. A **trusted directory of electronic addresses** for "principals" with which health information may be exchanged (i.e., organizations, departments, applications, and/or persons). These addresses, which may be maintained within the Provider Directory Service, are specific to the various kinds of HIE transactions offered (e.g., sending lab results, requesting medication lists, etc.). Users or information systems may use these directory entries to determine the correct address for sending specific kinds of transactions intended for specific recipients.

4. A **trusted directory of the communication protocols and data standards** that may be used to exchange health information with specific principals (i.e., organizations, departments, applications, and/or persons). These directory entries, also maintained in the Provider Directory Service, inform programmers and information systems about the set of transactions that are supported by various organizations, departments, applications, and persons and the appropriate communications protocols and data standards to use for each one.

The goal of the Core HIE Services is provide a light-weight and relatively flexible infrastructure to provide these functions, upon which additional services and resources for health information exchange may be layered.

Illustrative "use cases" of how the *Entity Registry Service*, *Provider Directory Service*, and *Provider Identity Service* may be leveraged to meet the HIE criteria for meaningful use are found in Appendix 10.

The following sections describe the proposed Core HIE Services in more detail.

5.2.4 Entity Registry Service

Purpose: The Entity Registry Service is intended to provide a trusted registry of the legal entities that are taking responsibility for authenticating the principals engaged in HIE transactions. It is also a trusted registry of the health network nodes that may be the senders or recipients of "transmissions" of HIE. The Service comprises part of a federated identity management system for HIE, and serves to inform parties and systems engaged in HIE transactions about the validity and authenticity of counterparties to their transactions.

The Entity Registry Service is not intended to be a registry of individual health care professionals, patients or consumers, nor to provide for the provisioning of such individuals for purposes of electronic transactions. Health care professionals (including physicians) will be provisioned and registered by their own institutions, by designated third parties (such as HIOs), or by the Provider Identity Registry. A registry of consumers/patients for purpose of identification and consent management is outside the scope of the HIE Service architecture at this time, but may be defined as part of the architecture in the future or may be provided outside of this architecture.

Description: Entries in the Entity Registry Service are essentially trusted "bindings" of legal entities (as defined by their names, locations, alternate unique identifiers such as National Provider Identifiers (NPIs), type (physician practice, lab, emergency room, etc.) to unique registry identifiers and to public encryption keys. These binding are typically represented as *digital certificates* that are signed by a trusted, centralized *Certificate Authority*. A cardinal element of the registry is that its entries are trusted as legitimate and accurate by all stakeholders in the healthcare system. This trust will require both a rigorous process for provisioning legal entities and a timely process for modifying entries in the registry (including certificate revocation) as information about the entities changes.

Among the attributes of entities registered in the Entity Registry Service is a URL that "points" to a directory of principals at the entity who may be the recipients of HIE transactions. This URL may reference a directory service hosted by the entity itself, hosted by a trusted third party (such as an HIO), or hosted by the HIE Provider Directory Service. Regardless of which organization hosts the directory service, the service must conform to a standard interface for directory information as defined by the State HIE Cooperative Agreement Program (see Section 4.3.3)

The mechanisms by which valid entries in the Entity Registry (e.g., digital certificates) are made available may vary. The Entity Registry Service itself could have a web-services interface that allows retrieval of certificates by systems wishing to validate specific legal entities. If no entry for a legal entity were returned, the entity would be considered invalid. Alternatively, the Entity Registry Service could publish only those entries that have been revoked (i.e., a "revocation list"). If no entry for a legal entity were returned, the entity would be considered valid.

Operational Policies:

- Access to the Entity Registry Service is confined to entities that also have entries in the registry. Information in the registry, while not confidential, could be abused if available to the general public. This policy is analogous to that currently specified for NHIN Service

Registry: "All Nationwide Health Information Exchange (NHIE) to Service Registry communication must be authenticated and digitally signed via [digital certificates] to ensure only authorized and properly authenticated NHIEs are allowed to communicate with the Service Registry.[5]

- Write access to the registry is very rigorously controlled, and confined to certificate authorities with special authorization. The process and policies by which entities will qualify for registration will need to be established and operationalized by the GE.

- Having an entry in the Entity Registry Service and/or using the service are entirely voluntary. If entities are able to achieve the health information exchange they require in the absence of an entry in this service, they are not obligated to have one, as long they comply with State and federal privacy and security requirements. Also, entities may maintain entries in the Entity Registry Service and access the entries of other entities without being obligated to use any other Cooperative Shared HIE Services (such as the Provider Directory Service). However, legal entities are obligated to have an entry in the Entity Registry Service if they wish to use any other Cooperative Shared HIE Services, because an entry is required for trusted authentication with respect to all Cooperative Shared HIE Services.

Technology:

Resources from the NHIN Architecture: The NHIN architecture does not include a discrete service that is identical to the Core Entity Registry Service described above. However, an analogous service exists in the form of the "NHIE[6] Service Registry" specification. This specification defines the capabilities and interfaces of a registry that maintain the information required for one NHIE to discover the existence of other NHIEs within the NHIN, and the associated information that enables one NHIE to establish a connection to another NHIE. Specifically, an NHIE Service Registry is intended to contain the following information about all NHIEs within the NHIN:

- The name of the NHIE

- The unique network identifier (Home Community ID) of the NHIE

[5] NHIE Service Registry, v1.1.
[6] "NHIE" = NHIN-enabled HIE, i.e. an HIE that is capable of discovering information in other NHIEs and exchanging information with these NHIEs. Note that "HIE" in this context is synonymous to "HIO" as defined in this document.

- A Uniform Resource Identifier (URI) where the public key of the NHIE x.509 security certificate can be accessed
- A URI where the Web Services Description Language (WSDL[7]) interface definitions for the NHIE can be accessed
- Contact information for the NHIE's technical point of contact

With this information, one NHIE can establish a secure connection to another (using its x.509 public key), locate and invoke the services of other NHIEs (based on the endpoints defined in the WSDLs), and uniquely identify and direct messages to other NHIEs.

The selected platform for the NHIE Service Registry is based on the Universal Description Discovery Interface (UDDI) version 3.0.2 specification.

NHIE Service Registries are similar to the Core Entity Registry Service described above in that they both represent certain identifying attributes of data trading partners and they both provide a means for accessing the public keys of trading partners for purposes of authentication.

However, there are also several differences between the Service Registry specified for the NHIN architecture and the Core Registry Service described above:

1. The NHIE Service Registry is intended to store information about HIEs (or HIOs, as referred to in this document). The Core Entity Registry Service is intended to store information about the various kinds of legal entities that may engage in HIE, such as physician practices hospitals, immunization registries, etc. Registered legal entities may participate in HIOs, but they are more granular organizations than HIOs themselves. It is possible that the specifications of the NHIE Service Registry could be repurposed for this different task by expanding the concept of "services" to include the individual legal entities that participate in HIE transactions.

2. The NHIE Service Registry provides the address of a WSDL specification for the HIO, which describes the services that an HIO supports and where and how to access those services. The Core Registry Service does not reference such a WSDL. Instead, comparable information is represented in separate directory services that are hosted by the registered entity or by the

[7] WSDL = Web Service Definition Language, a non-proprietary standard format for specifying the services provided by a web-services node (an HIE in this case), where and how to access these services, and the data formats in which information will be passed in service requests and responses.

Core Provider Directory Service, as described below. The Core Registry Service and *Core Provider Directory Service* could be consolidated into a single service, to more closely approximate an NHIE Service Registry. However, because only a subset of entities will choose to publish their providers' addressing information in the HIE Provider Directory Service, it may make more sense to keep the Entity Registry Service and Provider Directory Service separate.

5.2.5 Provider Directory Service

Purpose: The Provider Directory Service is intended to provide default information about where to direct transactions intended for specific principals to HIE transactions and how to formulate the transactions such that they can be correctly processed when received. Note that "provider" in this context denotes any principal to an HIE transaction, and is not confined to health care providers. Hence, entries may exist in the Provider Directory Service for physician practices, hospitals, hospital departments, laboratories, pharmacies, personal health records, immunization registries, payers, and any other entities to whom health information could be legitimately sent or from whom health information could be requested. Each principal, however, must be associated with a legal entity registered in the Entity Registry Service.

The Provider Directory Service allows registered legal entities to publish the address(es) at which their providers accept specific HIE transactions and the communication protocol(s) they support for these transaction. This information is available to any authorized counterparties who wish to conduct such transactions on an ad hoc basis, but would otherwise lack the addressing and protocol information to do so . For example, if a physician wishes to send a patient's key clinical information to a colleague at another organization, the Entity Registry Service would allow him to look up the electronic identity of the organization and the Provider Directory Service (if used by that entity) would inform his EHR as to the network address to which the transaction should be addressed and the communication protocol(s) with which the transaction should be conducted (including protocols for transport, security, and data representation).

Entities may publish a registry of their providers in any manner that conforms to the standards of the State HIE Cooperative Agreement Program, and need not use the HIE Provider Directory Service. This service is provided as a Core HIE Service for those entities that cannot or choose not to host their provider directory themselves (e.g., small practices).

The Provider Directory Service does not perform any of the network routing required to conduct HIE transactions – it only provides the network address to which the transaction should be directed (see

below). Network routing is expected to be performed by other means, including the existing public internet routing infrastructure as well as the existing infrastructure of enterprises, HIOs, and other HIE services.

Description: The Directory Service will provide a database of directory entries that provide the following mappings:

Entity + Principal + Transaction Type => Network Address + Protocol

Where

"Entity" is the identifier of an entry in the Entity Registry Service. This will be a key attribute that supports lookups by specific entity.

"Principal" is the identifier of a principal within the designated entity. Directory entries will include certain minimum attributes of these principals, such as name, mail and telephone contact information, secondary identifiers, professional role (if a person), etc. These attributes support discovery of principals, and they will likely vary depending on the type of principal.

"Transaction Type" is an element from a pre-defined set of transaction types. This set may include transactions such as "Submit New Medication Prescription", "Submit Laboratory Order", "Send Laboratory Result", "Send Encounter Summary", "Request Patient Summary", "Request Insurance Eligibility Information", etc. The set will be specified in the course of defining the Core HIE Services.

"Network Address" is a Uniform Resource Locator (URL), such as https://clinic.newport.com/inbox/DischargeSummary.

"Protocol" is a designation of the protocol "suite" that can be processed for the indicated transaction at the indicated network address. The protocol suite, in turn, designates the combination of transport, security, and data-representation protocols that are recognized at the specified network address. For example, a protocol suite might designate Simple Object Access Protocol (SOAP) v1.1 over HTTP for transport, TLS, 2-factor authentication, and the Security Assertion Markup Language (SAML) Token Profile v1.1 for user authentication, and the HL7 CCD for data representation. Multiple entries for a single combination of Entity, Principal, and Transaction Type could specify alternative addresses and/or protocol suites that may be used for a transaction.

Operational Policies:

- For principals that are part of a larger enterprise or participate in an HIO, the network address in some or all of their directory entries may be that of their enterprise or HIO. The enterprise or HIO is then responsible for routing the transaction to the intended providers[8] (for example, see "Enterprise-A" and "Principal-4" in Figure 2). This enables large enterprises and HIOs to manage the routing of traffic within their spheres to reach the final recipient, rather than having to maintain entries in the HIE Provider Directory Service for all of the physicians, departments, and applications that they represent.

- Information in the Provider Directory Service must be secure because it represents a trusted "binding" between a principal and the address to which transactions intended for that principal are directed. Hence, access control for modifying directory entries needs to be rigorous. If the addressing information were compromised, for example, a physician might send a message intended for another physician to an unintended and unauthorized third party. Also, read-access to the Directory Service should require authentication via a legal entities Entity Registry Service entry, so that entities will feel confident publishing their provider directory information in the Directory Service without undue risk of spoofing, denial of service attacks, and other malicious behavior.

- If a principal has an entry in the Provider Directory Service for a specific transaction type, then the principal must be have at least one entry for the transaction type that conforms to a designated set of communication protocols conformant with the Cooperative Shared HIE Services standards (see Section 4.3.3.2). In other words, principals must support at least the designated standard communication protocol for all transaction types that they publish in the Provider Directory Service. At the same time, providers (and their entities) may support other, non-standard communication protocols for the same transaction types. Note: The same policy applies when legal entities host their own provider directories, although any transactions they conduct privately (i.e., not using the CS-HIE Services) need not support the designated standard communication protocols.

The rationale for this policy is so that counterparties can count on principals supporting at least the designated standard communication protocol for the transactions they "publish" via the Provider Directory Service. Counterparties are not obligated to use the designated standard communication protocols, but principals are required to offer it if they offer any protocols for that transaction.

[8] Note that delivery, in this case, will require that the identity of the intended recipient (principal) is included with the transmitted message.

Having entries in the Provider Directory Service or using information from the Service for HIE transactions is entirely voluntary. Entities may choose to host their own provider directories or use the hosting services of a third party for their provider directories. However, every legal entity with an entry in the Entity Registry Service must make its provider directory accessible as a web service that is compatible with the interface specifications of the Provider Directory Service. Organizations may choose to acquire information about the network addresses and communication protocols that counterparties support for various transaction types in any manner they wish, including via direct agreements with their data trading partners or via referencing a separate third-party resources (such as an HIO). Even if providers publish directory entries for certain transaction types in the Provider Directory Service, they may accept instances of those transactions at different network addresses and/or via different communication protocols than those designated in the published entries. Last, providers need not publish in the Provider Directory Service all the addresses and/or communication protocols at which the will process transactions, but they must support the addresses and communication protocols that they do publish.

Technology

Resources from the NHIN Architecture: The NHIE Service Registry specification (referenced in Section 4.3.1.1) specifies that the registry be represented as a UDDI service catalog and that entries in the registry be represented per the UDDI data model. The data model for each entry consists of the following XML objects:

BusinessEntity – Information about the business or organization providing the services; each BusinessEntity may contain 0 to many instances of a BusinessService

BusinessService – Descriptive information about each of the services that the business entity provides; each BusinessService may contain 0 to many instances of a BindingTemplate

BindingTemplate – Technical information about the service entry point and implementation specifications for a service; each BindingTemplate may reference 0 to many instances of a tModel

tModel – The detailed technical specifications of the service interface, such as details of the SOAP protocol used, security specifications, data representations, etc.

These objects are analogous to the components of Directory Service entries, as specified above. In particular, the following correspondences exist:

BusinessEntity => Entity + Principal

BusinessService => Transaction

BindingTemplate => Network Address

tModel => Protocol Suite

If the Entity Registry Service and Provider Directory Service were combined into a single service, the UDDI model and the interface specifications of the NHIE Service Registry may be appropriate for representing the directory entries as specified above. Further evaluation of the UDDI data model, the NHIE Service Registry specification, and the requirements of the Entity Registry Service and Provider Directory Service as described above is required. If the NHIN specifications do not prove suitable for the functionality needed in the Directory Service, different technical standards also exist for directory services and will be considered.

5.2.6 Provider Identity Service

Purpose: The Provider Identity Service is intended to provide a widely trusted mechanism for provisioning and authenticating providers involved in HIE transactions (again, "providers" in this context refer to principals as defined in Appendix 10, i.e., individual health care providers, health care administrative staff, or health I.T. applications that engage in HIE transactions). Although many legal entities may be trusted by their counterparties to provision and authenticate principals themselves, other entities (particularly smaller ones) may not be trusted by their counterparties and may require a trusted "third party" identity service. The Core HIE Provider Identity Service is intended to fill this role.

Description: The service will be responsible for (1) maintaining the required information to authenticate principals registered with the service, (2) reliably performing the authentication step, (3) generating the necessary token(s) to assert a successful authentication, and (4) making these tokens available in a secure manner to the authenticated principals and/or the principals' counter-parties in transactions.

These authentication assertions will include the principal's key information from the Provider Identity Service, including unique identifier, identifying attributes, and public key. The assertions will also contain information about the authentication event, including the authentication method (password, two-factor, etc.). The assertion will serve as a trusted "binding" between a person or application that is

seeking access to health information and the identity of a principal as maintained in the Provider Identity Service.

Authentication assertions generated by the Provider Identity Service may be used to authenticate end users for "front channel" HIE transactions (such as web-browser-based interactions with an immunization registry) or they may be used to authenticate enterprises or information systems for "back channel" transactions (such as the transmission of a clinical summary from one EHR to another).

The Provider Identity Service may support multiple methods of authentication, including weak methods (password only) and strong methods (two-factor authentication involving software tokens, physical tokens, and/or biometrics). The Authentication Service, itself, will not require any specific level or technique of authentication for any specific transaction type. It will be up to the access-control policies of data-trading partners to accept or reject the authentication method used for a requested transaction. Note that transactions may also contain separate *authorization assertions* that indicate the role of the principal seeking access with respect to the patient and the reason for the requested access (see "Authorization" in Section 4.3.1.4).

Operational Policies

- Write access to the Provider Identity Service is very rigorously controlled. Specifically, only organizations (*certificate authorities*) that are certified by the GE to provision and credential providers will be entitled to update the information in the Provider Identity Service.

- To ensure the maximum degree of trust, management and operations of the Provider Identity Service will be assigned by the GE to a specially designated and certified organization. The organization(s) will be entrusted with, responsible for, and certified to perform the provisioning, credentialing, and authentication of principals in a secure and rigorous manner. The organization(s) may be non-profit, for-profit, or government entities.

- Authenticating via the Provider Identity Service for purposes of HIE is entirely voluntary. Authentication for HIE transactions may be performed directly by the entities involved in the transactions, if both parties to the transactions honor that method of authentication.

Technology

Resources from NHIN Architecture: The NHIN architecture does not include services or specifications for performing authentication, per se. It does, however, include in its Messaging Platform Specifications

the SAML Token Profile v1.1 (based on SAML v2.0). This profile may be used to standardize the representation of the authentication assertions generated by the Provider Identity Service and accepted by counterparties to HIE transactions.

5.2.7 Support for Other Core Functions

Authorization: The proposed HIE services currently includes no service for performing or facilitating the authorization of HIE transactions. This is for two reasons. First, it is assumed that many counterparties to HIE transactions will trust no other entity to make access-control decisions. Organizations are typically conservative with respect to the electronic disclosure of personal health information and even the acceptance of health information from other enterprises. Secondly, any centralized patient-consent database would require a registry of patient identities, which may not be politically feasible in the near term.

However, the TAC and TWG proposes to support authorization decisions by specifying use of standard SAML attribute assertions within transactions that use the HIE Services, as well as use of the standardized codes for "user role" and "purpose for use" as specified in the NHIN Authorization Framework.[9] This level of standardization will enable entities to better make access-control decisions when the only information they have about the counterparty to an HIE transaction is derived from the Entity Registry Service and the transaction itself.

Logging: This has been suggested as an additional Core HIE Service. In this architecture, however, logging of all interactions with the Core HIE Services (e.g., registry lookup, directory update, provider authentication) will be performed by logging modules of these services themselves, rather than by a separate "Logging" service. This will likely be easier to implement than a separate logging service, but may make it more difficult to provide auditing of such interactions as a core service in the near term. It is not yet clear how important it will be to provide an auditing service for interactions with the core HIE Services.

Logging of actual HIE transactions enabled by the Core HIE Services, including lab result delivery, request for key patient information, and eligibility check, will be performed by the service end points involved in HIE transactions, rather than by any component of the Core HIE infrastructure.

[9] NHIN Authorization Framework Service Interface Specification v2.2.

Protocol Translation: This has been suggested as an additional Core HIE Service. It remains to be determined whether it is feasible for protocol translation to occur centrally, or whether the sending and receiving systems should perform protocol translation before sending and/or after receiving transactions.

5.2.8 Non-Core HIE Services

In addition to the core services described above, enabling health information exchange needed to achieve meaningful use and other health policy goals may require additional services to be provided under the State HIE Cooperative Agreement Program. These services would provide specific functions needed for HIE that are not otherwise available to eligible providers and/or to the counterparties with whom they need to exchange health information. These services would be layered on top of the Core HIE Services on an as-needed basis over time.

One non-core Cooperative Shared HIE Service is planned at this time:

- A centralized "clearinghouse" for routing lab results to the appropriate ordering providers and public health agencies. This service would ostensibly replace the numerous point-to-point connections among labs, EHRs, and public health databases with a single routing hub connected to participating entities..

A number of other non-core CS-HIE Services are also under consideration, although further evaluation of the technical feasibility of and business case for these services is required::

- An NHIN gateway for provider organizations that are not part of enterprises, HIOs, or other provider aggregations that have their own NHIN gateways.

- A trusted consumer registry (or registries) that may be used as the basis for federated identity management, authentication, and authorization involving consumer identities and their attributes.

- Expanded functionality for the lab-routing clearinghouse, to include (1) a decision-support component able to automatically determine which test results can and/or must be transmitted electronically to which providers/ patients/ agencies per CA statutes and regulations, (2) a component to transform lab result messages to conform to the format, coding, and transport requirements of the receiving EHR or public health agency, and (3) a component to route and transform lab *orders* as well as results. .

- A central access point for EHRs and practice management systems to retrieve insurance eligibility information via EDI transactions across various payers in California. This service would facilitate electronic eligibility checking and the fulfillment of the corresponding meaningful use criterion for the users and vendors of EHR systems, suggesting a revenue model for sustainability. In concert, the same access point may be used to enable web-based access to eligibility information for those eligible providers as yet unable to take advantage of EDI transactions (primarily small physician practices). The California governance entity will work with the Integrated Healthcare Association (IHA), the California HealthCare Foundation, and other interested stakeholders to further investigate the value and feasibility of such a service.

- A patient-identity service that assists the recipients of exchanged health information (including intermediaries, such as HIOs) to associate the information with the correct patient health record. The service will help in the reconciliation of identifying attributes of patients, such as name, date of birth (DOB), local medical record number, and health plan identifier, when these attributes vary across health record systems.

- A centralized "clearinghouse" for routing and transforming clinical summary documents among providers and patient-designated entities. This service would be analogous to the lab-routing clearinghouse, and would enable organizations that may lack standards-compliant EHR systems to also exchange clinical summary data.

- A widespread secure-messaging system to enable patients and providers to communicate electronically. This service would include directory services and provide the requisite levels of authentication and encryption. Although various vendors provide secure messaging for patient-provider communications today, these capabilities are not yet widely available to patients, nor interoperable across vendors.

- A statewide appointment-scheduling system to facilitate and track the scheduling of primary-care appointments and specialist referrals. Such a system could improve the efficiency of referral processes, as well as enable the measurement of wait-times for medical appointments.

As envisioned for the HIE architecture, non-core HIE Services would be accessible to any principal, enterprise, or existing HIE service that could benefit from them. However, their use would be entirely optional, even for entities that otherwise use the core HIE Services for authentication and other functions. For example, an HIO that did not have its own NHIN gateway could route NHIN transactions through the

HIE gateway, whereas another HIO could operate its own NHIN gateway and only use the core HIE services to authenticate users of that gateway.

Use of non-core HIE services, however, would require at least an entry in the Entity Registry Service of the core CS-HIE layer.

5.2.9 Protocol Standards for Cooperative Shared HIE Services

The core and non-core HIE services will be based on and accessible through a set of specific standards for HIE transactions. The specification of a small set of standards is necessary to enable the HIE Services to support HIE across principals and enterprises whose information systems today use a large variety of mechanisms for transport, security, and data representation. Principals and enterprises in California are not required to use the standards below for all of their HIE transactions, only those involving the core and non-core HIE Services.

5.2.10 Standards for Core HIE Services

Entities wishing to use the Core HIE Services must interact with these services using the transport and security standards specified below.

- Transport Standards
    - SOAP v1.2 and RESTful communications protocols as specified in the NPRM.
- Security Standards taken from the NHIN specifications
    - SAML Token Profile v1.1 for authentication assertions
    - SAML Token Profile v1.1 for attribute assertions
    - SNOMED-CT Code Sets for “User Role” and NHIN Code set for “Purpose for Use”. This is the coding system that will be required by 2013. It is the ICD-10 CM and PCS (Procedural Classification System) – coding used for procedures and surgeries for clinical and billing use. Note, SNOMED is not currently in use now.

SNOMED CT (**S**ystematized **No**menclature of **Med**icine – **C**linical **T**erms), is a systematically organized computer processable collection of medical terminology covering most areas of clinical information such as diseases, findings, procedures, microorganisms, pharmaceuticals etc. It allows a consistent way to index, store, retrieve,

and aggregate clinical data across specialties and sites of care. It also helps organizing the content of medical records, reducing the variability in the way data is captured, encoded and used for clinical care of patients and research International Classification of Diseases (ICD 10) and Procedure Classification System (PCS) should also be included here

- X.509 Token Profile v1.0 for digital certificates
- TLS v1.0 for transport-level authentication and encryption
- UDDI v.3.0.2 for Registry Service and Directory Service, pending evaluation.

5.2.11 Standards for Other HIE Services

When using non-core HIE Services for HIE transactions, entities must interact with these services using the standards below, based on the transaction type. Also, as specified in the operational policies of Section 5.2.4, the transport, security, and information-payload standards specified below must be *offered* for every transaction that a principal publishes in the Provider Directory Service, or in an alternative directory service hosted elsewhere.

The reason for this requirement is to specify a well-defined "service bus" for transactions that use HIE services, so that these services can be implemented and supported efficiently and need not support the many transport, security, and data standards that are in current use for HIE across the California health care system. The specification does not, however, obligate the participants in HIE transactions to use these standards if they use no Core or Non-Core HIE services for HIE. For example, if a reference laboratory and EHR already used a non-standard format for exchanging lab results, they could continue to do so. However, if users of the EHR published one or more entries in the Provider Directory Service for receiving lab results, at least one of the entries would need to specify the standard protocol for those transactions. The proposed standard protocols are:

- The transport and security standards specified above for the Core HIE Services, plus:
- Health information payload standards, by transaction type
    - Transmit Electronic Prescription => SCRIPT 8.1, with any medication terminology that's mapped to RxNorm in UMLS

○ Transmit Electronic Lab Result to EHR =>	HL7 v2.5.1? ELINCS? HITSP C36? [no standards were specified in CMS IFR]
○ Check Insurance Eligibility =>	ANSI X12 270/271 compliant with CAQH CORE Rules, Phase 1
○ Submit Insurance Claim =>	ANSI X12 837 compliant with CAQH CORE Rules, Phase 1
○ Provide Patients with Health Information =>	HL7 CCD Level 2, based on HL7 CDA R2 *or* ASTM E2369 CCR
○ Provide Summary-of-Care Record =>	HL7 CCD Level 2, based on HL7 CDA R2 *or* ASTM E2369 CCR
○ Submit to Immunization Registry =>	HL7 2.3.1 or HL7 2.5.1, HL7 CVX Code Set
○ Submit Lab Result to Public Health =>	HL7 v2.5.1 LOINC codes must be used.
○ Submit Syndromic Data to Public Health =>	HL7 v2.3.1 or HL7 v2.5.1

5.2.12 Integration of the HIE resources/services from various sectors

Please refer to Figure 2 in Section 4.3 for a graphical representation of the relationships described below.

5.2.12.1 From Governance Entity (i.e., the HIE Services)

Integration of Core and Non-Core HIE Services. Non-Core HIE Services will use elements of the Core services to the extent needed. At a minimum, non-core services will leverage the Entity Registry Service to authenticate the legal entities and the principals that wish to access non-core services. For example, one potential non-core service is a centralized gateway for accessing insurance eligibility information across multiple payers (see Section 4.3.2). Access to the gateway may only granted for requests originating from health network nodes registered in the Entity Registry Service and made by users and applications authenticated by legal entities registered in the Entity Registry Service.

5.2.12.2 From Private Sector

Regional HIOs: RHIOs may use certain of the Core HIE Services to facilitate various HIE services they provide to local stakeholders. For example, a RHIO that provides a service for standardizing the format of lab results and routing results to the appropriate recipients could leverage the Provider Directory Service to store the addresses and supported reporting formats for various labs and physician practices

within its region. The RHIO could also leverage the Entity Registry Service to authenticate legal entities from outside its region that send lab results to providers within the region, thereby providing a "gateway" for other RHIOs to send lab results to local providers.

One example is how an e-prescribing network can leverage the Entity Registry Service to streamline its own processes for provisioning and authenticating the physician practices in their network. A physician practice that has an existing Entity Registry Service entry but is not yet part of the e-prescribing network could begin using the network more quickly if its entry in the Entity Registry Service were honored by the network. Similarly, the e-prescribing network could leverage the contents of the Provider Directory Service to correctly route renewal requests to ordering providers or new prescriptions to pharmacies that may currently be outside its network.

5.2.12.3 From State and Local Governments

With respect to the architecture depicted in Figure 1, the administrative systems and clinical data registries operated by State and local governments comprise *Enterprises* that need to exchange information with each other and with enterprises in the private sector for purposes of collecting or disseminating patient-specific health information. Examples of such enterprises include the Department of Health Care Services (and its MMIS systems) and the State and local departments of public health (and their various registries). Several examples are provided below.

Medicaid Management Information System (MMIS): The MMIS may interact with the HIE Services in at least two ways:

1. MMIS may leverage the Entity Registry Service and (possibly) Provider Identity Service to authenticate and authorize requests from providers for administrative information, such as eligibility and benefits information for Medi-Cal beneficiaries. In this mode, requests to MMIS would include authentication and authorization assertions signed by legal entities registered in the Entity Registry Service. If the MMIS trusted the legal entities thus registered, this trust would obviate the need for MMIS to maintain its own registry of providers authorized to access to MMIS (include their passwords, etc.) and to perform the authentication itself. These functions could be delegated to the trusted legal entities.

2. MMIS may leverage the Entity Registry Service and Provider Directory Service to make requests to providers for access to clinical information, such as medication lists or lab results for Medi-Cal beneficiaries. In this mode, MMIS would, itself, be a registered legal entity in the Entity Registry Service. An MMIS user would locate the provider of interest in the

Provider Directory Service and submit a request to retrieve clinical information for a specific Medi-Cal beneficiary (identified by name, DOB, and Client ID, for example). The contacted provider would authenticate the request using MMIS's entry in the Entity Registry Service. The information would be sent back over a secure channel, because both the MMIS system and the provider's EHR were health network nodes also registered in the Entity Registry Service.

Immunization Registries: Immunization registries could use the Core HIE Services when authenticating requests from providers to submit or retrieve immunization records. This process would be very similar to case #1 described above for MMIS. The immunization registry could leverage the trust infrastructure established by the Entity Registry Service to supplement or replace its own registry of users (for a more detailed description of this process, see Section 4.6).

Public Health Databases: Public health databases used to monitor reportable diseases could also use the Core HIE services when authenticating requests from providers to submit data (including lab results and syndromic findings) and from public health agencies to access the data.

Quality Reporting Programs: California's Office of Statewide Health Planning and Development (OSHPD) collect over 16 million patient records annually from hospitals and licensed ambulatory surgery clinics. The data are used by OSHPD to measure quality of care as well as service utilization and cost and are provided to researchers under strict control. Facilities report these data by uploading files via an internet web page. Data are then subject to editing and correction. These data reporting activities could potentially use Core CS-HIE Services to transmit data. As noted in section 1.3.2.5 above, the capacity to have this reporting accomplished automatically will result in decreased workload for providers and allow OSHPD and other public health agencies to shift from the business of collecting data to analyzing data and providing aggregate results back to providers and others in a timely fashion.

5.2.13 Alignment with NHIN and NHIN Direct

The technical architecture is intended to align with both the NHIN Direct and the original NHIN initiatives at ONC.

In March, the NHIN Workgroup of the HIT Policy Committee announced the launch of NHIN Direct, a new initiative to provide services, standards, and policies that allow the secure exchange of health information directly between providers over the internet.

The Core CS-HIE Services share several goals with this initiative, in that they provide a relatively basic infrastructure for securely transmitting information directly between communicating entities. These services are well suited for the largely "push" transactions needed to fulfill meaningful use (as illustrated in Appendix 10). As such, the core services serve a role comparable to that envisioned for the NHIN Direct components, enabling trusted communications and directory information. The Governance Entity and the State of California are participating in the NHIN Direct Implementation Group to identify areas in which collaboration can benefit both organizations and can help ensure that the California infrastructure is well aligned with the NHIN Direct vision. Near-term areas of interest include the design of provider directory services and identity management techniques.

At the same time, the proposed technical architecture is also intended to accommodate the larger NHIN architecture, in which NHIN-enable HIO nodes (NHIOs) in California and other states can exchange information via gateways that implement the NHIN reference architecture. For providers that are part of regional HIOs and integrated delivery networks, the NHIN Gateways may be provided by their parent organizations, using the Federal Health Architecture CONNECT software, a commercial gateway supplier, or their local implementation. For providers that do not belong to organizations willing or able to provide NHIN Gateways, a non-core CS-HIE Service may be created to serve as a shared NHIN Gateway if allowed by NHIN policies.

In March, it was announced that NIEM, a partnership of the federal Justice Department and the Department of Homeland Security, will be a new framework for developing information exchange standards which describe content and processes among organizations that share data as part of their daily business operations. Organizations in California providing NHIN Gateway services will adapt their specifications to confirm to the new NIEM framework as appropriate.

5.3 Necessary Policy Support and Participation Rules

The following policies are proposed for potential users of HIE Services:

- "Net Neutrality" => if an entity publishes a provider directory (either itself or via the Provider Directory Service) for a specific type of transaction, the entity must support transactions of that type originating from any other entity that has valid access to the provider directory (subject to the authentication and access-control policies of the principals). The network infrastructures of principals may not limit access or give preferential treatment to traffic based on the source of the traffic.

- Minimum Participation => Every entity that wishes to use the HIE services for any purpose must have (at a minimum) a validated entry in the Entity Registry Service and must publish a provider directory that is compliant with the standards of the State HIE Cooperative Agreement Program.

- Optionality => the use of CS-HIE Services (core or otherwise) is entirely optional for any entity, enterprise, or other HIE service. However, if an entity chooses to use the CS-HIE Services, then it may be subject to certain rules and obligations (which are to be defined).

- Transaction Independence => An entity, enterprise, or HIE service may use the HIE Services (core or otherwise) for any supported transaction without being obligated to use HIE Services for any other transaction (with the exception of having an entry in the core Entity Registry Service, which is required to for an entity to access any of the HIE Services)

5.3.1 The role of DURSA(s)

The Data Use and Reciprocal Support Agreement (DURSA) is a comprehensive, multi-party trust agreement that will be signed by all NHIOs both public and private, wishing to participate in the NHIN. The DURSA provides the legal framework governing participation in the NHIN by requiring the signatories to abide by a common set of terms and conditions. These common terms and conditions support the secure, interoperable exchange of health data between and among numerous NHIEs across the country.

The DURSA has been developed as a vehicle for creating trust relationships among the NHIOs participating in the NHIN. It memorializes the expectations for NHIOs in a "network of networks" with respect to the behavior and activities of other NHIEs. Since it is a multi-party agreement, it avoids the need for each NHIE to enter into "point-to-point" agreements with each other NHIO, which becomes exceedingly difficult, costly and inefficient as the number of NHIEs increases.[10]

The DURSA is a voluntary model document which is likely not intended to override California's existing privacy rules, or rules a State may develop in its judgment to protect privacy during exchange of information. The GE and CalPSAB are responsible for determining the utility of the DURSA for California HIE.

---

[10] Draft Data Use and Reciprocal Support Agreement developed by the NHIN Cooperative DURSA Team, November 18, 2009, http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_11673_910332_0_0_18/DURSA_2009_VersionforProductionPilots_20091123.pdf.

6. Business and Technical Operations

<Content omitted from this excerpted version>

7. Patient and Consumer Engagement with HIE

<Content omitted from this excerpted version>

8. Vulnerable and Underserved Populations and the Providers Who Serve Them

<Content omitted from this excerpted version>

9. Legal and Policy

<Content omitted from this excerpted version>

10. Finance

<Content omitted from this excerpted version>

11. Evaluation

<Content omitted from this excerpted version>

12. Appendix: Scenarios Illustrating Use of HIE Architecture for Meaningful Use

This section contains examples of the way that the CS-HIE Services may be used by various types of stakeholders to achieve meaningful use. Its purpose is to illustrate the value of the CS-HIE Services where they are needed, the ways that CS-HIE Services may interact with other HIE services available in California, and the options that stakeholders have with respect to using or not using the HIE services to achieve meaningful use.

Electronic transmission of structured lab results to EHRs

Example HIE Use Case:

CareMore Hospital has a lab outreach program for patients seen at the offices of local community physicians. These physicians are scattered around the community in practices of varying sizes using different EHR systems. The hospital is medium-sized and does not have the resources to implement a separate laboratory interface for each of these practices and EHR systems.

Each of the physician practices is registered in the HIE Entity Registry, and all test orders sent to the lab include an identifier for the entity from which the order originated. Each order also includes an identifier for the ordering provider that is unique to the entity. The CareMore hospital lab uses this information to correctly route electronic lab results to the ordering providers.

For each result that it wishes to deliver electronically, the lab system looks up in the HIE Entity Registry the practice from which the test was ordered. Within that registry entry is a URL for an electronic directory of providers at that entity. Larger practices may host their own provider directories. Smaller practices use the HIE Provider Directory Service for this function. The lab submits a query to the directory URL to retrieve specific addressing instructions where the ordering provider may receive lab results.

These addressing instructions include the URL to which the transmission should be directed and one or more sets of communication protocols and data standards that may be used. At least one set of these protocols/standards must conform to the designated standards of the State HIE Cooperative Agreement Program (in this case, this is the protocol and data standard that the lab will use). Also, the URL indicated in these addressing instructions must reference an entity registered with the Entity Registry Service (either the physician practice itself or a registered intermediary, such as an HIO). Based on this information, the lab system generates an appropriately formatted result message (which includes the name and other identifying information for the patient) and securely transmits this to the indicated entity via the selected communication protocol.

Within this transmission is included the identity of the ordering provider, a digital certificate for CareMore hospital, an authentication assertion signed by CareMore hospital that verifies the lab system that initiated the transaction, and an authorization assertion signed by CareMore hospital that verifies the role of the lab system with respect to the patient, as well as the reason for the information exchange. Before transmitting these data, the lab system verifies that the receiving system specified in the addressing instructions has a valid active entry in the Entity Registry (by ensuring it has an active certificate) and that the actual recipient of the transmission is, in fact, the same entity (by authenticating it at the outset of the transaction).

The address to which a lab result is sent may be:

1. The EHR at ordering provider's practice, in which case the result is loaded into the patient's record in that EHR and the provider is notified.

2. An intermediate routing service that further directs the result to the appropriate EHR. Such a service may be provided by an HIO, by an EHR vendor, or by another entity. In all cases, the routing service that initially receives the result and forwards it to the provider must be a registered entity.

In certain communities, a subset of the physician practices may be able to receive results directly from the hospital lab (perhaps the larger practices), whereas other practices may require an intermediate service for routing and/or translation. In either case, the Entity Registry Service and the Provider Directory Service allow the lab to (1) ascertain the proper routing information by accessing a single source (i.e., the Entity Registry Service) and (2) implement a single protocol to deliver lab results to any community provider via the default protocol required by the State HIE Cooperative Agreement Program.

Note that, for certain ordering providers and/or physician practices, the CareMore Hospital lab could choose to circumvent use of the HIE Entity Registry and the other mechanisms described above to send results directly to the EHR of that lab (for example, a very large practice with whom the hospital already has a legacy lab interface). This interface could continue to operate unchanged if it serves the needs of the hospital and the practice, while the delivery of results to other practices and providers could use the resources of the State HIE Cooperative Agreement Program.

Patient access to health information

Example HIE Use Case:

Dr. Moore is a rheumatologist in a mid-size multi-specialty group, MultiSpec, that has used the Acme EHR system for several years. Acme provides an effective paperless record system for MultiSpec and can export data in the CCD document format, but it is an older product that does not offer a patient-portal module. The product's vendor is relatively small and does not have the capacity to develop a patient-portal module in the near future.

One of Dr. Moore's patients, Mary Byrne, has requested to review her lab results and medication list as they are updated in Acme. To achieve this, Dr. Moore has advised Mary to open a personal health record account with OurPHR, a commercial vendor of PHR services. To fulfill the meaningful use criterion, Dr. Moore will send the health information to Mary's OurPHR account.

MultiSpec is an entity registered in the HIE Entity Registry Service. The OurPHR system is also registered there. To authorize Dr. Moore to send data to her OurPHR account, Mary accesses the HIE Entity Registry via the OurPHR application and looks up the entry for MultiSpec. This entry contains the

URL for the provider registry of MultiSpec, which may reference a registry hosted by MultiSpec itself or may reference the HIE Provider Directory Service (depending on how MultiSpec has chosen to publish its provider directory). The OurPHR application submits a query to this URL to display to Mary the providers at MultiSpec, allowing her to select Dr. Moore and other members of his staff who will be authorized to update her OurPHR account. Earlier, Mary has provide her unique OurPHR account ID to Dr. Moore.

When Dr. Moore or his staff wish to send information to Mary's OurPHR account, they log into the Acme EHR and use it to look up the entry for OurPHR in the HIE Entity Registry Service (the EHR is capable of interfacing to this service and others provided under the State HIE Cooperative Agreement program). Within this registry entry is a URL that references a directory of services provided by OurPHR. The Acme EHR accesses this directory and retrieves addressing instructions for the "update PHR record" transaction. These instructions are not specific to Mary Byrne, but allow EHRs and other applications to update the PHR records of any specified account holder, provided the update is authorized.

These addressing instructions includes a URL to which such transactions should be sent, as well as one or more sets of communication protocols and data standards that may be used for the transaction. At least one set of these protocols/standards must conform to the designated standards of the Cooperative HIE Agreement Program. The URL address of the OurPHR PHR system must be registered in the Entity Registry Service. Using this information, the Acme EHR generates an appropriately formatted document and securely transmits it to the indicated entity (OurPHR) via the selected communication protocol.

Within this transmission is included the OurPHR account ID for Mary Byrne, a digital certificate for the MultiSpec entity, an authentication assertion signed by the MultiSpec entity that verifies the identity and authentication of the Acme user who initiated the transaction, and an authorization assertion signed by the MultiSpec entity that verifies the role of this user with respect to Mary Byrne, as well as the reason for the information exchange. Before transmitting these data, the lab system verifies that the receiving system specified in the addressing instructions has a valid active entry in the Entity Registry (by ensuring it has an active certificate) and that the actual recipient of the transmission is, in fact, the same entity (by authenticating it at the outset of the transaction).

Upon receipt of this transmission, the he OurPHR PHR authenticates the sender as the MultiSpec Group and verifies that MultiSpec has a active entry in the Entity Registry. The entity then uses the authentication assertion, authorization assertion, and Mary Byrne's OurPHR ID to authorize the loading of the CCD document into Mary Byrne's record.

Provide summary of care records for transitions of care

Example HIE Use Case:

Sea View hospital in San Diego is discharging John Smith after an emergency appendectomy. John Smith's regular physician is Dr. Clarence Hill at the Montrose Internist Group in La Jolla. John Smith has given the staff at Sea View Dr. Hill's name and mailing address, so that Sea View can send Dr. Hill a copy of John's discharge summary. Per the meaningful use criteria, Sea View hospital would like to send the summary electronically. Sea View hospital does not know whether Montrose Internist Group is entirely independent, is part of an IPA, participates in a regional HIO, or uses other commercial services for HIE.

The hospital clerk at Sea View hospital uses the hospital's EHR (which is integrated with the Core HIE Services) to look up the Montrose Internist Group by name in the HIE Entity Registry Service. There are seven Montrose Internist Groups in California, but only one in La Jolla at the address given by John Smith. The hospital clerk selects the entity corresponding to the correct Montrose Internist Group and retrieves the entity's indicated URL for a local registry of providers there. The clerk issues a query to the directory service at this URL to look up Dr. Clarence Hill and then retrieve his specific addressing instructions for receiving a hospital discharge summary.

These addressing instructions include the URL to which the transmission should be directed on behalf of Dr. Hill and one or more sets of communication protocols and data standards that may be used. At least one set of these protocols/standards must conform to the designated standards of the Cooperative HIE Agreement Program. Also, the URL address indicated in these instructions must reference an entity registered with the Entity Registry Service (either Montrose Internist Group or another entity serving as an intermediary for Montrose). Using this information, the Sea View EHR generates an appropriately formatted discharge summary (which includes the name and other demographic information of John Smith, for purposes of identification) and securely transmits this to the indicated entity via the selected communication protocol.

Within this transmission is included the identity of the receiving principal (Dr. Hill), a digital certificate for Sea View hospital, an authentication assertion signed by Sea View hospital that verifies the identity and authentication of the clerk who initiated the transaction, and an authorization assertion signed by Sea View hospital that verifies the role of the clerk with respect to John Smith, as well as the reason for the information exchange. Before transmitting these data, the lab system verifies that the receiving system specified in the addressing instructions has a valid active entry in the Entity Registry (by ensuring it has

an active certificate) and that the actual recipient of the transmission is, in fact, the same entity (by authenticating it at the outset of the transaction).

Upon receipt of this transmission, the receiving entity (which may be Montrose Internist Group or an intermediary, such as an HIO) authenticates the sender as Sea View Hospital and verifies that Sea View has a active entry in the Entity Registry. The entity then delivers the discharge summary to Dr. Hill in whatever way is appropriate. If the entity is the EHR at Montrose Internist Group, it may add the discharge summary to the record of John Smith, and notify Dr. Hill of its arrival. If the entity is an intermediary, such as an HIO, it may forward the entire transmission to the information system at Montrose Internist Group for processing. The authorization decision may be made by either the intermediary system or the EHR at Montrose Internist Group, and will be based on the information within the transmission itself about the sending entity, the sending user, the role of the user with respect to the patient, and the reason for the transaction. The relevant assertions are forwarded with the transaction to whichever entity is required to authorize the transaction.

Variation:

If Montrose Internist Group is small and does not have the means to publish its own provider directory via the required standard mechanism, it may have another entity host its provider directory, such as a local HIO or the HIE Provider Directory Service.

If Sea View Hospital and Montrose Internist Group are part of the same HIO, the services and standards defined under the State HIE Cooperative Agreement Program may not be needed at all for transmitting the discharge summary. The HIO may maintain the registries and directories of all the relevant health care entities within the HIO, manage the authentication and authorization processes, and define the communication protocols and data standards. However, when Sea View Hospital wishes to send a discharge summary to an entity outside the HIO (e.g., in another part of the State), the hospital would need a mechanism to look up that entity in the Entity Registry and perform the other steps required, as described above. In this case, either the HIO could provide a "gateway" to translate between the mechanisms used for internal HIE and the "standard" mechanisms specified under the State HIE Cooperative Agreement Program, or the individual entities in the HIO could themselves support the standard mechanisms when communicating with entities outside the HIO. The same choice would apply to entities within integrated delivery networks or other large organizations.

Exchange of key clinical information among providers and patient-authorized entities

Example HIE Use Case:

Dr. Stenson is a cardiologist at a two-physician practice outside of Sacramento. She has recently referred one of her patients, Frank Taylor, to the Health Sciences Medical Center (HSMC) in Sacramento for a mitral valve replacement, and would like to forward key information about Mr. Taylor's medical history, current medications, allergies, and recent lab results to the hospital. Dr. Stenson's practice uses an EHR from a major vendor, but it is different than the EHR used by HSMC. Her EHR is capable of generating a CCD summary document and interacting with the HIE Services available in California.

The exchange of the patient summary between Dr. Stenson and HSMC is very similar to that of the discharge summary between the Sea View hospital and Dr. Hill, with the exception that HSMC requires two-factor authentication for users who request information from or supply information to its clinical information systems. Dr. Stenson's EHR supports password authentication only. Being aware of this limitation, Dr. Stenson has registered herself with the HIE Provider Identity Service, which has rigorously verified her identity and issued her a physicial security token for purposes of two-factor authentication.

Dr. Stenson's EHR can interface to the HIE Provider Identity Service. This enables her to authenticate via the service using her SecurID card and have the authentication token that is generated by the service returned to her EHR. Her EHR then generates an appropriately formatted clinical summary (which includes the name and other demographic information of Frank Taylor, for purposes of identification) and securely transmits this to HSMC via the supported communication protocol.

Within this transmission is included a digital certificate for Dr. Stenson's practice (i.e., the registered entity), the authentication assertion signed by the HIE Provider Identity Service, and an authorization assertion signed by Dr. Stenson's practice that verifies the role of Dr. Stenson with respect to Frank Taylor, as well as the reason for the information exchange. Because HSMC trusts the user-provisioning and two-factor authentication performed by the HIE Provider Identity Service, the medical center will authorize the transaction. Note that, with the exception of the authentication assertion, all aspects of this information exchange are comparable to that of the discharge summary exchange described above.

Variation:

Certain entities may not accept even two-factor authentication when performed by counterparties because they lack confidence in the counterparty's procedures for provisioning users and performing authentication, for example, when information is requested or provided by a small practice that is entirely unknown to the entity holding the PHI. In these cases, there may also be a need for users at such

practices to authenticate via the HIE Provider Identity Service. This may particularly be the case for entities that are not a party to multi-lateral data-use agreements that otherwise establish trust among counterparties in each others authentication mechanisms.

Submit electronic immunization data

Example HIE Use Case:

St. Jude's, a public hospital clinic, has administered three vaccines to a young child and wishes to submit a record of these vaccinations to a regional immunization registry. The transaction may be initiated by an individual user at the hospital, or it may be initiated automatically by an EHR, a billing system, or some other information system at the hospital. In either case, the vaccination information has already been captured by the hospital's information system, and the hospital wishes to transmit these data electronically to the immunization registry, without a user needing to manually log into the registry and re-enter the data.

The immunization registry has an entry in the Entity Registry Service, which the EHR system at St. Jude's retrieves to begin the transaction Again, a URL is provided in this registry entry, which allows the hospital to retrieve a directory of services provided by the immunization registry and addressing information for these services. The addressing information includes the appropriate URLs for the services, as well as the supported communication protocols and data standards. The directory is hosted and maintained by the immunization registry. One of the available services is "Add an unsolicited immunization record", which specifies the use of a specific SOAP protocol and the HL7 v2.5.1 message standard with the Common Vaccine Codeset (CVX). Using this information, the hospital EHR generates an appropriately formatted immunization record, which includes the name and other demographic information of the vaccinated child, and securely transmits this to the immunization registry via the indicated communication protocol.

Within this transmission is included the a digital certificate for the St. Jude's entity, an authentication assertion signed by the St. Jude's entity that verifies the identity and authentication of the EHR user who initiated the transaction (or the application that initiated it if it was automated), and an authorization assertion signed by the St. Jude's entity that verifies the role of this user or application with respect to patient, as well as the reason for the information exchange.

Upon receipt of this transmission, the immunization registry authenticates the sender as St. Jude's hospital and verifies that St. Jude's has a valid active entry in the Entity Registry Service. The registry

then authorizes the addition of the immunization record based on the attributes of the sending entity, per its digital certificate, the relationship of the authenticated user or system with respect to the patient, and the Stated purpose of the transmission. The registry then matches the patient's demographic information to its own database and adds the immunization data to the appropriate patient record. Because the Entity Registry Service maintains an active listing of all valid entities and their attributes and because the data transmission entailed mutual authentication of the sending and receiving entities, the immunization registry does not need to maintain its own user registry and perform its own authentication process.

Submit reportable lab results electronically

Example HIE Use Case:

BioLife is a small regional laboratory in Redding, CA that performs outpatient testing for physician offices in the community. BioLife recently tested a patient specimen that was positive for hepatitis A, a reportable disease in California. The Lab Information System at BioLife is configured to flag all positive test results for reportable conditions and send copies of these results CalREDIE, the State's reporting system.

BioLife begins this transaction by retrieving the entry for CalREDIE in the Entity Registry Service. A URL is provided in this registry entry, which allows the L.I.S. to retrieve a directory of services provided by CalREDIE and addressing information for these services. The addressing information includes the appropriate URLs for the services, as well as the supported communication protocols and data standards. The directory is hosted and maintained by CalREDIE. One of the available services is "Submit a Reportable Lab Result", which specifies the use of a specific SOAP protocol, the HL7 v2.5.1 message standard, and LOINC codes. Using this information, the LIS generates an appropriately formatted lab-result message and securely transmits this message to CalREDIE via the indicated communication protocol.

Within this transmission is included the digital certificate for the BioLife entity, an authentication assertion signed by the BioLife entity that verifies the identity and authentication of the L.I.S. process that generated the submission, and an authorization assertion signed by the BioLife entity that verifies the role of this application with respect to patient, as well as the reason for the information exchange.

Upon receipt of this transmission, CalREDIE authenticates the sender as BioLife and verifies that BioLife has a valid active entry in the Entity Registry Service. CalREDIE then authorizes the processing of the lab result based on the attributes of the sending entity (per its digital certificate), the relationship of the

authenticated system with respect to the patient, and the Stated purpose of the transmission. CalREDIE then forwards the test result to the appropriate public health database for recording and analysis. Because the Entity Registry Service maintains an active listing of all valid entities and their attributes and because the data transmission entailed mutual authentication of the sending and receiving entities, CalREDIE does not need to maintain its own registry of authorized laboratories and perform its own authentication process.

Exchange of information with non-clinical entities for care coordination

Thomas Cooper is an eight year old child who has recently been placed in a new foster home that is located in a different county from his prior placement. Thomas has been previously diagnosed with asthma and is currently experiencing coughing, shortness of breath, and a tightness in his chest consistent with an asthma attack. His foster parents schedule an appointment for him with the family physician they use for all their family's health care, Dr. Greene. In scheduling the appointment, they inform Dr. Greene's staff that Thomas is in foster care.

Dr. Greene practices at a community clinic that is registered in the HIE Entity Registry Service. California's Statewide Automated Child Welfare Information System (SACWIS)is also registered there. SACWIS provides child welfare case workers with information and tools to manage the needs of children in their caseloads, including tools to maintain the federally-mandated Health and Education Passport (HEP), a key component of the case file of a child living in foster care. The HEP is a document that is intended to store key data about a child in order to supply caseworkers, foster caretakers, and individuals involved in the health and education of the child with essential information about the health and educational status of the child. SACWIS also manages case workers' access to and provision of information via HIE, including authenticating users and managing access controls.

In preparation for Thomas's visit, Dr. Greene's staff uses the clinic's EHR to interface to the HIE Entity Registry Service and access the entry for SACWIS, which allows Dr. Greene's EHR to retrieve a directory of services provided by SACWIS, addressing information for these services, and the supported communication protocols and data standards. The clinic's EHR accesses this directory and retrieves addressing instructions for the "access HEP" transaction. These instructions are not specific to Thomas or his case worker, Dee Andrews, but allow EHRs and other applications to access HEP data for any specific child, provided the access is authorized.

Based on this information, the clinic's EHR securely transmits the "access HEP" transaction to SACWIS. The transmission includes the name and other identifying information for Thomas (for purposes of

identification), the identity of the case worker (Dee Andrews), the identity of the treating physician (Dr. Greene), a digital certificate for the clinic, an authentication assertion signed by the clinic that verifies the identity and authentication of the staff member who initiated the transaction, and an authorization assertion signed by the clinic that verifies the role of the staff with respect to Thomas, as well as the reason for the information exchange. Before transmitting the HEP data to the clinic's EHR, SACWIS verifies that the clinic has a valid entry in the HIE Entity Registry (by ensuring that it has an active certificate) and that the actual recipient of the transmission is, in fact, the same entity (by authenticating it at the outset of the transaction). Once verification has occurred, SACWIS transmits the results of the "access HEP" transaction to the clinic's EHR, which delivers it to Dr. Greene.

Once Dr. Greene has completed his visit with Thomas, his staff uses the clinic's EHR to interface to the HIE Entity Registry Service and access the entry for SACWIS, which includes a URL for an electronic directory of case workers. The EHR submits a query to the directory URL to retrieve specific addressing instructions where Dee Andrews may receive summary of care information. The addressing instructions include the URL to which the transmission should be directed and one or more sets of communication protocols and data standards that may be used. Based on this information, Dr. Greene's EHR generates an appropriately formatted summary of care record and securely transmits it to SACWIS via the selected communication protocol. SACWIS then manages the delivery of the information to Dee Andrews and updates the HEP.

Variation:

If the clinic's EHR does not support the "access HEP" transaction, it may utilize the services of an intermediary, such as an HIO, to perform the required steps to request and receive the results of the transaction on behalf of Dr. Greene and translate them into a standard that is supported by the clinic's EHR.

Summary

As the meaningful use criteria, the needs of the California healthcare system, the technical specifications of the NHIN, and the availability and capabilities of the State HIE evolve, the TAC and TWG will modify the set of core and non-core services. As a primary example, as CalPSAB completes the review of privacy and security regulations and provides guidance to the GE, the TAC and TWG are responsible for harmonizing the HIE technical infrastructure to comply with that guidance.