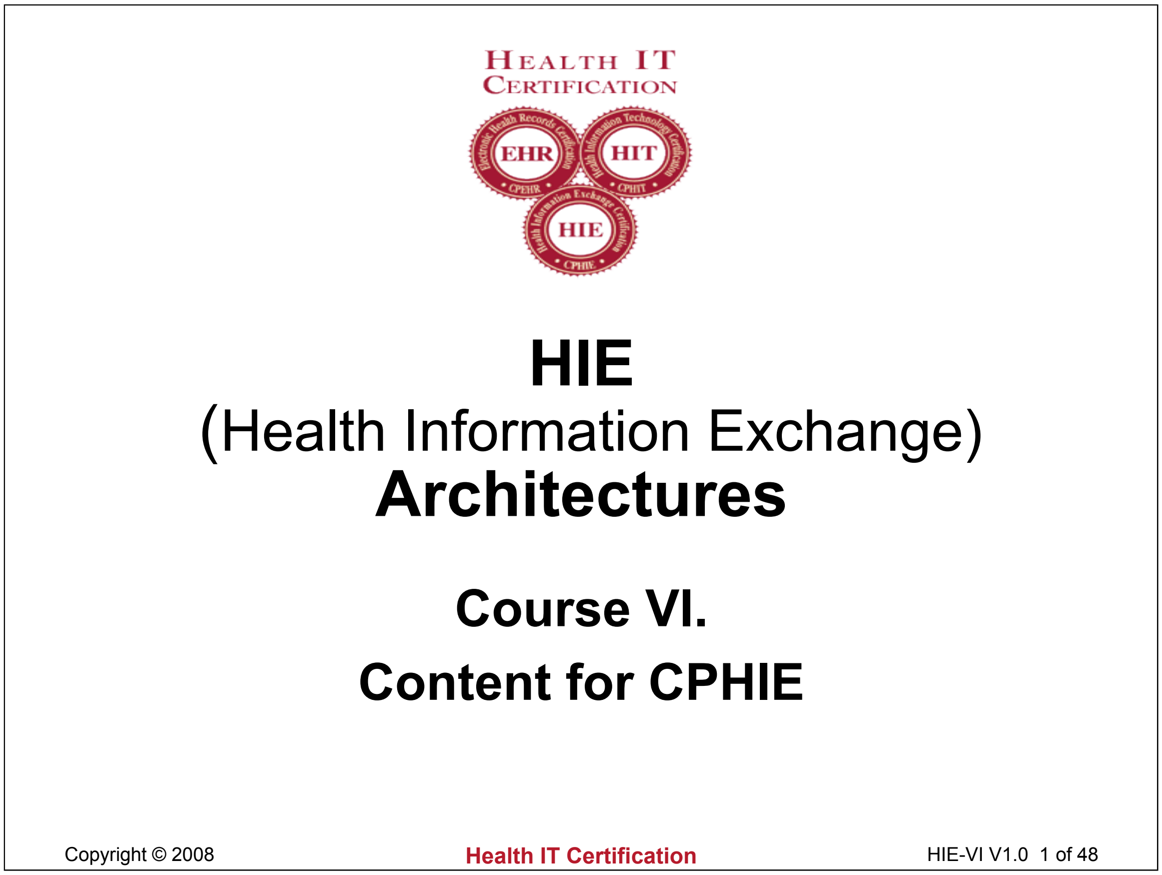


HEALTH IT CERTIFICATION

HIE
(Health Information Exchange)
Architectures

Course VI.
Content for CPHIE

Copyright © 2008 Health IT Certification HIE-VI V1.0 1 of 48

Welcome to the Health IT Certification program on Health Information Exchange (HIE) Architectures. This is the second of the six courses in the Certified Professional in Health Information Exchange (CPHIE) track. Other courses in this track cover:

V - HIE Goals and Governance
VII - Data Stewardship
VIII - Personal Health Records
IX - Telehealth and Home Monitoring
X - Nationwide Health Information Network

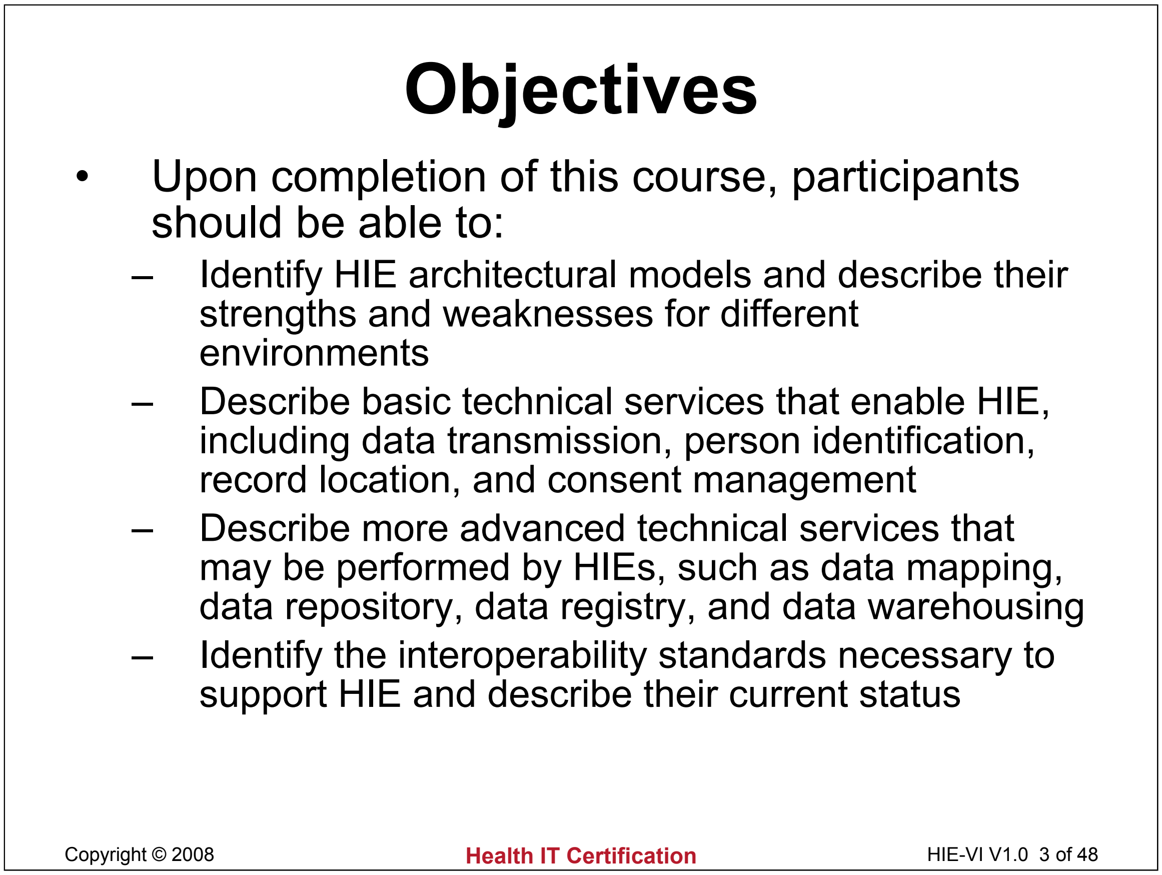
Introducing . . .

Margret Amatayakul, MBA, CPEHR, CPHIT, RHIA, CHPS, FHIMSS
President, Margret\A Consulting, LLC; Adjunct Faculty, College of St. Scholastica; formerly with CPRI; AHIMA; associate professor, University of Illinois. Schaumburg, IL

W. Holt Anderson
Executive Director, North Carolina Healthcare Information and Communications Alliance, Inc., Research Triangle Park, NC

Atif Zafar, MD
Associate Professor of Medicine, Indiana University School of Medicine, Affiliated Scientist, Regenstrief Institute, Inc., Academic Staff, AHRQ, National Resource Center for Health IT, Indianapolis, IN

Steven S. Lazarus, PhD, CPEHR, CPHIT, FHIMSS
President, Boundary Information, Member, Board of Examiners, Health IT Certification, LLC, Past Chair, Workgroup on Electronic Data Interchange, Denver, CO

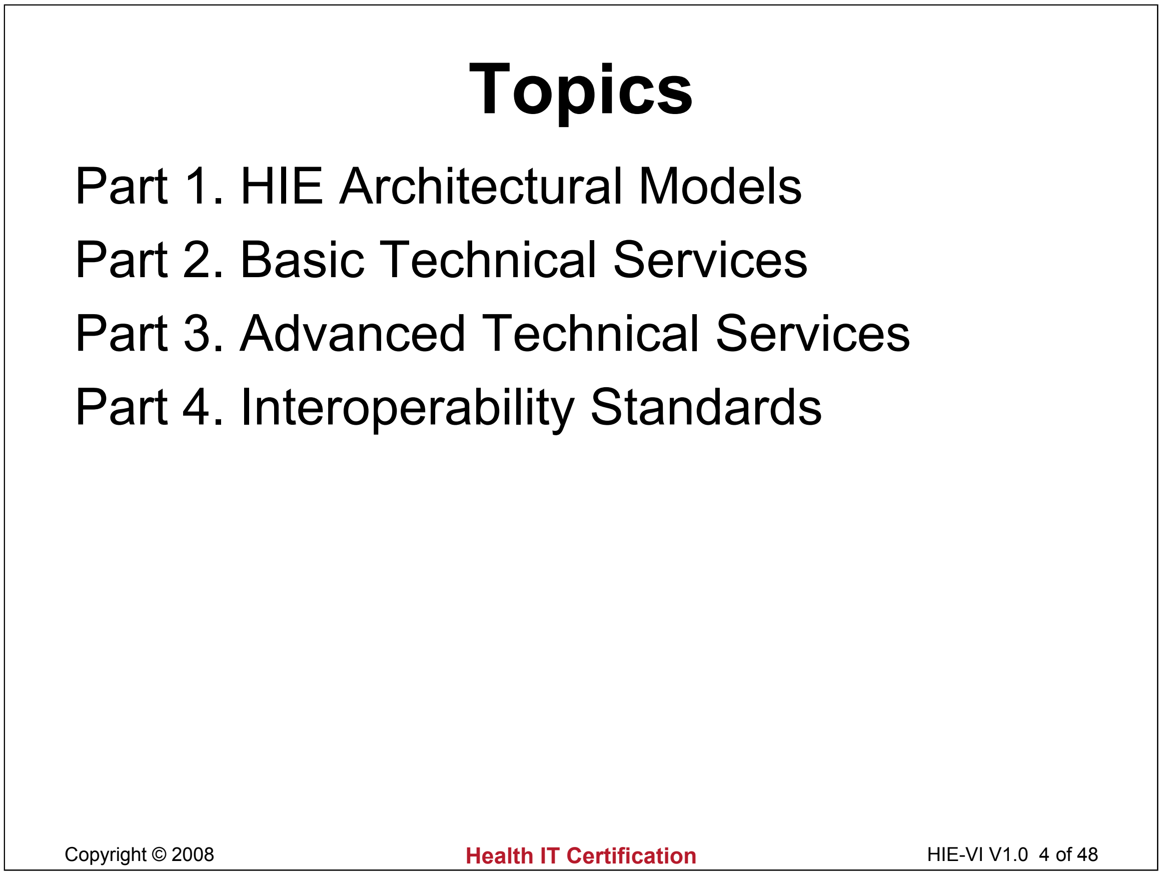


Objectives

- Upon completion of this course, participants should be able to:
  - Identify HIE architectural models and describe their strengths and weaknesses for different environments
  - Describe basic technical services that enable HIE, including data transmission, person identification, record location, and consent management
  - Describe more advanced technical services that may be performed by HIEs, such as data mapping, data repository, data registry, and data warehousing
  - Identify the interoperability standards necessary to support HIE and describe their current status

Health IT Certification

The objectives of the HIE Architectures Course include describing the various architectural models deployed by HIE organizations, discussing their suitability for different environments, exploring the technical services that may be performed by HIEs to achieve their missions, and identifying interoperability standards that especially apply to HIE.



Topics

Part 1. HIE Architectural Models

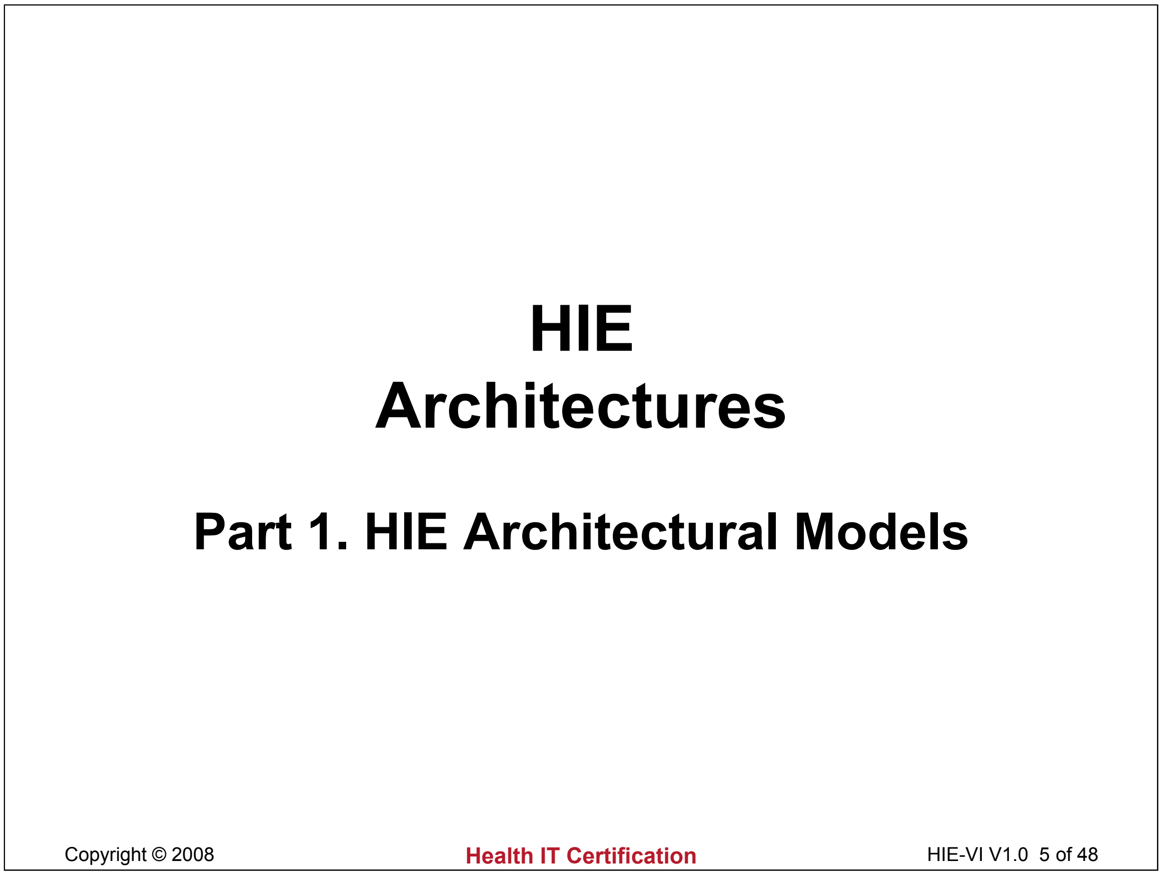
Part 2. Basic Technical Services

Part 3. Advanced Technical Services

Part 4. Interoperability Standards

Copyright © 2008 **Health IT Certification** HIE-VI V1.0 4 of 48

Whether new to HIE or working in an existing HIE, topics covered in this Course should help you consider HIE architectural models at any phase of your planning or evolution, basic and advanced technical services, and current status of interoperability standards – a topic that probably changes faster than any other in relationship to HIE!



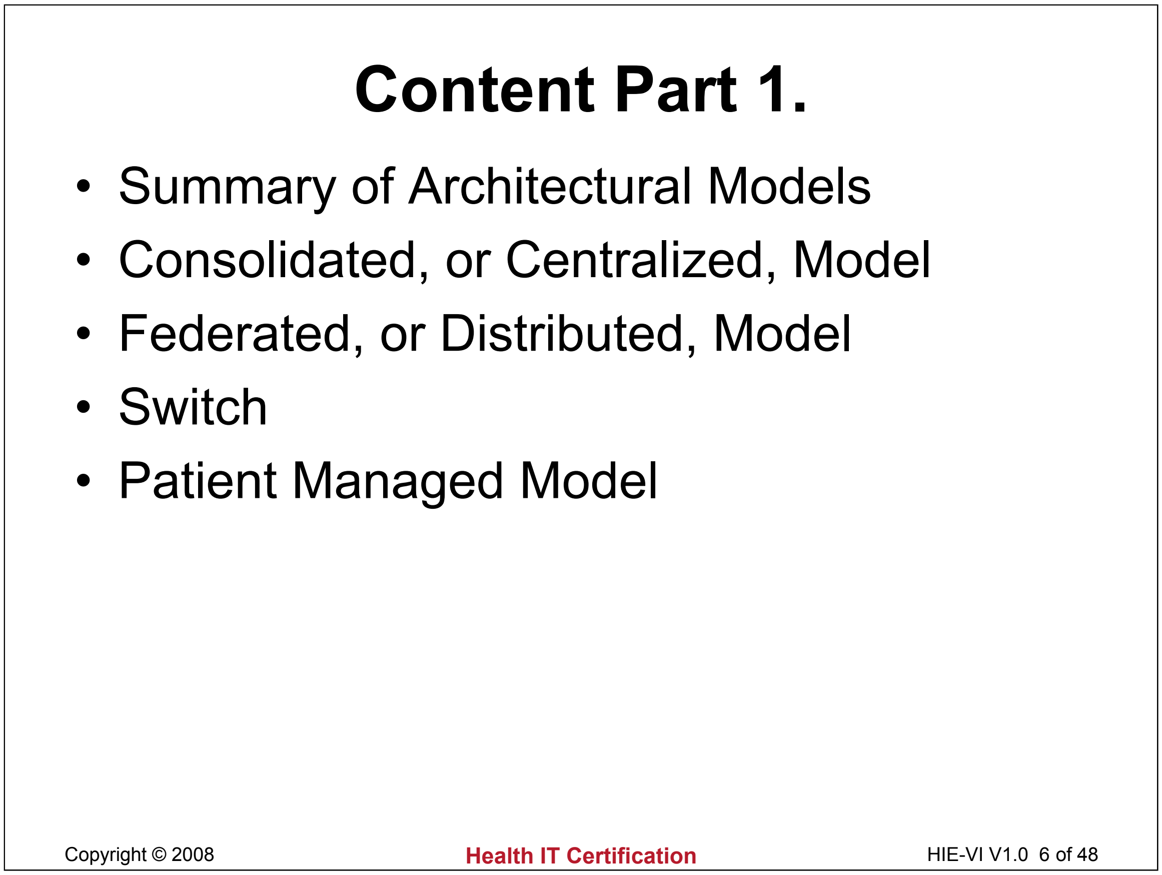
HIE Architectures

Part 1. HIE Architectural Models

Health IT Certification

HIE-VI V1.0 5 of 48

Although it can truly be said that “if you’ve seen one HIE, you’ve seen one HIE,” Part 1. of the HIE Architecture Course reviews the major categories of architectures being deployed by HIEs and discusses how various HIEs may evolve and find suitable architectures as each new phase in HIE is undertaken.

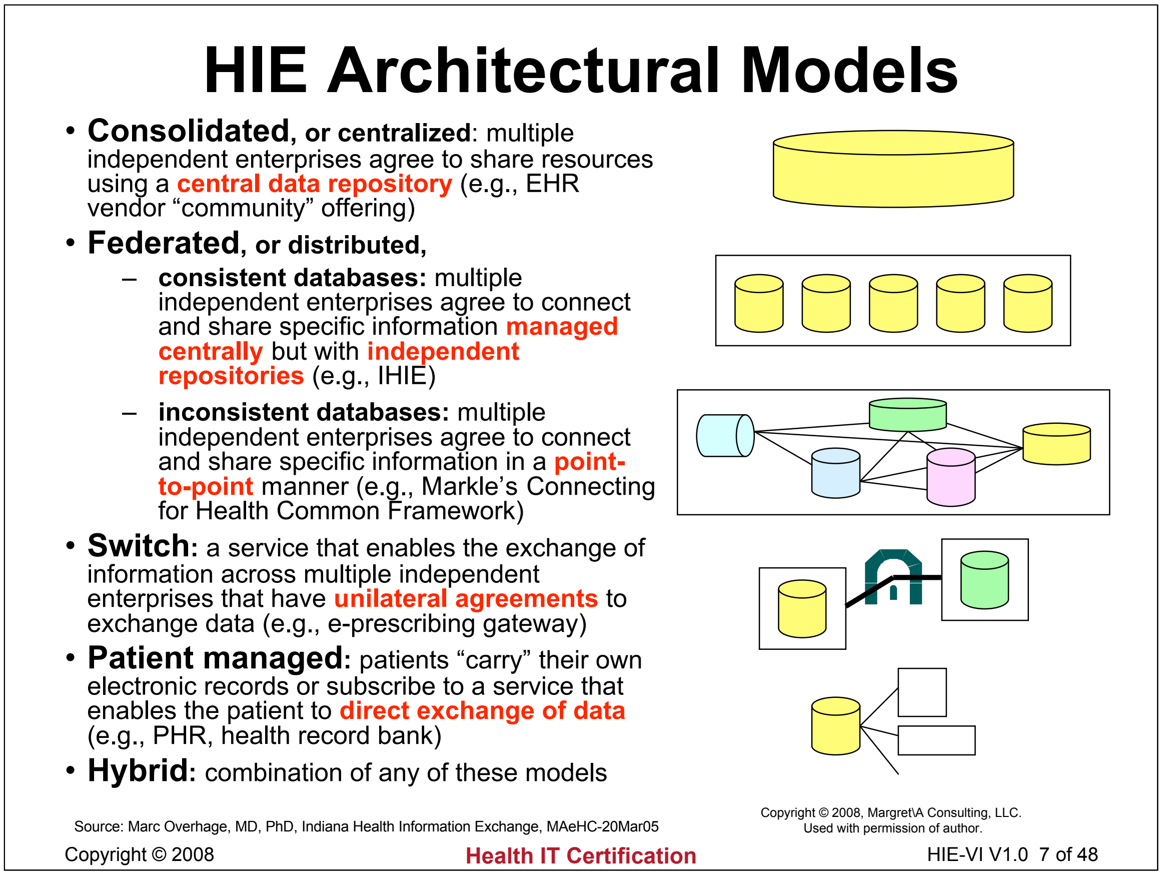


Content Part 1.

- Summary of Architectural Models
- Consolidated, or Centralized, Model
- Federated, or Distributed, Model
- Switch
- Patient Managed Model

Copyright © 2008 **Health IT Certification** HIE-VI V1.0 6 of 48

A brief overview of the major architectural models of HIEs is provided, then a closer look at the four major types: consolidated, federated, switch, and patient managed, recognizing that most HIEs are a hybrid of some or all of the architectures.



HIE Architectural Models

- **Consolidated, or centralized**: multiple independent enterprises agree to share resources using a **central data repository** (e.g., EHR vendor "community" offering)
- **Federated, or distributed,**
  - **consistent databases:** multiple independent enterprises agree to connect and share specific information **managed centrally** but with **independent repositories** (e.g., IHIE)
  - **inconsistent databases:** multiple independent enterprises agree to connect and share specific information in a **point-to-point** manner (e.g., Markle's Connecting for Health Common Framework)
- **Switch**: a service that enables the exchange of information across multiple independent enterprises that have **unilateral agreements** to exchange data (e.g., e-prescribing gateway)
- **Patient managed**: patients "carry" their own electronic records or subscribe to a service that enables the patient to **direct exchange of data** (e.g., PHR, health record bank)
- **Hybrid**: combination of any of these models

Source: Marc Overhage, MD, PhD, Indiana Health Information Exchange, MAeHC-20Mar05

Copyright © 2008, Margret\A Consulting, LLC.
Used with permission of author.

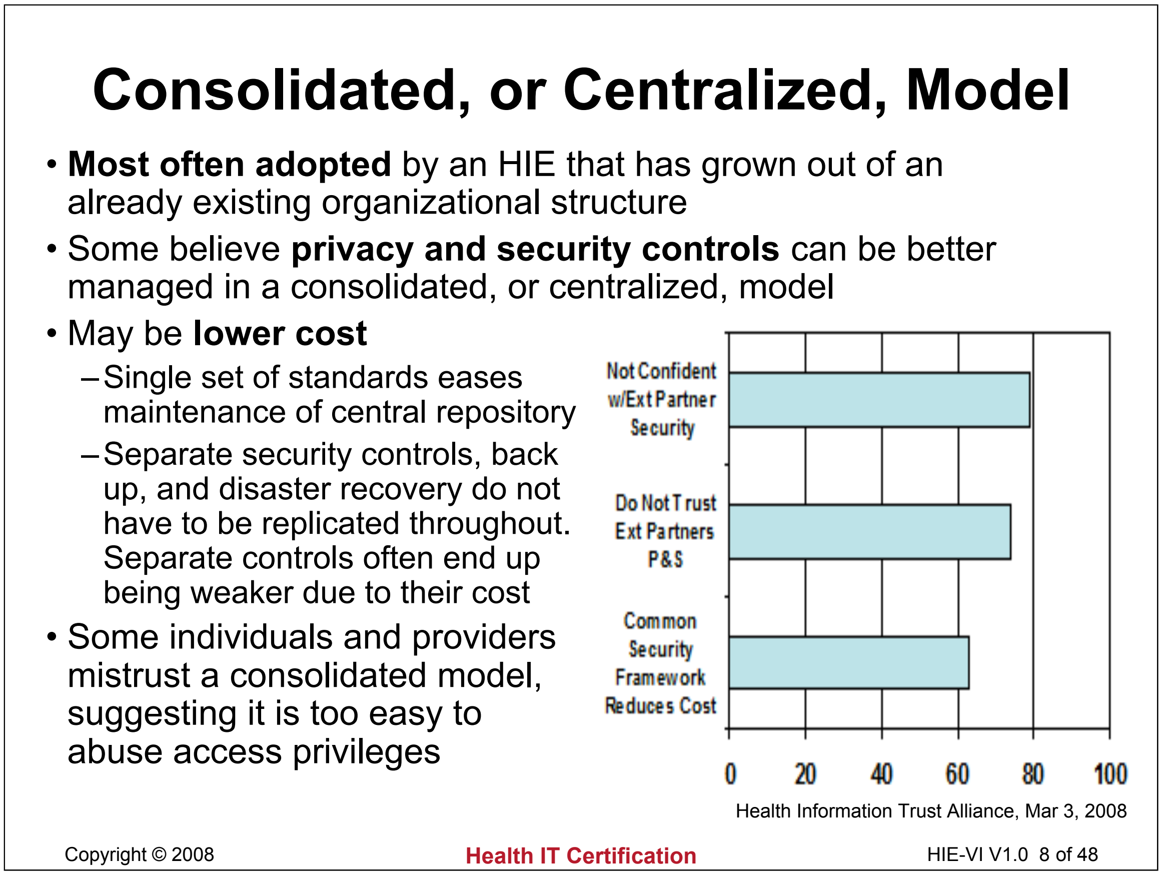
Copyright © 2008 Health IT Certification HIE-VI V1.0 7 of 48

At a very high level, most HIE organizations predominantly adopt one of three architectural models:

1. The consolidated model has a central repository to manage most of the information exchange. Some of EHR vendors are promoting this model, sometimes called a "community offering." In this case, one, generally large facility such as a hospital, implements an EHR and serves as the host for affiliated providers or others to acquire the EHR functionality. A central data repository maintains all information; access controls establish who may have access to what information; but there are not separate records for each provider treating the patient.
2. In general, the federated model is one in which multiple organizations exchange information without a centralized repository to maintain the data. There are two flavors: one where the patient would essentially have separate records from each provider organization but all are managed by a single organization; and another where the patient would have separate records at separate provider organizations, each maintained separately. The consistent database version is very much like an application service provider (ASP) for information systems, or a bank vault, where everyone has their own deposit box but all in one big vault. The inconsistent database version is much like we operate today – every provider has its own records, but instead of mailing information to another provider, it is exchanged electronically.
3. The hybrid approach is a combination of consolidated and federated, where components of both models are present. While in reality many HIEs have some elements of both architectures, an HIE is generally not identified as a hybrid model unless one of the other two do not predominate.

In addition to these models, there is the model that essentially is a switching service, or third party that enables exchange of information without the formation of a convening organization, such as a regional health information organization. An e-prescribing gateway might be classified as a switch, because any applicable organization can subscribe. Some HIE organizations have actually set as their goal to help start up the formation of HIE services and then go away, with the switch providing the service everyone has agreed upon. This is an interesting vision that is too early to determine viability.

A patient managed model of HIE is also emerging. When a personal health record (PHR) or other such structure is used as the basis for the HIE organization, it typically is like either of the federated models, but patients are more active in directing the exchange of information through a consent process.



Consolidated, or Centralized, Model

- **Most often adopted** by an HIE that has grown out of an already existing organizational structure
- Some believe **privacy and security controls** can be better managed in a consolidated, or centralized, model
- May be **lower cost**
  - Single set of standards eases maintenance of central repository
  - Separate security controls, back up, and disaster recovery do not have to be replicated throughout. Separate controls often end up being weaker due to their cost
- Some individuals and providers mistrust a consolidated model, suggesting it is too easy to abuse access privileges

Not Confident w/Ext Partner Security
Do Not Trust Ext Partners P&S
Common Security Framework Reduces Cost
0
20
40
60
80
100

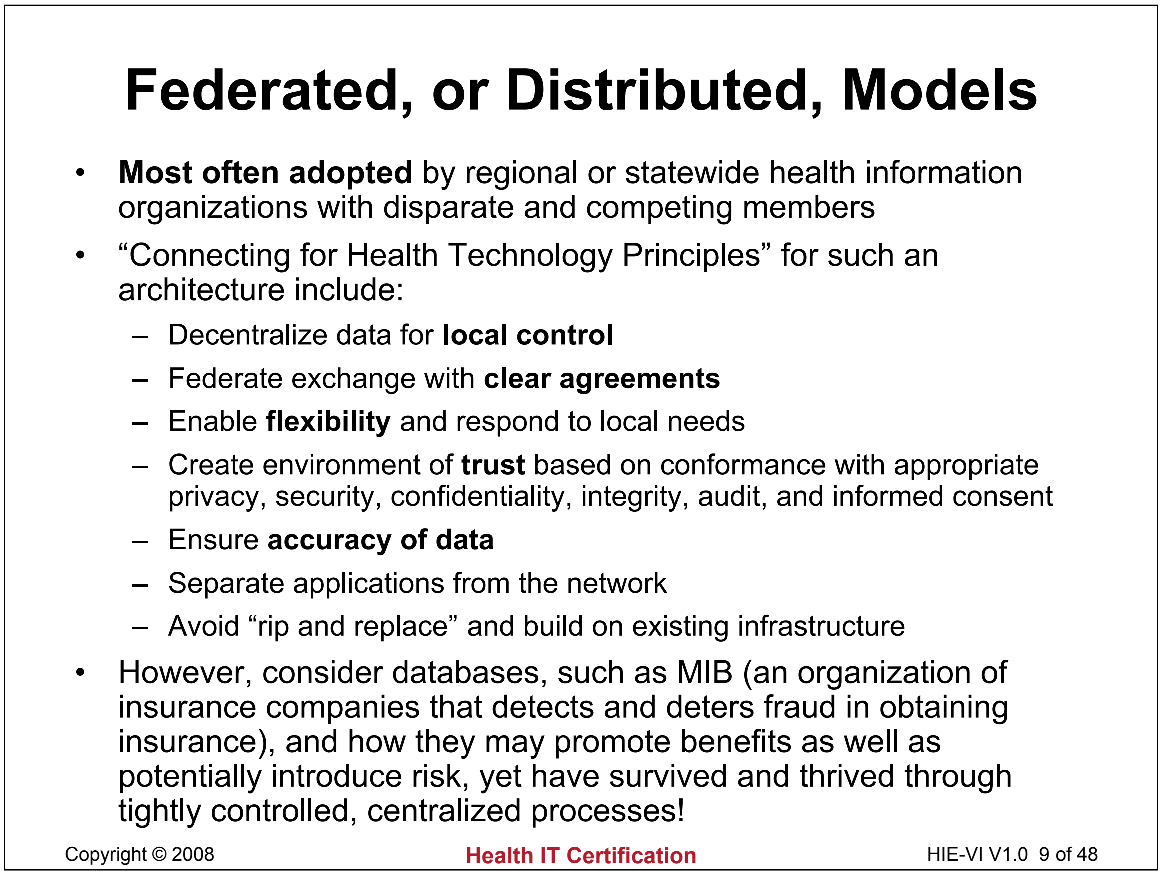
Health Information Trust Alliance, Mar 3, 2008

Copyright © 2008 **Health IT Certification** HIE-VI V1.0 8 of 48

Looking at each model more closely, it appears that the consolidated model is one that is most frequently adopted by an HIE organization that essentially has grown out of an already existing organizational structure – which may be as tight as a commonly owned integrated delivery network (IDN), moderately integrated such as an academic medical center (ACM) where faculty may be closely aligned with but still a separate organizational entity, or loosely linked as an organized health care arrangement (OHCA) or other form of collaborative, especially in small/rural communities where distances are great, competition is minimal, sharing of providers is common, and other common bonds exist, such as group purchasing.

There is some controversy over whether such a model can be more or less secure than the federated model. Some believe a consolidated approach enables everyone to share a single robust set of security technologies, which in many cases few of the individual participants could afford to put into place on their own. A central master person index (MPI) assigns unique identification, significantly reducing the risk of accessing the wrong person's data. There is a strong incentive for the vendor or host to assure security, or risk going out of business. A recent survey conducted by the Health Information Trust Alliance suggests that trust concerns are as high as 60 to 80% when sharing data with partners – a consolidated approach could essentially eliminate the partner relationship since all security is controlled centrally.

Lack of trust in partners' privacy and security (P&S) is a critical issue that must be addressed as HIE organizations consider which architectural model to adopt. In fact, the model chosen might be a hybrid because there are benefits and risks to each. As an HIE organization evolves and trust is enhanced through building relationships, as discussed in the CPHIE Course VI on Goals and Governance, the architectural model may also shift with new lines of business.



Federated, or Distributed, Models

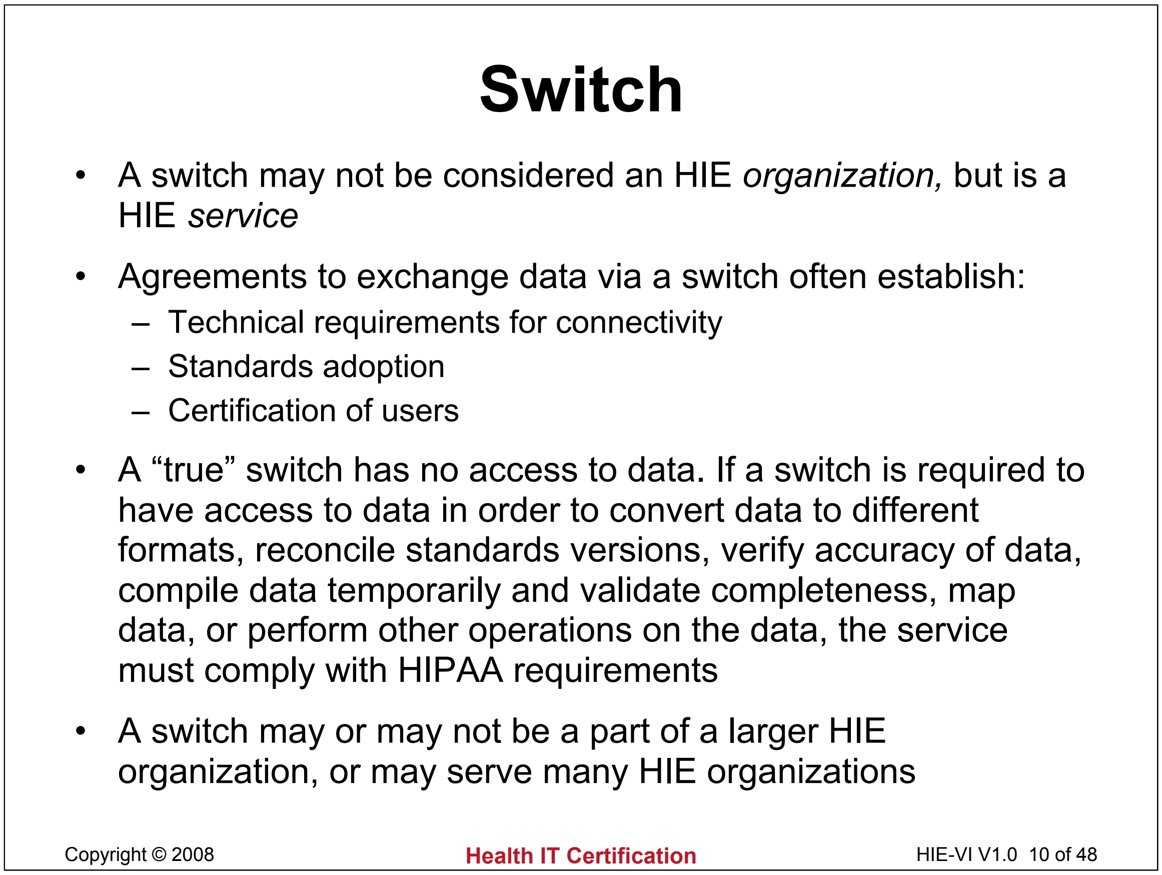
- **Most often adopted** by regional or statewide health information organizations with disparate and competing members
- “Connecting for Health Technology Principles” for such an architecture include:
  - Decentralize data for **local control**
  - Federate exchange with **clear agreements**
  - Enable **flexibility** and respond to local needs
  - Create environment of **trust** based on conformance with appropriate privacy, security, confidentiality, integrity, audit, and informed consent
  - Ensure **accuracy of data**
  - Separate applications from the network
  - Avoid “rip and replace” and build on existing infrastructure
- However, consider databases, such as MIB (an organization of insurance companies that detects and deters fraud in obtaining insurance), and how they may promote benefits as well as potentially introduce risk, yet have survived and thrived through tightly controlled, centralized processes!

Copyright © 2008 Health IT Certification HIE-VI V1.0 9 of 48

The federated model, and actually the inconsistent database configuration version of the federated model, is the one that seems to be most popular today. The Markle Foundation’s Connecting for Health is a strong proponent of this model and has developed some technology principles for this architecture.

For those who believe that the consolidated model can better enhance security, they might also argue that local control reduces security to the lowest common denominator, or at least results in weaknesses within the chain of trust among the partners – so that the “security chain” becomes only as strong as the weakest link. It often appears that the federated model seems stronger because only “part” of a single person’s information might be at risk at a single point in time. As it is unlikely that there will ever be a totally consolidated model for everyone throughout the nation – for many reasons – these principles can be useful to address in any HIE organization.

One issue that should be borne in mind when evaluating the federated approach is that today, there are already very large databases of information that exist about the health care of many people in the nation. Several of these were identified in the CPHIE Course V: HIE Goals and Governance. Another example is the MIB Group, Inc. once known as the "Medical Information Bureau“ (www.mib.com). It is a membership organization of over 600 insurance companies that has been in continuous operation for over 105 years pursuing its primary mission of detecting and deterring fraud that may occur in the course of obtaining life, health, disability income, critical illness, and long-term care insurance. MIB saves its member companies an estimated $1 billion annually. These savings may be passed on to insurance buying consumers in the form of lower premiums (and higher dividends payable by mutual companies). MIB may also be used to help a family locate unclaimed life insurance policy death benefits. MIB files do *not* include the totality of one's medical records as held by a health care provider. Rather the files consist of codes signifying certain health conditions and lifestyle choices that insurance companies consider significant. The code translation is tightly maintained. The MIB is *not* subject to HIPAA. It is a consumer reporting agency subject to the federal Fair Credit Reporting Act (FCRA), that affords certain rights, including the ability to obtain a free report and the right to have erroneous information corrected.



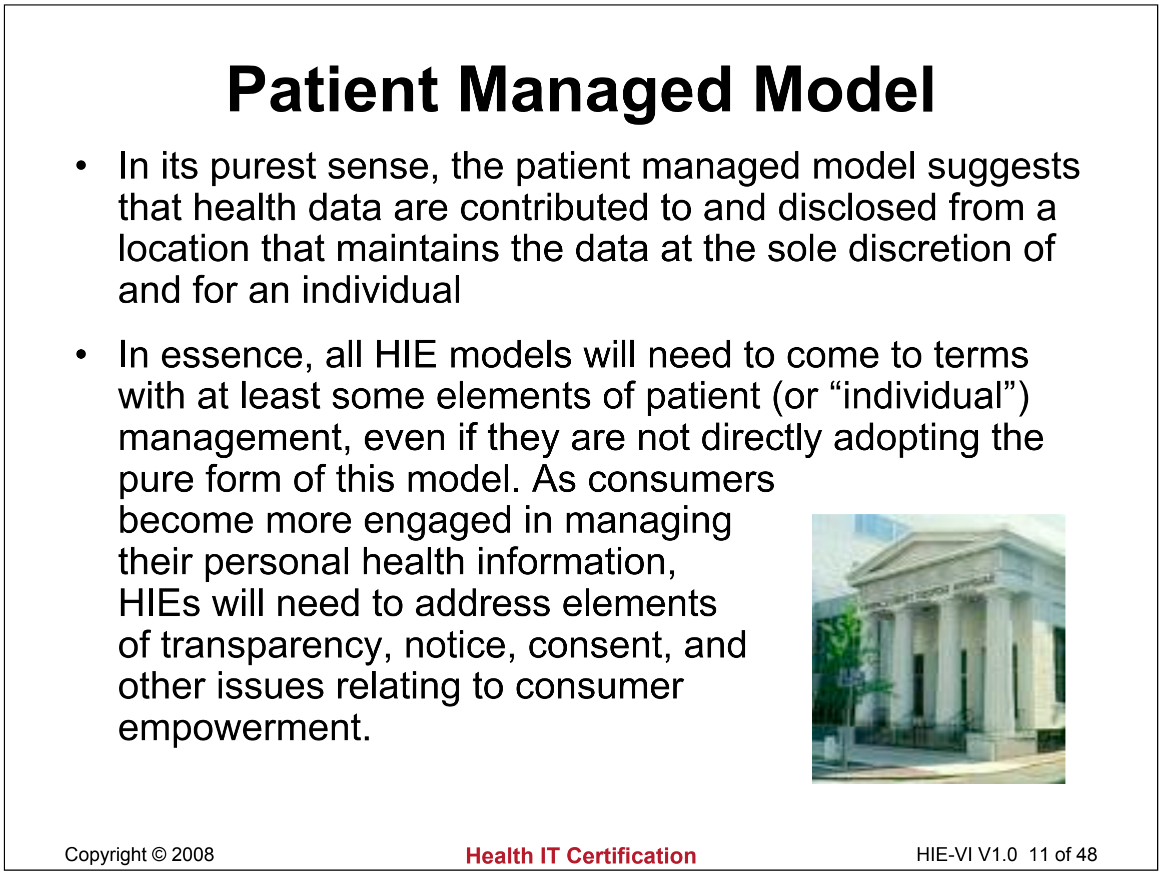
Switch

- A switch may not be considered an HIE *organization,* but is a HIE *service*
- Agreements to exchange data via a switch often establish:
  - Technical requirements for connectivity
  - Standards adoption
  - Certification of users
- A “true” switch has no access to data. If a switch is required to have access to data in order to convert data to different formats, reconcile standards versions, verify accuracy of data, compile data temporarily and validate completeness, map data, or perform other operations on the data, the service must comply with HIPAA requirements
- A switch may or may not be a part of a larger HIE organization, or may serve many HIE organizations

Copyright © 2008 **Health IT Certification** HIE-VI V1.0 10 of 48

Technically, a switch is a computer networking device that connects network segments. The term, however, is also used sometimes synonymously with a clearinghouse, or company that provides data transmission services. For example, banks use automated clearinghouses (ACH) to manage the dispersion of funds where checks have been written. In healthcare, clearinghouses are used to distribute claims to the myriad of payers from which providers expect reimbursement. An e-prescribing gateway is another example of a switch, or clearinghouse, that routes prescription transactions to designated pharmacies.

Healthcare clearinghouses are HIPAA covered entities because they are expected to convert non-standard claims and other financial and administrative transactions to standard formats, and back. As such, they “open the envelope” of the claim and have access to its information. Just as e-prescribing gateways also supply standards conversion services but were not initially considered part of the HIPAA definition of healthcare clearinghouse, other such forms of switches will evolve to perform various roles. Many of them are already considered business associates by HIPAA covered entities, yet they may also argue that they do not access data if they truly are performing only the switching function.



Patient Managed Model

- In its purest sense, the patient managed model suggests that health data are contributed to and disclosed from a location that maintains the data at the sole discretion of and for an individual
- In essence, all HIE models will need to come to terms with at least some elements of patient (or “individual”) management, even if they are not directly adopting the pure form of this model. As consumers become more engaged in managing their personal health information, HIEs will need to address elements of transparency, notice, consent, and other issues relating to consumer empowerment.

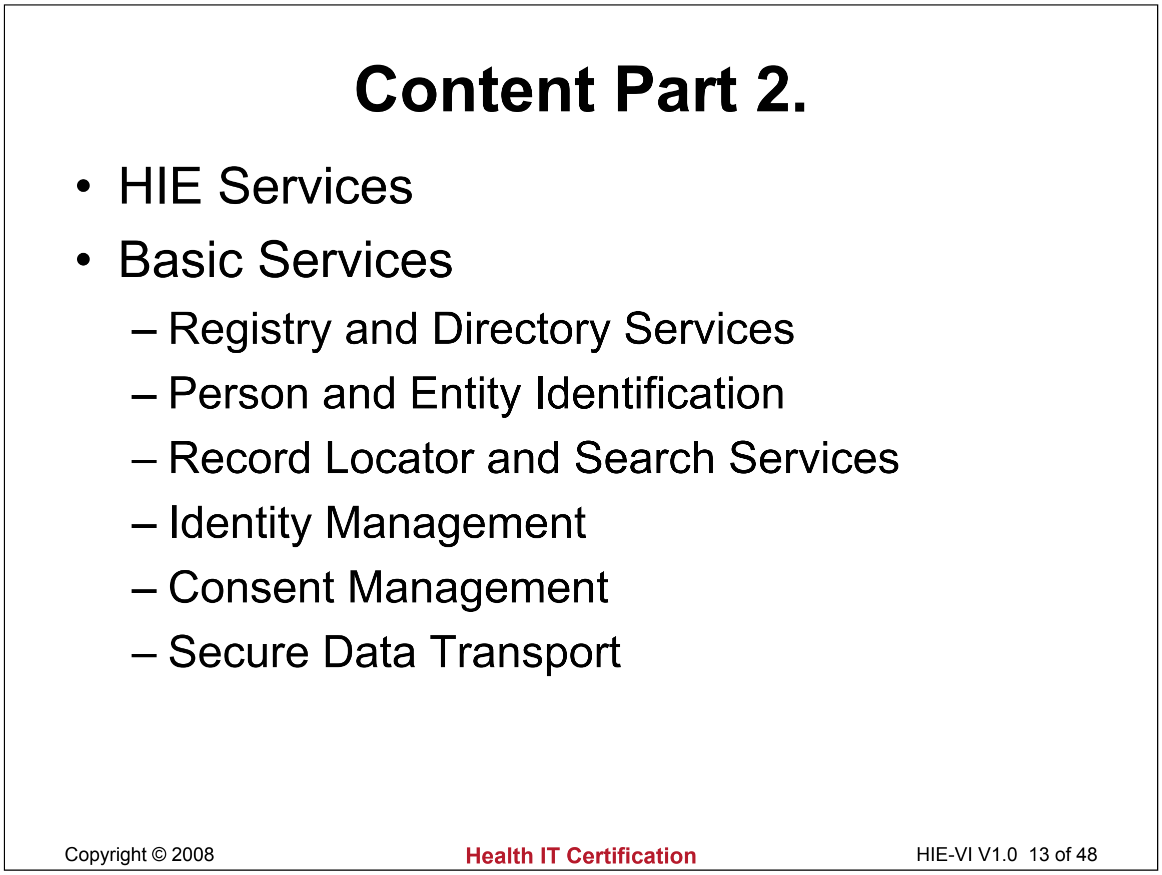
The patient managed model is today considered a separate HIE model, although certainly most HIE organizations are looking to add patient consent and other individual control elements as part of the HIE architecture they are adopting.

The patient managed model is considered a separate model because some HIEs are organizing themselves explicitly around a personal health record, health record bank, or other such structure – in comparison to provider driven models.

HIE Architectures

Part 2. Basic Technical Services

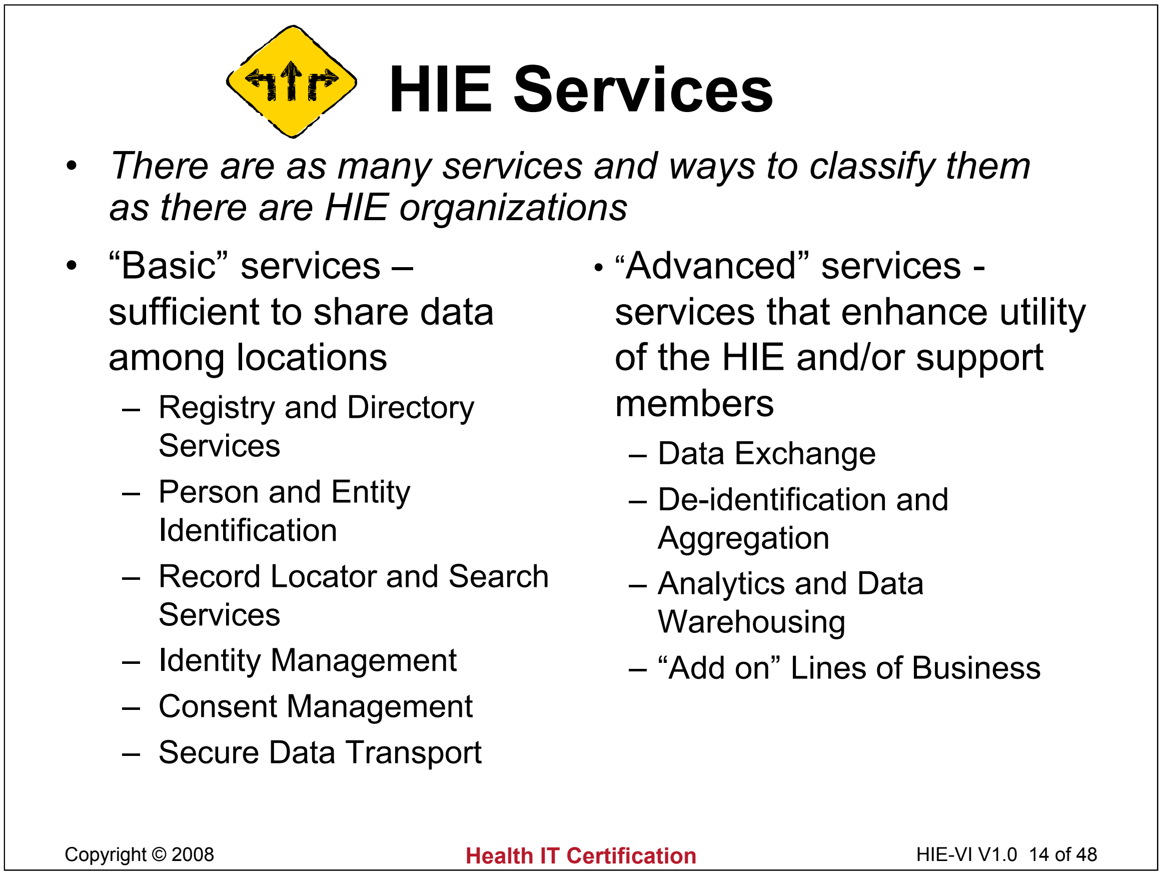
Although there are variations in how some of the basic technical services may be deployed in different architectures, each of the architectural models must deploy at least some elements of the basic technical services discussed in Part 2. of this Course.



Content Part 2.

- HIE Services
- Basic Services
  - Registry and Directory Services
  - Person and Entity Identification
  - Record Locator and Search Services
  - Identity Management
  - Consent Management
  - Secure Data Transport

This Part of the Course begins with an overview comparison of basic and more advanced technical services; then explores the basic services in more depth.



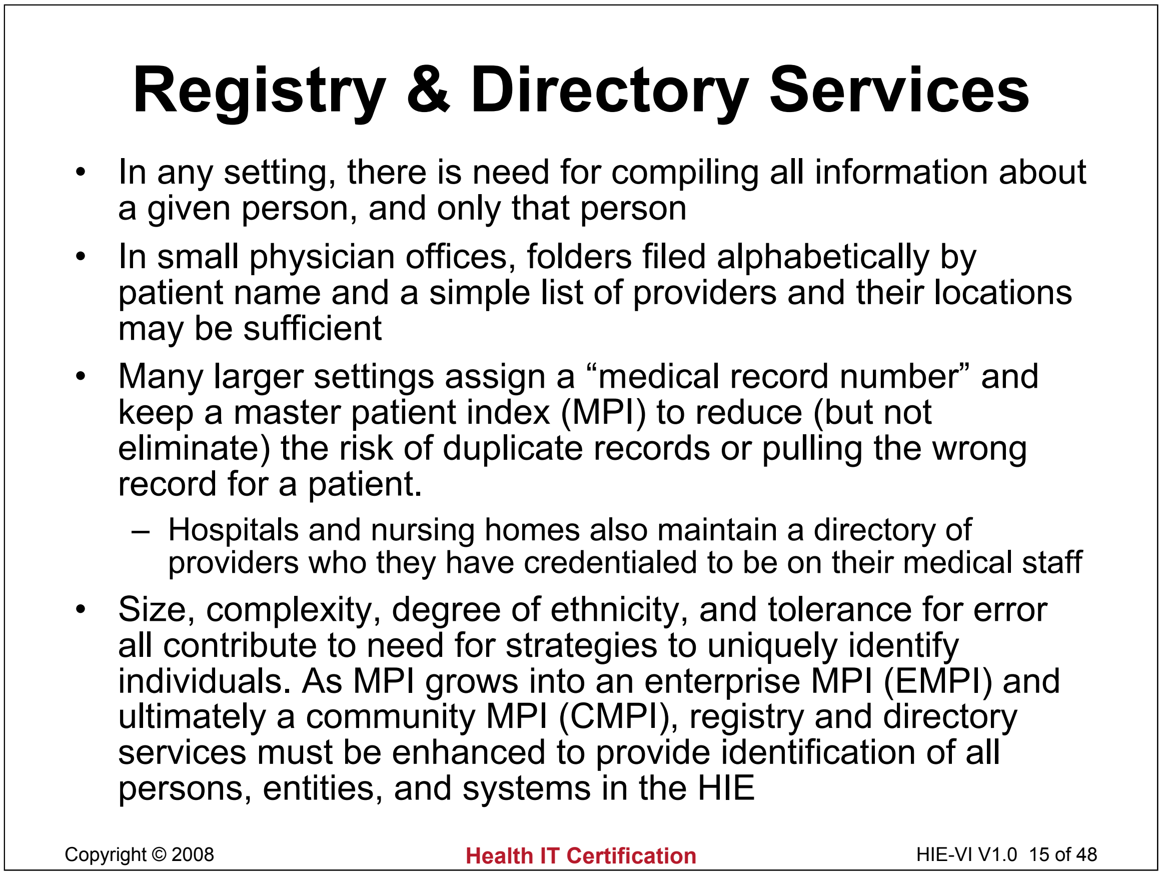
HIE Services

- *There are as many services and ways to classify them as there are HIE organizations*
- “Basic” services – sufficient to share data among locations
  - Registry and Directory Services
  - Person and Entity Identification
  - Record Locator and Search Services
  - Identity Management
  - Consent Management
  - Secure Data Transport
- “Advanced” services - services that enhance utility of the HIE and/or support members
  - Data Exchange
  - De-identification and Aggregation
  - Analytics and Data Warehousing
  - “Add on” Lines of Business

Health IT Certification HIE-VI V1.0 14 of 48

While there are potentially many services that an HIE organization can provide, those which are basic, or fundamental, to enabling data sharing among disparate organizations generally relate to the ability to identify the individual about whom information is sought, find where that information may be located, ensure that only authorized entities or systems have access to the data sought in accordance with the individual’s consent, and send the data in a secure manner that is logged and auditable.

In addition, HIE organizations may decide they want to support more advanced services. In order to ensure that data exchange is meaningful, a variety of vocabulary and code set standardization requirements and data mapping services may be necessary. Many HIE organizations want to enhance protection of the data they exchange, not only through technical security services, including encryption, but want to de-identify the data in some form – depending upon whether they are exchanging data with HIPAA covered entities and business associates, or outside of HIPAA protections. One of the most important purposes of an HIE other than the ability to provide better access to data for direct patient care is to warehouse and aggregate the data and support analysis for quality measurement, reporting, and improvement; research; and other uses of merit. Finally, there are other lines of business an HIE organization may consider adding for various purposes, including as a source of revenue, and each such service has certain technical requirements.



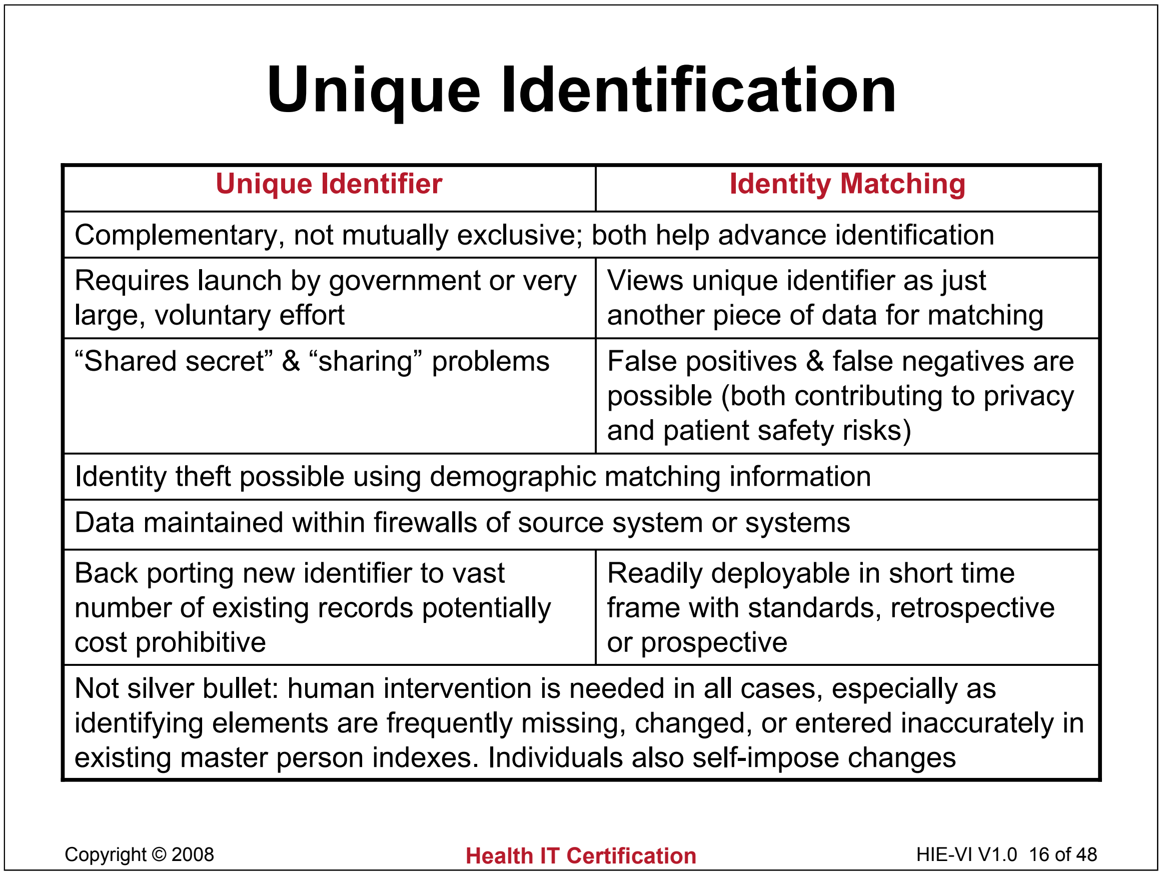
Registry & Directory Services

- In any setting, there is need for compiling all information about a given person, and only that person
- In small physician offices, folders filed alphabetically by patient name and a simple list of providers and their locations may be sufficient
- Many larger settings assign a “medical record number” and keep a master patient index (MPI) to reduce (but not eliminate) the risk of duplicate records or pulling the wrong record for a patient.
  - Hospitals and nursing homes also maintain a directory of providers who they have credentialed to be on their medical staff
- Size, complexity, degree of ethnicity, and tolerance for error all contribute to need for strategies to uniquely identify individuals. As MPI grows into an enterprise MPI (EMPI) and ultimately a community MPI (CMPI), registry and directory services must be enhanced to provide identification of all persons, entities, and systems in the HIE

Copyright © 2008 **Health IT Certification** HIE-VI V1.0 15 of 48

Registry and directory services support the ability to identify individuals. Virtually every organization has some form of index, registry, or directory of patients they treat, members for whom they supply health plan benefits, or citizens counted in a community census. As an HIE organization forms, the ability to identify individuals (and locate their records) requires a process to manage the identification process. This is much more difficult to accomplish in an HIE than even a very large MPI in an integrated delivery network or other environment that uses the same patient registration system throughout. In an HIE, the participants generally do not change their internal ways of assigning medical record numbers. Some of the participants may not even have a formal MPI. Even with an MPI, the type of demographic data collected may vary, the quality of data captured may vary, and the rigor with which duplicates are purged internally may vary.

As registry and directory services are approached by an HIE organization, there are many issues to incorporate in policy and procedure, including the assignment of internal identifiers and change control. For example, when a member of an HIE confirms an address change, is that shared with all of the other HIE participants or is it only updated in the HIE’s registry? Furthermore, is the change date/time stamped, so a change is not made back to an old address.



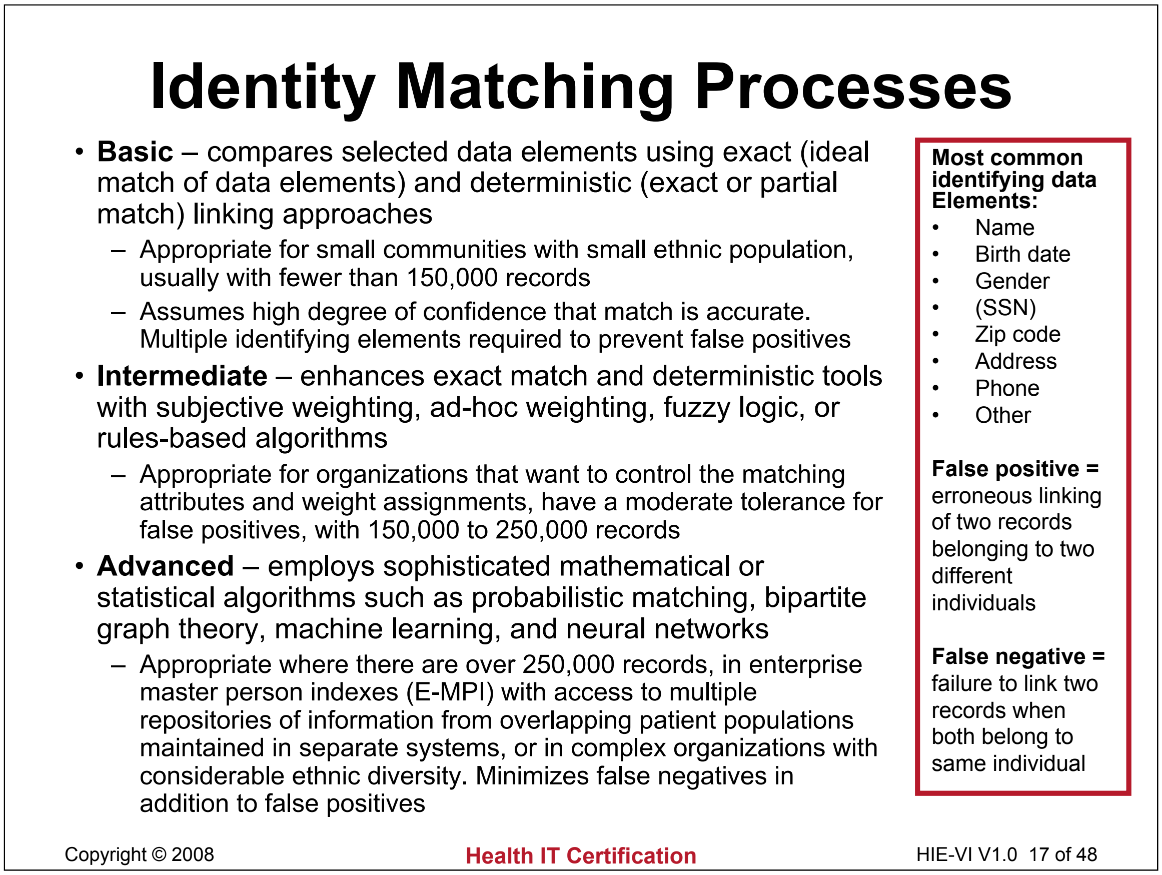
Unique Identification

Unique Identifier	Identity Matching
Complementary, not mutually exclusive; both help advance identification	
Requires launch by government or very large, voluntary effort	Views unique identifier as just another piece of data for matching
“Shared secret” & “sharing” problems	False positives & false negatives are possible (both contributing to privacy and patient safety risks)
Identity theft possible using demographic matching information	
Data maintained within firewalls of source system or systems	
Back porting new identifier to vast number of existing records potentially cost prohibitive	Readily deployable in short time frame with standards, retrospective or prospective
Not silver bullet: human intervention is needed in all cases, especially as identifying elements are frequently missing, changed, or entered inaccurately in existing master person indexes. Individuals also self-impose changes	

Health IT Certification

Although many call for a unique health identifier, the U.S. has been reluctant to invoke the HIPAA requirement for issuing such an identifier due to privacy concerns. While those calling for such an identifier believe security is strengthened through a unique identifier used exclusively for health care purposes, others believe a single identifier will be misused. This comparison of a unique identifier vs. a matching process to identify individuals illustrates that the two means for identification are actually complimentary, and that neither method provides an absolute, right answer.

In addition to the controversy surrounding whether a unique identifier is appropriate or not, there is also no consensus on whether either method is more cost effective. Proponents argue that a unique identifier would be expensive to implement up front, but save money over time. Opponents believe that at best the cost might be equivalent. Opponents argue a unique identifier will not only have a large up front cost, but will have some ongoing maintenance costs. These costs are unknown and could be more or less than the cost of continual identity matching. Of course, the cost of identity matching could be reduced by adoption of standards demographics and more sophisticated, and standardized, matching algorithms.



Identity Matching Processes

- **Basic** – compares selected data elements using exact (ideal match of data elements) and deterministic (exact or partial match) linking approaches
  - Appropriate for small communities with small ethnic population, usually with fewer than 150,000 records
  - Assumes high degree of confidence that match is accurate. Multiple identifying elements required to prevent false positives
- **Intermediate** – enhances exact match and deterministic tools with subjective weighting, ad-hoc weighting, fuzzy logic, or rules-based algorithms
  - Appropriate for organizations that want to control the matching attributes and weight assignments, have a moderate tolerance for false positives, with 150,000 to 250,000 records
- **Advanced** – employs sophisticated mathematical or statistical algorithms such as probabilistic matching, bipartite graph theory, machine learning, and neural networks
  - Appropriate where there are over 250,000 records, in enterprise master person indexes (E-MPI) with access to multiple repositories of information from overlapping patient populations maintained in separate systems, or in complex organizations with considerable ethnic diversity. Minimizes false negatives in addition to false positives

Most common identifying data Elements:
- Name
- Birth date
- Gender
- (SSN)
- Zip code
- Address
- Phone
- Other

False positive = erroneous linking of two records belonging to two different individuals

False negative = failure to link two records when both belong to same individual

Copyright © 2008 **Health IT Certification** HIE-VI V1.0 17 of 48

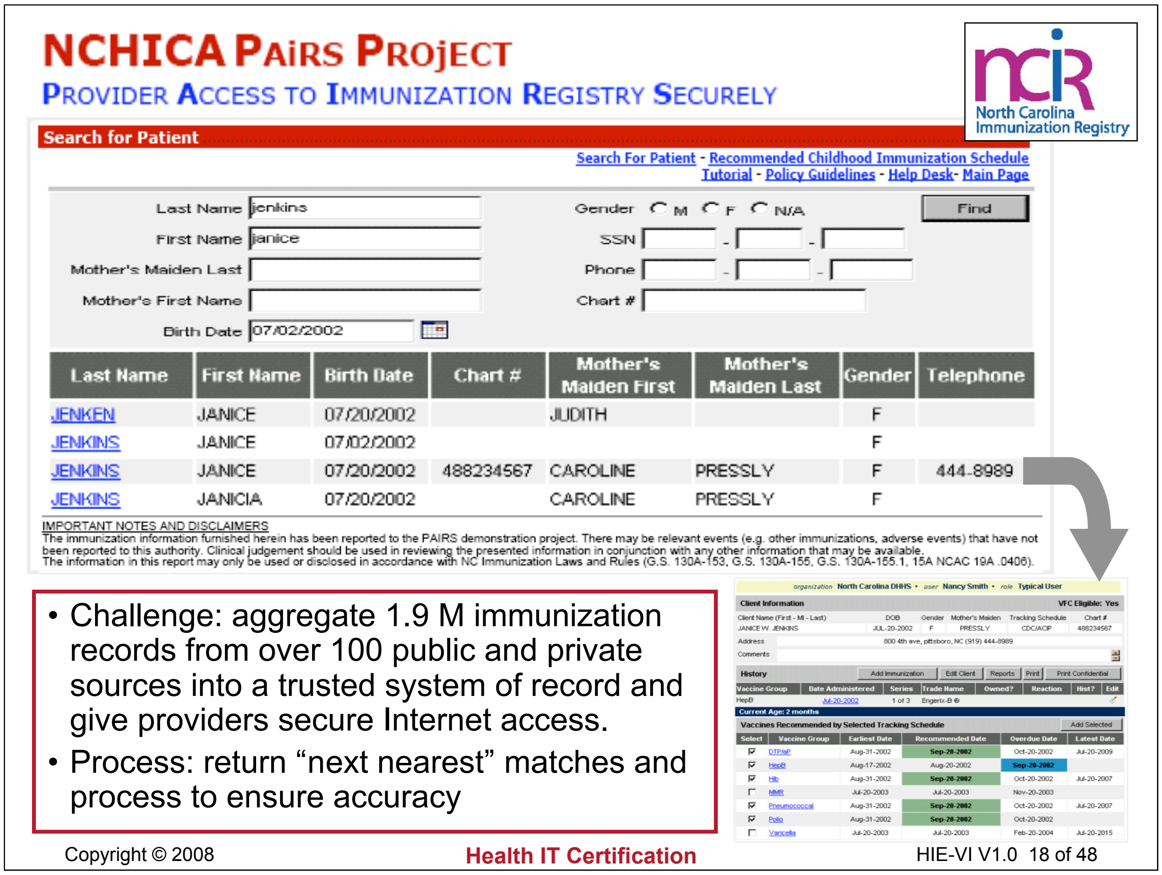
Matching individuals so that a positive identification can be determined is as much a science as it is an art. The process can require highly sophisticated mathematical or statistical algorithms to reduce false positives and false negatives. The size and characteristics of individuals to be identified determine the level of sophistication that may be needed. And, health care is not alone in this challenge. Initiate Systems, Inc., a company that supplies customer data integration (CDI) services, observes that the retail sector, for example, faces the very same challenges as in health care, although false-positive thresholds may be different than those for the health care sector.

In a survey of 21 HIEs reported on in January 2006, the American Health Information Management Association (AHIMA) found that basic linking techniques most frequently compare name, birth date, Social Security number, or gender, using exact (requiring identical match of data elements) or deterministic (exact or partial match requiring human intervention) linking approaches. Intermediate approaches in larger HIEs include:

- Subjective weighting, where users apply rules to score field match based on significance
- Ad hoc weighting that applies numeric values that indicate the overall importance of a comparison relative to other comparisons
- Fuzzy logic that, in this context, involves using rules built to emulate common errors made by users, such as transposing digits, using Soundex encoding for names, swapping data elements (e.g., first and last name, month and day of birth), or searching for any date of birth within five years.

Advance matching techniques may utilize:

- Probabilistic matching is matching that increases or decreases the field weight match based upon frequency of the data (e.g., decreasing the field weight match score if Smith were common in the population)
- Bipartite graph theory uses mathematical graphs to determine similarity of data between strings of data that models human similarity.
- Machine learning is a discipline that involves pattern recognition to model human decision making.
- Neural networks employ machine learning in an iterative process.



NCHICA PAiRS PROJECT

PROVIDER ACCESS TO IMMUNIZATION REGISTRY SECURELY

Search for Patient

Search For Patient - Recommended Childhood Immunization Schedule
Tutorial - Policy Guidelines - Help Desk- Main Page

Last Name	jenkins	Gender	○ M ○ F ○ N/A
First Name	janice	SSN	_ - _ - _
Mother's Maiden Last		Phone	_ - _ - _
Mother's First Name		Chart #	
Birth Date	07/02/2002		

Last Name	First Name	Birth Date	Chart #	Mother's Maiden First	Mother's Maiden Last	Gender	Telephone
JENKEN	JANICE	07/20/2002		JUDITH		F	
JENKINS	JANICE	07/02/2002				F	
JENKINS	JANICE	07/20/2002	488234567	CAROLINE	PRESSLY	F	444-8989
JENKINS	JANICIA	07/20/2002		CAROLINE	PRESSLY	F	

IMPORTANT NOTES AND DISCLAIMERS
The immunization information furnished herein has been reported to the PAIRS demonstration project. There may be relevant events (e.g. other immunizations, adverse events) that have not been reported to this authority. Clinical judgement should be used in reviewing the presented information in conjunction with any other information that may be available.
The information in this report may only be used or disclosed in accordance with NC Immunization Laws and Rules (G.S. 130A-153, G.S. 130A-155, G.S. 130A-155.1, 15A NCAC 19A .0406).

- Challenge: aggregate 1.9 M immunization records from over 100 public and private sources into a trusted system of record and give providers secure Internet access.
- Process: return "next nearest" matches and process to ensure accuracy

organization **North Carolina DHHS** • *user* **Nancy Smith** • *role* **Typical User**

Client Information **VFC Eligible: Yes**

Client Name (First - MI - Last)	DOB	Gender	Mother's Maiden	Tracking Schedule	Chart #
JANICE W. JENKINS	JUL-20-2002	F	PRESSLY	CDC/ACIP	488234567

Address: 800 4th ave, pittsboro, NC (919) 444-8989
Comments:

History

Vaccine Group	Date Administered	Series	Trade Name	Owned?	Reaction	Hist?	Edit
HepB	Jul-20-2002	1 of 3	Engerix-B ®				✎

Current Age: 2 months

Vaccines Recommended by Selected Tracking Schedule

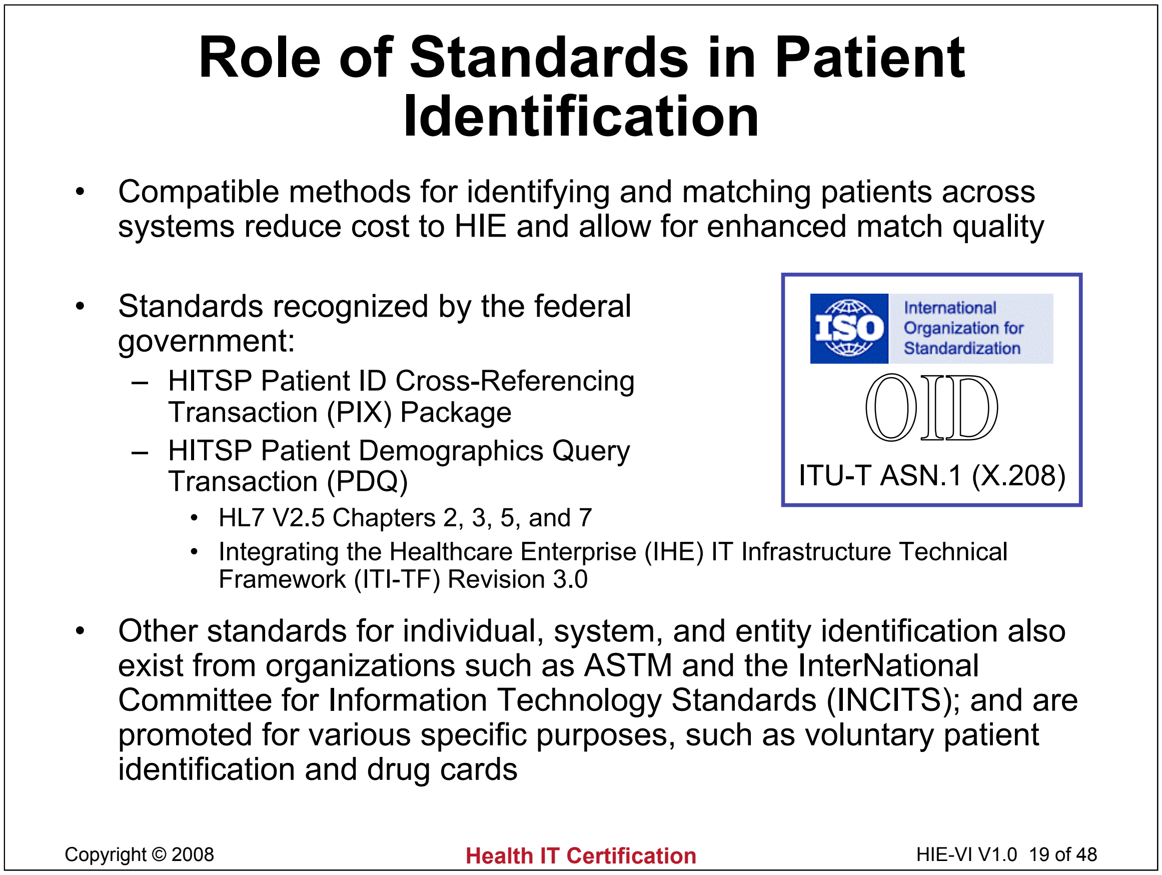
Select	Vaccine Group	Earliest Date	Recommended Date	Overdue Date	Latest Date
☑	DTP/aP	Aug-31-2002	**Sep-20-2002**	Oct-20-2002	Jul-20-2009
☑	HepB	Aug-17-2002	Aug-20-2002	**Sep-20-2002**	
☑	Hib	Aug-31-2002	**Sep-20-2002**	Oct-20-2002	Jul-20-2007
☐	MMR	Jul-20-2003	Jul-20-2003	Nov-20-2003	
☑	Pneumococcal	Aug-31-2002	**Sep-20-2002**	Oct-20-2002	Jul-20-2007
☑	Polio	Aug-31-2002	**Sep-20-2002**	Oct-20-2002	
☐	Varicella	Jul-20-2003	Jul-20-2003	Feb-20-2004	Jul-20-2015

Copyright © 2008 **Health IT Certification** HIE-VI V1.0 18 of 48

The North Carolina Healthcare Information and Communications Alliance, Inc. (NCHICA), is a nonprofit organization that champions the adoption of IT to improve health care. Its members include leading organizations in healthcare, research, and IT. NCHICA leads demonstration projects, hosts educational sessions, fosters collaborative efforts, and supports initiatives that promote HIT.

Through a Federal Preventative Health Services Immunization Grant and nearly $1M worth of in-kind goods and services, NCHICA members developed a database, built Internet access, installed strong security, and committed to support the operation of a pilot Provider Access to Immunization Registry Securely (PAiRS) service. While it does not have all the functionality of an immunization registry, it offered providers access to child immunization data contained in the North Carolina Immunization Registry (NCIR), as well as immunization data from Blue Cross and Blue Shield of North Carolina and Kaiser Permanente. The Initiate Identity Hub™ software was the underlying technology used to match and link similar immunization records with the PAiRS system. Lessons learned from the PAiRS project included the need for a strong clinical champion (i.e., the Secretary of the NC DHHS who was a pediatrician); cost-effective results (the total state outlay was $79,000 annually after the 3 year demonstration); digital certifications for identity authentication of users that are portable, since providers move among different machines in their clinical settings; and a broad range of state-based organizations to provide leadership and consensus for change.

As part of the challenge in building PAiRS, NCHICA needed to match the identities of children throughout the state from over 100 public and private sources. Of special interest was the decision to return "next nearest" matches and create a manual process to ensure accurate final identification. While this process may not be applicable when time is of the essence in an emergency department, for instance, the process did provide highly accurate conclusions.



Role of Standards in Patient Identification

- Compatible methods for identifying and matching patients across systems reduce cost to HIE and allow for enhanced match quality
- Standards recognized by the federal government:
  - HITSP Patient ID Cross-Referencing Transaction (PIX) Package
  - HITSP Patient Demographics Query Transaction (PDQ)
    - HL7 V2.5 Chapters 2, 3, 5, and 7
    - Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 3.0
- Other standards for individual, system, and entity identification also exist from organizations such as ASTM and the InterNational Committee for Information Technology Standards (INCITS); and are promoted for various specific purposes, such as voluntary patient identification and drug cards

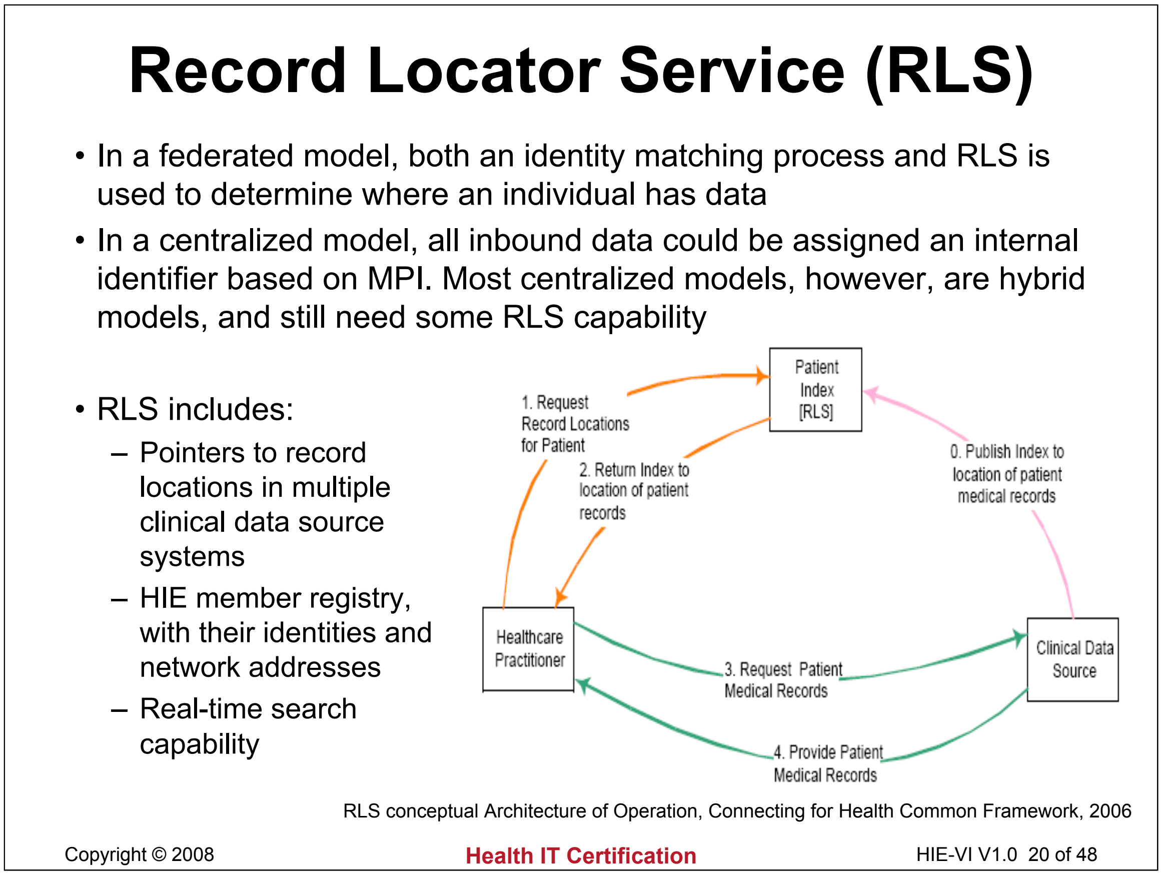
ISO International Organization for Standardization

OID

ITU-T ASN.1 (X.208)

Standards to enable identification and matching of patients across systems reduce cost and enhance match quality (i.e., ensuring a positive identification). The standards recommended by the Health Information Technology Standard Panel (HITSP) include two within the Integrating the Healthcare Enterprise (IHE) framework, and rely on HL7 messages with additional PID segment constraints, including use, *only*, of the ISO object identifier (OID) for an assigning authority's universal ID type. Object identifiers are strings of numbers, allocated in a hierarchical manner, used in a variety of protocols. The formal definition of OID comes from the ITU-T recommendation ASN.1 (X.208). The International Telecommunications Union – Telecommunication Standardization Sector (ITU-T) develops standards for all forms of telecommunications, including for telephone numbers, sending a text message between mobile phones (using the SMS [Short Message Service] communication protocol), or receiving streaming video to a computer. HL7 and other health care information interchange standards, use OIDs for globally unique identifiers for individual information objects as well as references to code systems and data element dictionaries. The Centers for Disease Control and Prevision (CDC) has adopted OIDs to manage the many complex value sets used in public health. The various OIDs are available in the Public Health Information Network (PHIN) Vocabulary Access and Distribution System (VADS). In computer security, OIDs serve to name almost every object type in X.509 certificates (for digital signatures).

It is also observed that in addition to these recommended standards, there are other identifier standards in existence and being developed. For example, E1714-00 Standard Guide for Properties of a Universal Healthcare Identifier from the standards development organization ASTM (www.astm.org). It recommends an encrypted universal healthcare identifier (EUHID) for patients to address clinical information fragmentation and privacy issues. In 2007, ASTM provided additional information on implementing the Universal Healthcare Identifier in a voluntary manner (the Voluntary National Healthcare Identifier [VNHID]). The Workgroup on Electronic Data Interchange (WEDI) has also recommended an Implementation Guide for a Standard ID Card, based on a new revision of the ISO Standard INCITS 284, expected to be balloted in mid-2008 and available in the U.S. from ANSI (www.ansi.org). The National Council for Prescription Drug Programs (NCPDP) applies INCITS 284 to Drug Benefit Cards in its Implementation Guide. Part 4. of this Course provides additional information on healthcare standards development organizations – and clearly, the need for standards harmonization!



Record Locator Service (RLS)

- In a federated model, both an identity matching process and RLS is used to determine where an individual has data
- In a centralized model, all inbound data could be assigned an internal identifier based on MPI. Most centralized models, however, are hybrid models, and still need some RLS capability
- RLS includes:
  - Pointers to record locations in multiple clinical data source systems
  - HIE member registry, with their identities and network addresses
  - Real-time search capability

Patient Index [RLS]

1. Request Record Locations for Patient

2. Return Index to location of patient records

0. Publish Index to location of patient medical records

Healthcare Practitioner

Clinical Data Source

3. Request Patient Medical Records

4. Provide Patient Medical Records

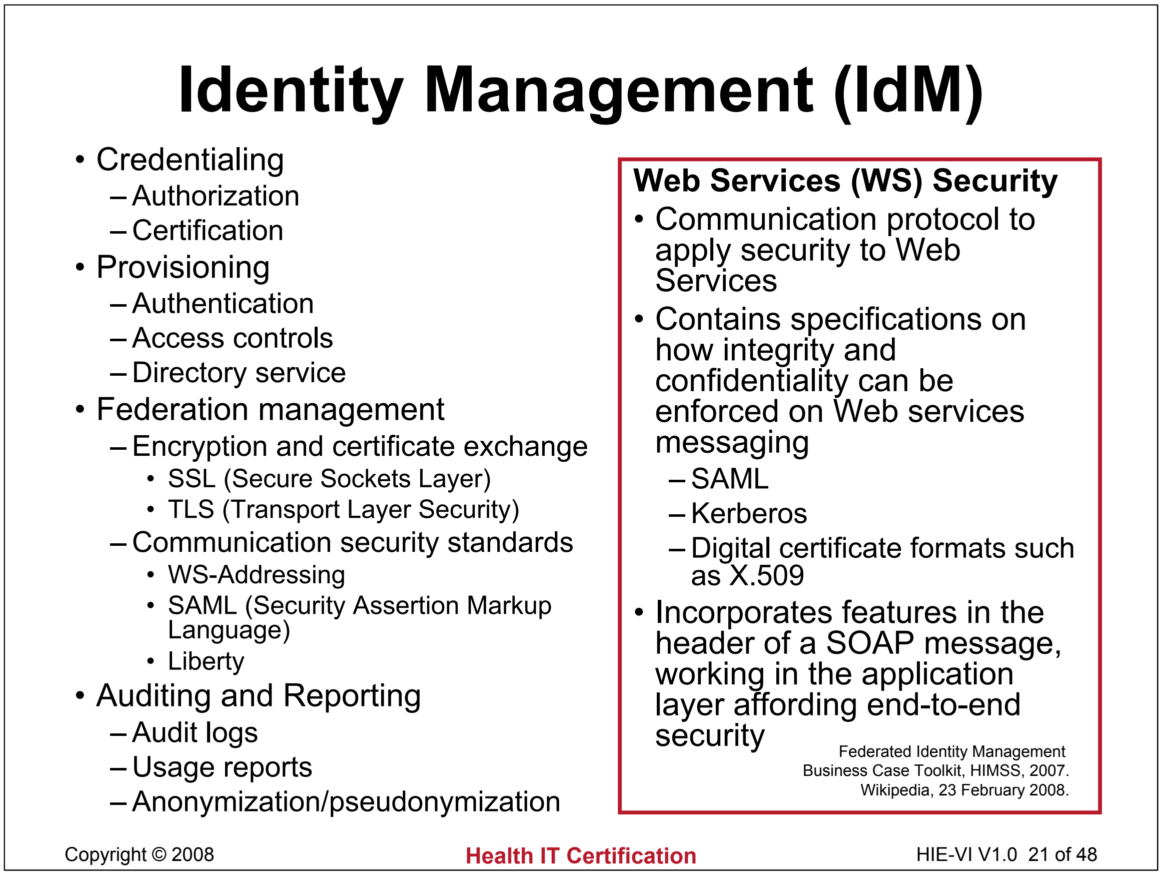
RLS conceptual Architecture of Operation, Connecting for Health Common Framework, 2006

Copyright © 2008 **Health IT Certification** HIE-VI V1.0 20 of 48

Identification is only one of several elements in the ability for an HIE to exchange data on individual patients. While an HIE organization with a centralized architecture may not need a separate record locator service (RLS), those with federated architectures need a means to identify where records for a given patient, once identified, exist. Very often, an HIE with a centralized architecture will have an enhanced master person index (MPI) that will identify the nature of the records available, such as that there are records for several admissions at two different hospitals and visits to three different clinics. Such a system may more likely be deployed when the HIE is focused more on document rather than data exchange, as documents will be indexed by electronic folder.

In whatever architecture uses or requires a RLS, it is an extension of the directory and identity matching process. In a federated architecture, the identification process may be initiated locally, but without some form of HIE-assigned internal identifier, the RLS adds another layer of identification and then pointers to where records exist.

A RLS also identifies HIE members (as a separate process, indicated in the diagram as “0.Publish index to location of patient medical records”). So just as there must be an index of all individual patients who are registered in the locator service, so too must there be the identities and network addresses of record locations. Depending on the more granular architecture of any given member, the identity of the members may be the member enterprise, or may be various applications within it, such as Hospital A’s lab (for results), Hospital A’s radiology department (for reports and PACS images), Hospital A’s emergency department (for ED records), and Hospital A’s medical record department (for all other documents and/or data).



Identity Management (IdM)

- Credentialing
  - Authorization
  - Certification
- Provisioning
  - Authentication
  - Access controls
  - Directory service
- Federation management
  - Encryption and certificate exchange
    - SSL (Secure Sockets Layer)
    - TLS (Transport Layer Security)
  - Communication security standards
    - WS-Addressing
    - SAML (Security Assertion Markup Language)
    - Liberty
- Auditing and Reporting
  - Audit logs
  - Usage reports
  - Anonymization/pseudonymization

Web Services (WS) Security

- Communication protocol to apply security to Web Services
- Contains specifications on how integrity and confidentiality can be enforced on Web services messaging
  - SAML
  - Kerberos
  - Digital certificate formats such as X.509
- Incorporates features in the header of a SOAP message, working in the application layer affording end-to-end security

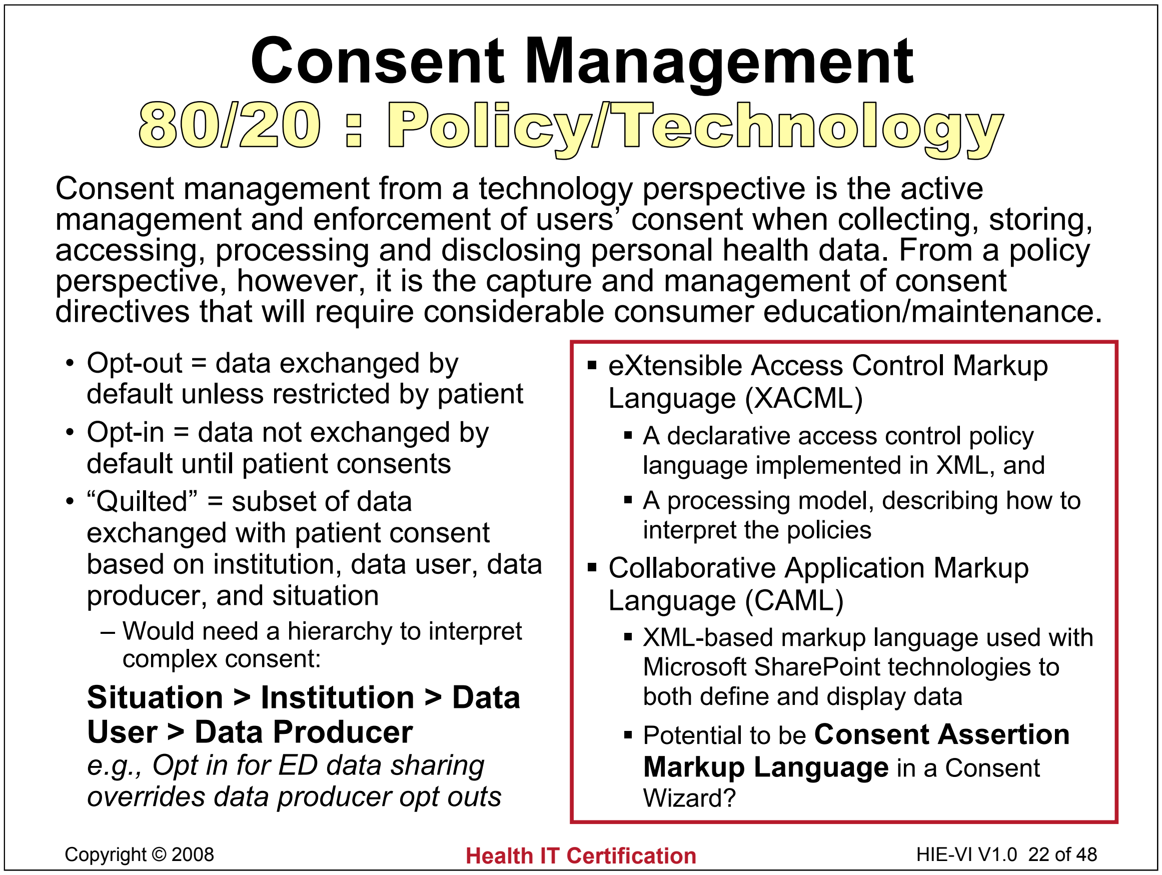
Federated Identity Management Business Case Toolkit, HIMSS, 2007.
Wikipedia, 23 February 2008.

Once identification and record location are determined, the next service evoked by an HIE is identity management. These are the security services that include affirmation that a user of the HIE is authorized, or certified, to gain access to the HIE, also referred to as a credentialing process. This is usually a one-time process, although it may change as the role of the user may change, and certainly when a user is terminated and when new users are added. Within HIPAA, this process is a combination of the Privacy Rule's minimum necessary standard and the Security Rule's information access management standard that incorporates access authorization, establishment, and modification. Another security service incorporated in identity management is authentication and access control, usually requiring a directory to manage the process, also known as provisioning. These functions are consistent with HIPAA's Security Rule.

Because HIE organizations are not operating within the closed environment of one organizational entity, there must be security among all parties in the exchange, so federation management provides encryption and communication security services across the HIE members (what would be, in the HIPAA Security Rule, the transmission security standard). Although there is no "HIPAA for HIE" per se, HIE organizations are adopting transmission security controls that afford strong protection. There are certainly many options, but most HIE organizations are looking to not only afford protection at the outer, "envelope," layer of a message (e.g., SSL), but to incorporate security within the message as well (e.g., WS-Addressing, SAML, Liberty). Web Services Security (WS-Security) is a suite of security services applicable to transmission of messages across the Web, often including a digital signature.

Finally, auditing and reporting of usage is enabled via identity management. Although auditing may frequently be discussed in association with consent management, to be discussed next, it is the access that is audited and made available for reporting. Auditing and consent management are sometimes grouped in discussion with the public because it conveys the assurance that the individuals' consent directives are being monitored.

In addition to these basic identity management services, an HIE may support further protection of the data via a de-identification process that enables secure re-identification once the message has reached its destination. Anonymization and pseudonymization will be discussed further in Part 3. of this Course, as it tends to be an "advanced" service not needing to be deployed by all HIEs.



Consent Management

80/20 : Policy/Technology

Consent management from a technology perspective is the active management and enforcement of users' consent when collecting, storing, accessing, processing and disclosing personal health data. From a policy perspective, however, it is the capture and management of consent directives that will require considerable consumer education/maintenance.

- Opt-out = data exchanged by default unless restricted by patient
- Opt-in = data not exchanged by default until patient consents
- "Quilted" = subset of data exchanged with patient consent based on institution, data user, data producer, and situation
  - Would need a hierarchy to interpret complex consent:

  Situation > Institution > Data User > Data Producer

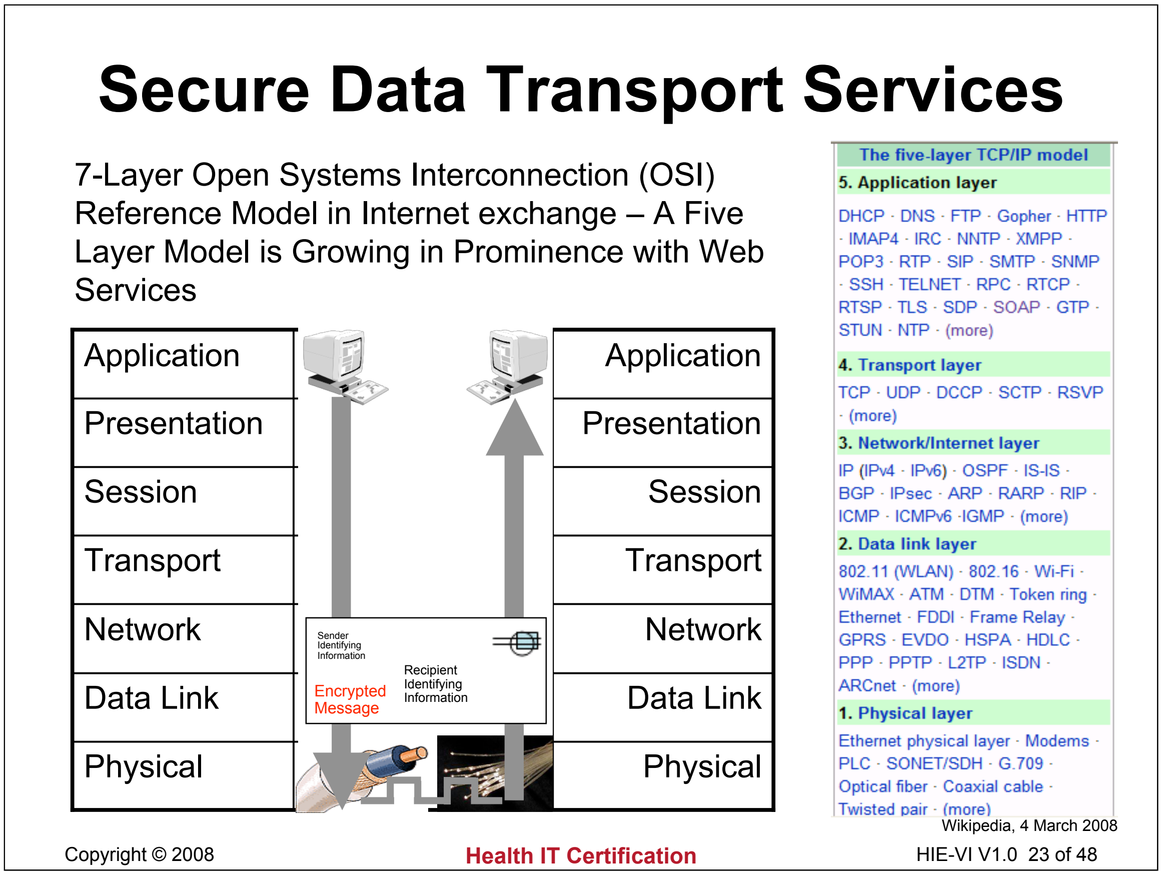
  e.g., Opt in for ED data sharing overrides data producer opt outs

- eXtensible Access Control Markup Language (XACML)
  - A declarative access control policy language implemented in XML, and
  - A processing model, describing how to interpret the policies
- Collaborative Application Markup Language (CAML)
  - XML-based markup language used with Microsoft SharePoint technologies to both define and display data
  - Potential to be **Consent Assertion Markup Language** in a Consent Wizard?

Another basic service for an HIE is consent management. This is an individual-centric method for controlling access to individual-specific information. When such information is attempted to be accessed by another party, the request is compared to the individual's existing access permissions, or consent directives. If there is no existing access permission, the request is compared to the individual's default preferences. If default preferences permit the requested access, the request is filled. If default preferences do not permit the request to be filled, a consent interface may be invoked that presents one or more consent options to a party with authority to grant consent, thereby permitting the individual to control whether the access request will be filled.

In an HIE environment, John Halamka, MD, chair of the Health Information Technology Standards Panel (HITSP), has proposed a "Consent Wizard" that could record patient preferences about information sharing, transfer these preferences among stakeholders, and manage continually changing privacy preferences, situations, and use cases. Such a Consent Wizard might be an enhancement of the existing XACML or elaboration on CAML. (XACML is used by major IT companies supplying single sign on and authentication services to the financial services sector, health care, manufacturing, and a broad range of government agencies such as the IRS and companies such as Verizon and Office Depot. CAML is currently used in Microsoft's SharePoint technologies.) The result of a Consent Wizard would be the ability to manage a "quilt" of consent preferences based on institution, data user, data producer, and situation.

Dr. Halamka suggests that together, the parts of the quilt could become quite complex, where a utility would need to enforce integrity of consent directives to avoid conflicting preferences (i.e., individuals cannot both opt-out and opt-in for data sharing with the same data user and situation). Perhaps the greatest challenge in achieving such a schema, however, may not be the technology, but the ability for the individual patient to make informed decisions about their consent preferences, and the ongoing management of the consent directives. While there are some companies that exist today that provide consent management utilities, if such a utility is not included in the HIE products and services acquired by an HIE, it will need to consider the level of consent management services it can provide. HIEs around the country are largely using a strict opt-out approach, although a few are entering the market with an opt-in strategy.



Secure Data Transport Services

7-Layer Open Systems Interconnection (OSI) Reference Model in Internet exchange – A Five Layer Model is Growing in Prominence with Web Services

Application	Application
Presentation	Presentation
Session	Session
Transport	Transport
Network	Network
Data Link	Data Link
Physical	Physical

Sender Identifying Information
Recipient Identifying Information
Encrypted Message

The five-layer TCP/IP model

5. Application layer

DHCP · DNS · FTP · Gopher · HTTP · IMAP4 · IRC · NNTP · XMPP · POP3 · RTP · SIP · SMTP · SNMP · SSH · TELNET · RPC · RTCP · RTSP · TLS · SDP · SOAP · GTP · STUN · NTP · (more)

4. Transport layer

TCP · UDP · DCCP · SCTP · RSVP · (more)

3. Network/Internet layer

IP (IPv4 · IPv6) · OSPF · IS-IS · BGP · IPsec · ARP · RARP · RIP · ICMP · ICMPv6 ·IGMP · (more)

2. Data link layer

802.11 (WLAN) · 802.16 · Wi-Fi · WiMAX · ATM · DTM · Token ring · Ethernet · FDDI · Frame Relay · GPRS · EVDO · HSPA · HDLC · PPP · PPTP · L2TP · ISDN · ARCnet · (more)

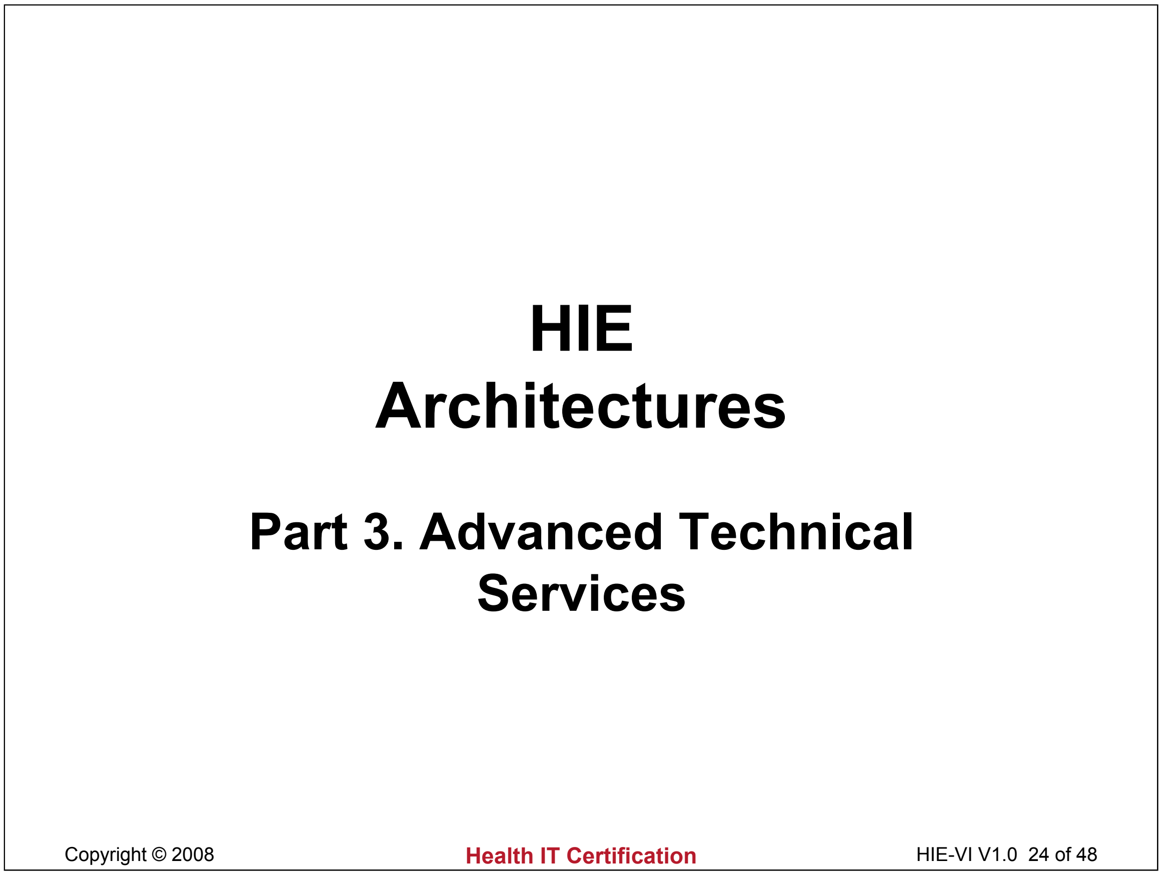
1. Physical layer

Ethernet physical layer · Modems · PLC · SONET/SDH · G.709 · Optical fiber · Coaxial cable · Twisted pair · (more)

Wikipedia, 4 March 2008

Copyright © 2008 Health IT Certification HIE-VI V1.0 23 of 48

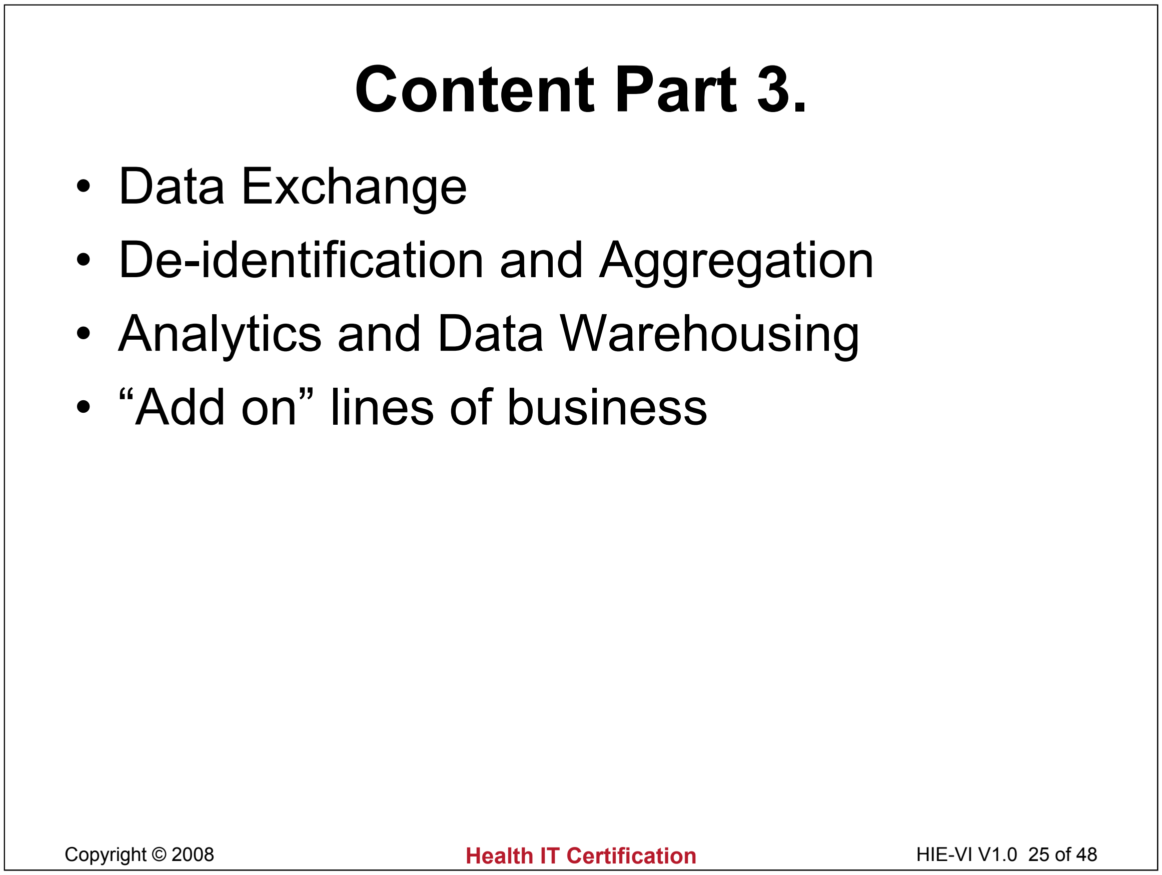
Although identity management includes secure transmission services, the actual transmission does not occur until after a user authenticates and access controls determine the user's privileges and consent management processes match the request with the individual's consent directives. Then federation management enables the secure data transmission. The applicable data transport security services are largely standard across the Internet, for any industry. The Transmission Control Protocol/Internet Protocol (TCP/IP) suite of standards assures security throughout all layers of the process to move data at the sender's application level through its conversion ultimately to electrical pulses and back to the recipient's application. Although the five-layer TCP/IP model of is growing in prominence with Web services as the data transport construct, it is clearly consistent with the 7-layer OSI Reference Model that has been in existence as the construct for Internet exchange of data. In health care, the separation of application and presentation layers, as well as the session and transport layers are still very much present in design of systems and networks.



HIE Architectures

Part 3. Advanced Technical Services

In addition to basic services of managing the actual exchange of information, an HIE may perform other, more advanced, technical services.

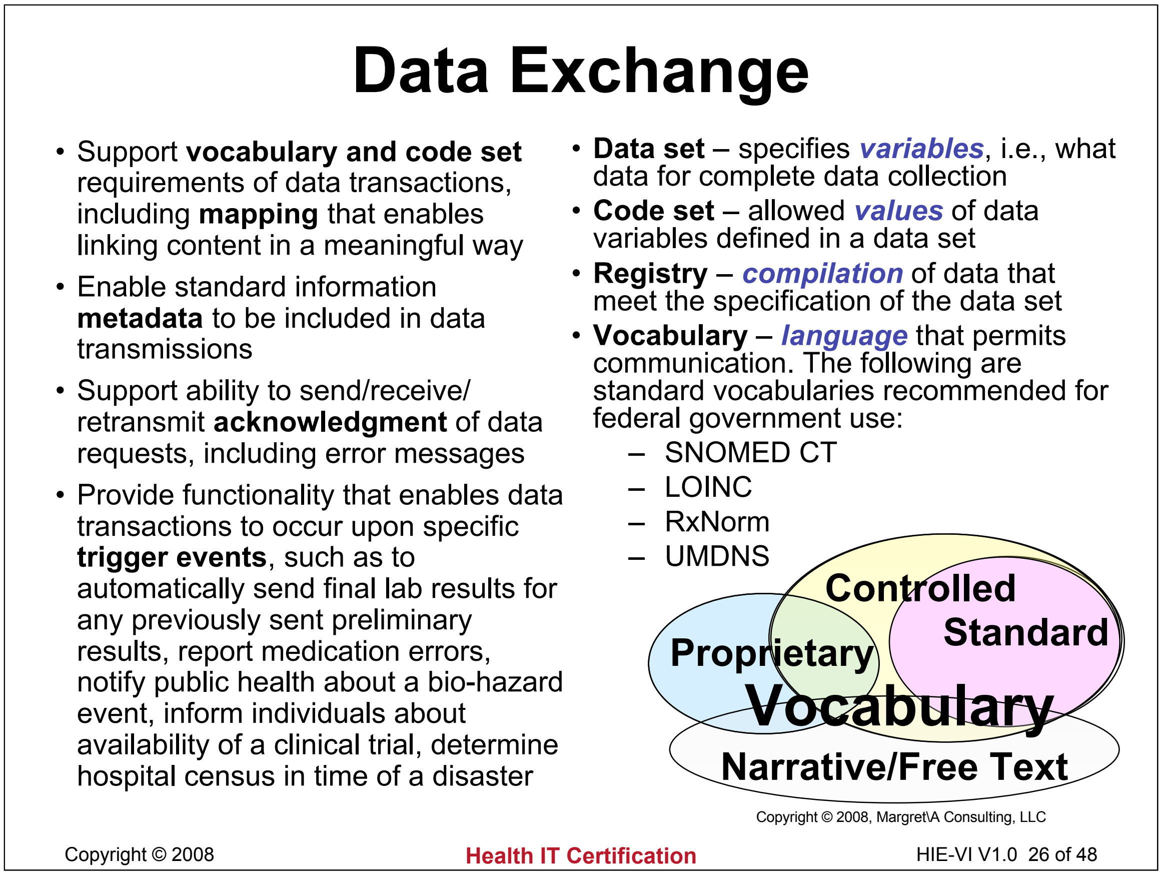


Content Part 3.

- Data Exchange
- De-identification and Aggregation
- Analytics and Data Warehousing
- “Add on” lines of business

Health IT Certification

Part 3. identifies and describes some of the more common advanced technical services an HIE may perform and also discusses some of the “add on” lines of business that an HIE may want to provide.



Data Exchange

- Support **vocabulary and code set** requirements of data transactions, including **mapping** that enables linking content in a meaningful way
- Enable standard information **metadata** to be included in data transmissions
- Support ability to send/receive/ retransmit **acknowledgment** of data requests, including error messages
- Provide functionality that enables data transactions to occur upon specific **trigger events**, such as to automatically send final lab results for any previously sent preliminary results, report medication errors, notify public health about a bio-hazard event, inform individuals about availability of a clinical trial, determine hospital census in time of a disaster

- **Data set** – specifies ***variables***, i.e., what data for complete data collection
- **Code set** – allowed ***values*** of data variables defined in a data set
- **Registry** – ***compilation*** of data that meet the specification of the data set
- **Vocabulary** – ***language*** that permits communication. The following are standard vocabularies recommended for federal government use:
  - SNOMED CT
  - LOINC
  - RxNorm
  - UMDNS

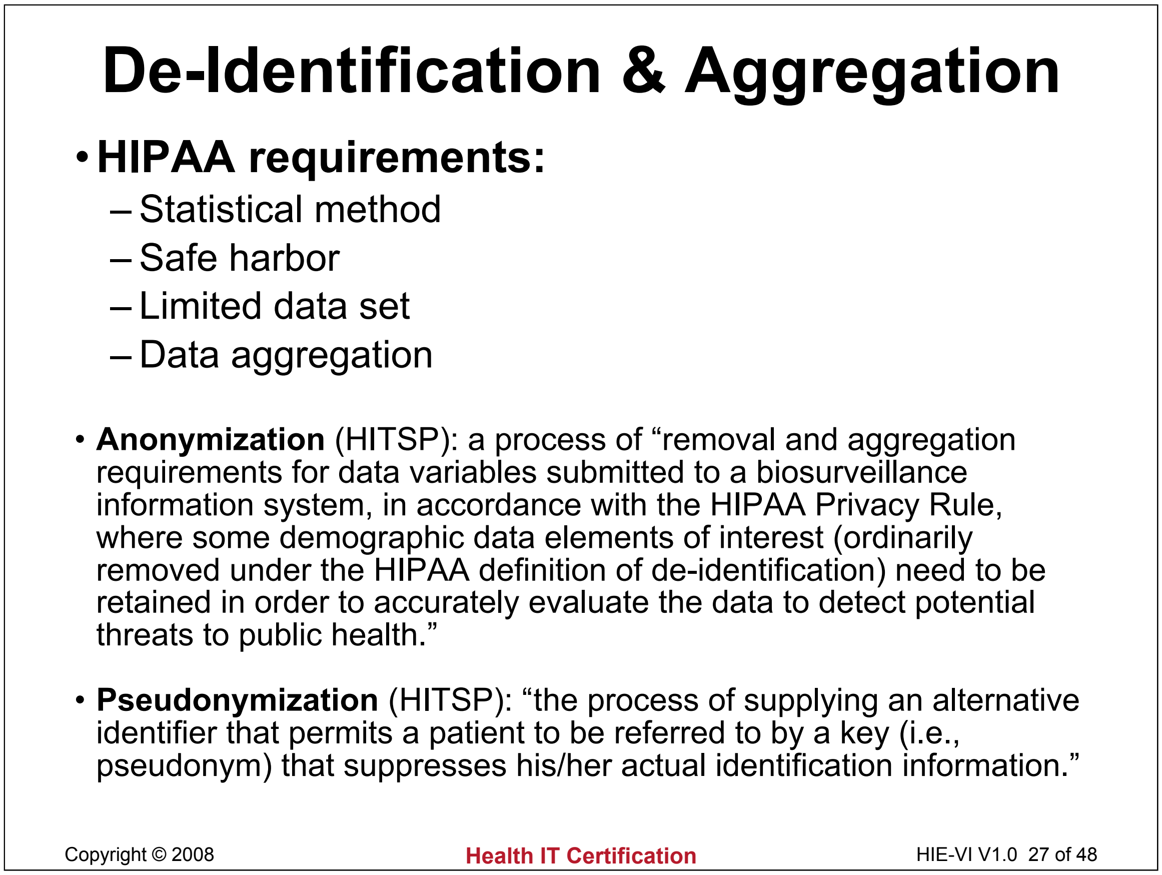
Copyright © 2008, Margret\A Consulting, LLC

Copyright © 2008 Health IT Certification HIE-VI V1.0 26 of 48

Although it would be desirable for any exchange of health data to use standard vocabulary to ensure “semantic interoperability” and hence common meaning for all words used in the communication, adoption of such level of standardization, although recommended standards have been identified, is likely to be a ways into the future. Many HIT vendors continue to use proprietary vocabularies, and many organizations do not maintain a controlled vocabulary, even when using some standards. However, an increasing number of communications are requiring the adoption of a standard code set and in some cases a standard vocabulary. Certainly for any quality measurement and reporting activities, it is critical to have standard values for the data to be collected.

One advanced technical service that some HIEs are finding demand for is the support of vocabulary and code set requirements, especially providing mapping services that enables linking content from one data set that may use one standard code set or vocabulary to another that uses a different code set or vocabulary (often for legitimate reasons). For example, clinical lab orders may utilize LOINC (Logical Observations Identifiers Names and Codes) to encode laboratory test name and describe results. However, for billing purposes, these may need to be converted to CPT (Current Procedural Terminology) codes. An HIE could supply a mapping service that converts LOINC codes to CPT codes as needed. Another example may be that clinical documentation is recorded using SNOMED from the International Health Terminology Standards Development Organization (IHTSDO), but again for reimbursement purposes, some of the information must be translated into ICD-9-CM (International Classification of Diseases, Ninth Edition, Clinical Modification for the U.S.), for which an HIE could provide a mapping service.

Other advanced technical services relating to data exchange include special messaging services, such as acknowledgments and data transactions as a result of trigger events. It may also serve as a registry for certain data. There are many types of registries, but some of the more popular ones which an HIE may support include immunization registries, trauma registries, communicable disease registries, and chronic illness registries (such as diabetes, heart disease, tumor, and others). Registry functionality might include the ability to view or receive prompts relative to immunization needs; data to identify at-risk traffic patterns; or provide reminders to patients and their providers for preventive care measures, such as mammography or colorectal cancer screening.



De-Identification & Aggregation

- **HIPAA requirements:**
  - Statistical method
  - Safe harbor
  - Limited data set
  - Data aggregation

- **Anonymization** (HITSP): a process of “removal and aggregation requirements for data variables submitted to a biosurveillance information system, in accordance with the HIPAA Privacy Rule, where some demographic data elements of interest (ordinarily removed under the HIPAA definition of de-identification) need to be retained in order to accurately evaluate the data to detect potential threats to public health.”

- **Pseudonymization** (HITSP): “the process of supplying an alternative identifier that permits a patient to be referred to by a key (i.e., pseudonym) that suppresses his/her actual identification information.”

Copyright © 2008 Health IT Certification HIE-VI V1.0 27 of 48

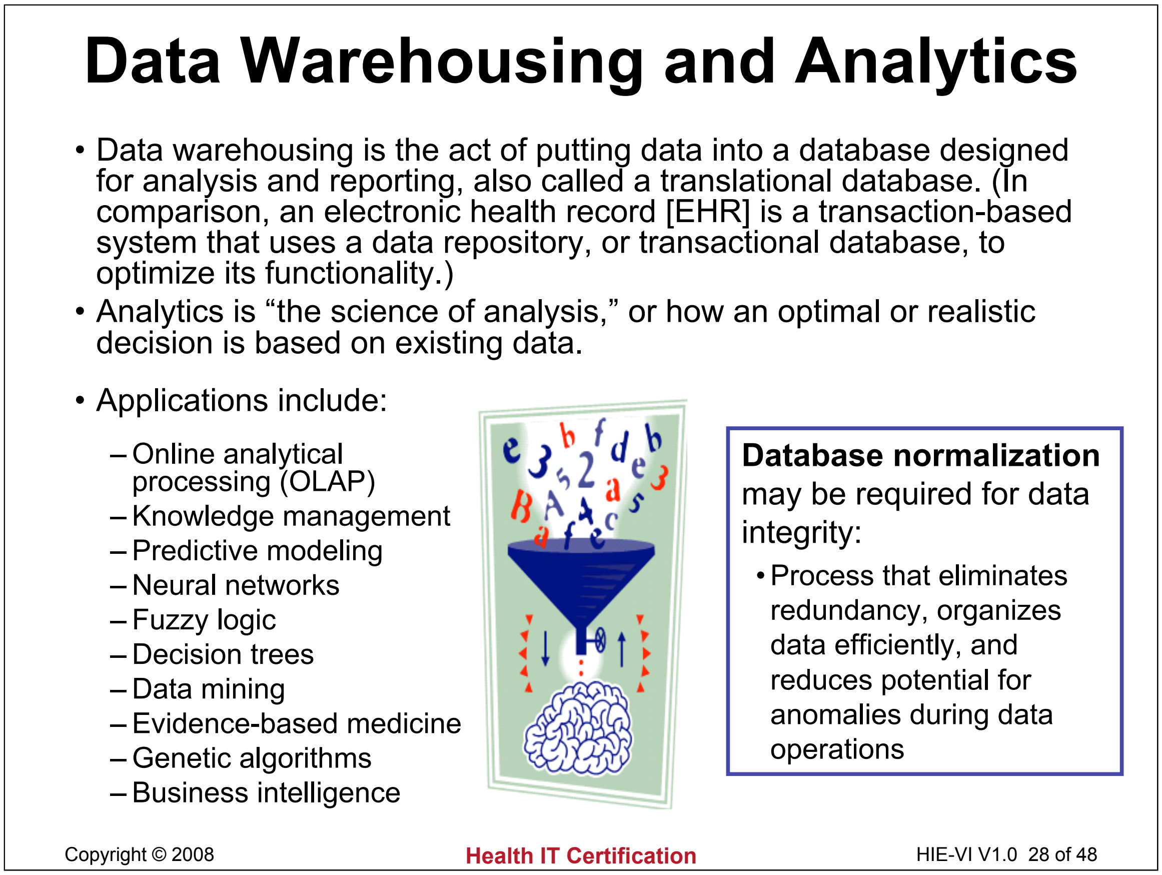
De-identification and aggregation are services that an HIE may also perform. HIPAA provides a number of ways that protected health information may either be converted into de-identified data which is no longer required to be under the protection of HIPAA or a limited data set which is partially identifiable and may be used only for research, public health, or healthcare operations. HIPAA’s de-identification requirements include:

- Statistical method - use of generally accepted statistical and scientific principles and methods for rendering information not individually identifiable by a person with appropriate knowledge and experience; determining that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information; and documents the methods and results of the analysis that justify such determination.
- Safe harbor – removal of 17 identifying data elements plus any other unique identifying number, characteristic, or code except as permitted for re-identification by the covered entity.

A Limited Data Set, as defined by HIPAA Privacy Rule is protected health information that excludes all direct identifiers of the individual or of relatives, employers, or household members of the individual as defined in HIPAA’s Privacy Rule’s definition of de-identification, *except* city, State, and zip code; all elements of dates related to the individual; and any other unique identifying number, characteristic, or code not included in the HIPAA definition of de-identification.

HIPAA also permits data aggregation services to be performed by business associates and describes data aggregation as the combining of such protected health information with the protected health information of another covered entity, to permit data analyses that relate to the healthcare operations of the respective covered entities.

Two additional approaches to de-identification are primarily used in the context of public health services. While public health has the right, under HIPAA, to receive protected health information, many local and/or state public health agencies and Centers for Disease Control and Prevention (CDC) prefer to de-identify this data to the extent possible as an extra precautionary measure. Anonymization and pseudonymization standards for such public health uses have been recognized by HITSP.



Data Warehousing and Analytics

- Data warehousing is the act of putting data into a database designed for analysis and reporting, also called a translational database. (In comparison, an electronic health record [EHR] is a transaction-based system that uses a data repository, or transactional database, to optimize its functionality.)
- Analytics is "the science of analysis," or how an optimal or realistic decision is based on existing data.
- Applications include:
  - Online analytical processing (OLAP)
  - Knowledge management
  - Predictive modeling
  - Neural networks
  - Fuzzy logic
  - Decision trees
  - Data mining
  - Evidence-based medicine
  - Genetic algorithms
  - Business intelligence

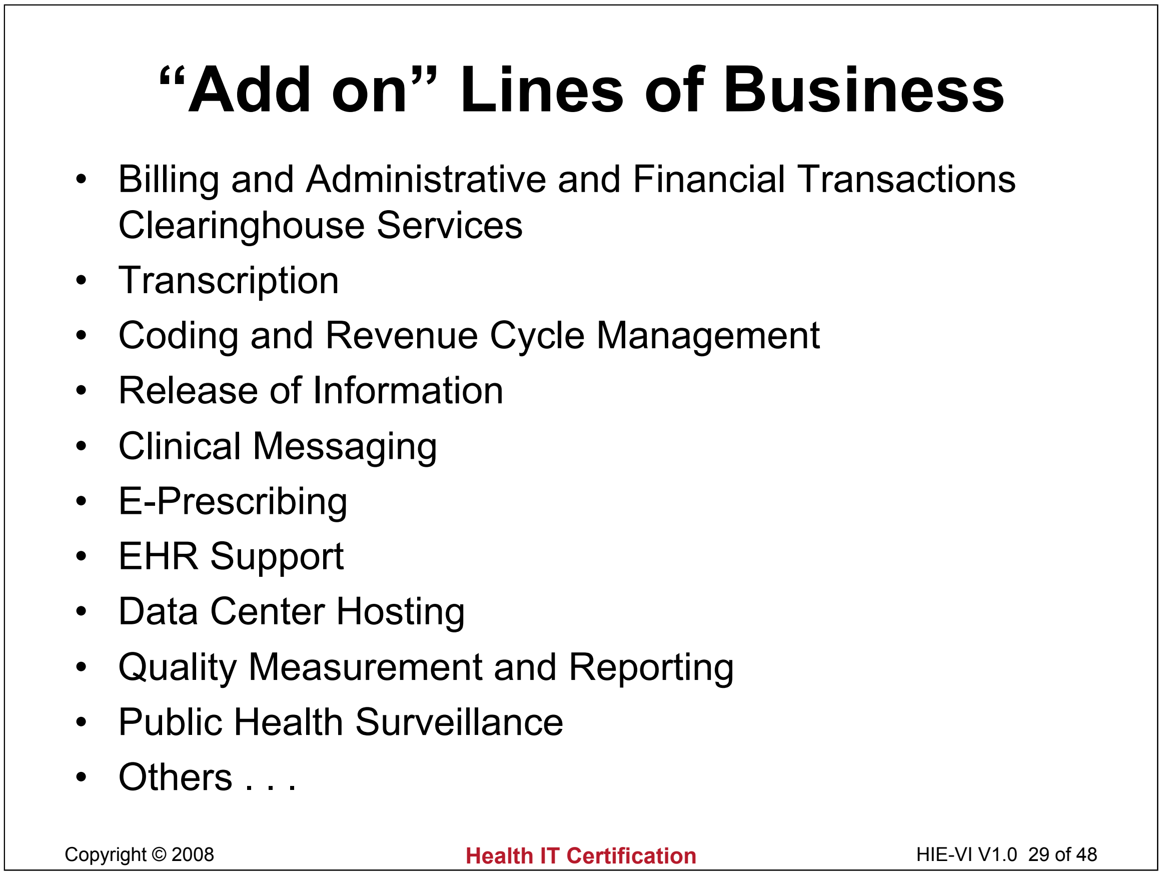
Database normalization may be required for data integrity:

- Process that eliminates redundancy, organizes data efficiently, and reduces potential for anomalies during data operations

Copyright © 2008 Health IT Certification HIE-VI V1.0 28 of 48

Another advanced technical service HIEs may provide include data warehousing and various analytics services. Many individual healthcare organizations do not have the means to support a data warehouse and staff trained in analytics, but would value the ability to better understand and learn from their data. The federal government has identified four cornerstones for health care improvement, all of which impact and are impacted by the ability to analyze (good quality) health data:

- **Health IT Standards:** Interoperable health information technology has the potential to create greater efficiency in health care delivery. Standards enable health information systems to communicate and exchange data quickly and securely to protect patient privacy.
- **Quality Standards:** To make confident decisions about their health care providers and treatment options, consumers need quality of care information. Similarly, this information is important to providers who are interested in improving the quality of care they deliver. Quality measurement should be based on measures that are developed through consensus-based processes involving all stakeholders, such as the processes be used by the AQA (multi-stakeholder group focused on physician quality measurement) and the Hospital Quality Alliance.
- **Price Standards:** To make confident decisions about their health care providers and treatment options, consumers also need price information. Uniform approaches to measuring and reporting price information for the benefit of consumers is essential. In addition, strategies are being developed to measure the overall cost of services for common episodes of care and the treatment of common chronic diseases.
- **Incentives:** All parties - providers, patients, insurance plans, and payers - should participate in arrangements that reward both those who offer and those who purchase high-quality, competitively-priced health care. Such arrangements may include implementation of pay-for-performance methods of reimbursement for providers or the offering of consumer-directed health plan products, such as account-based plans for enrollees in employer-sponsored health benefit plans.



“Add on” Lines of Business

- Billing and Administrative and Financial Transactions Clearinghouse Services
- Transcription
- Coding and Revenue Cycle Management
- Release of Information
- Clinical Messaging
- E-Prescribing
- EHR Support
- Data Center Hosting
- Quality Measurement and Reporting
- Public Health Surveillance
- Others . . .

Copyright © 2008 Health IT Certification HIE-VI V1.0 29 of 48

“Add on” lines of business for an HIE may those provided because they are cheaper to deliver through a local HIE, more meaningful within the context of a given region, or are enabled through group purchasing.

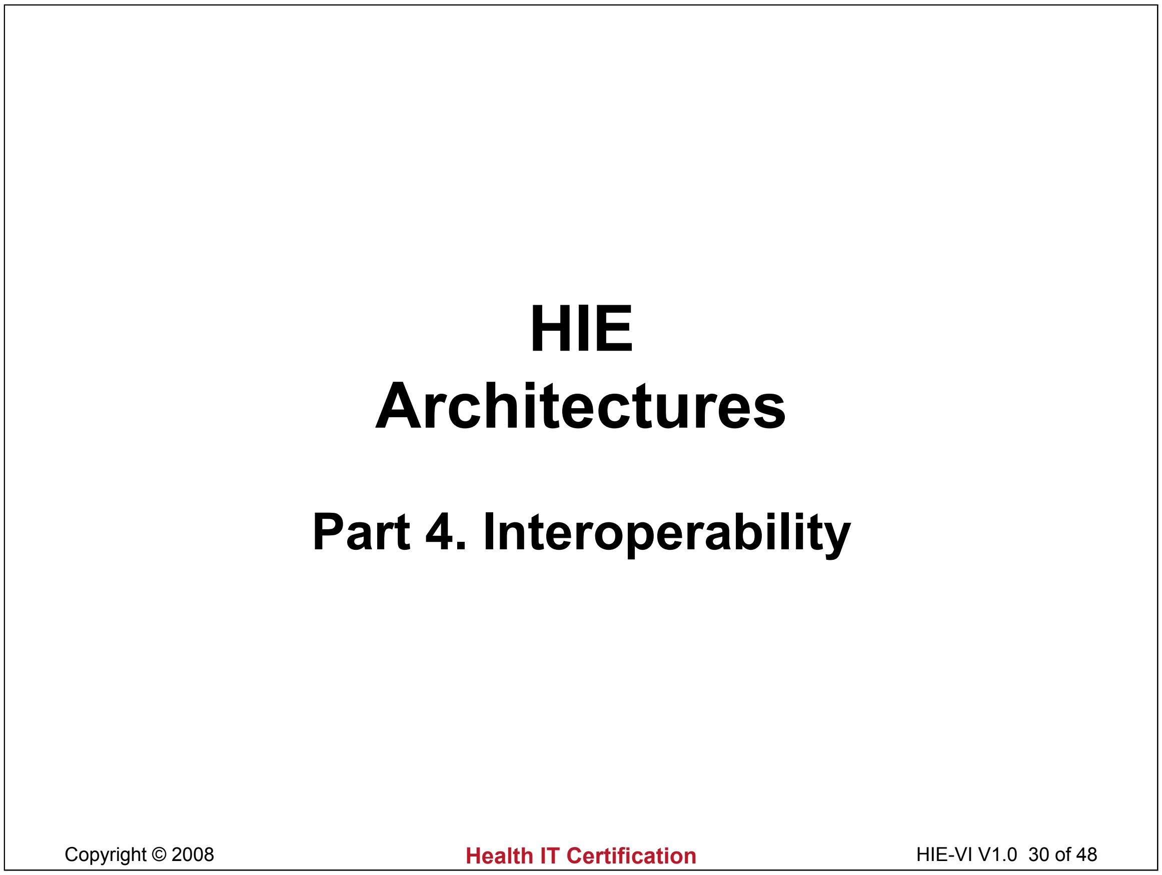
Several of the early HIEs actually got their start providing billing and clearinghouse services in a more cost-effective manner for their local or regional constituents. Likewise, transcription, coding, and release of information services are becoming more commodity services that are often more cost-effective when consolidated. Clinical messaging is usually the first service offered when an HIE enters the clinical health information exchange business, so may not be considered “add on,” unless other services initiated the HIE.

E-prescribing may currently be enabled through commercial gateways and processes, but an HIE could potentially benefit its community by supporting more targeted services. For example, national formulary information consolidators may be in a competitive position and not able to supply formulary information for all plans in a given region. An HIE could take over this function for its members.

Some HIEs are looking to support EHR adoption throughout their community. “Community-wide health networks” provide exceptions to Stark and Anti-Kickback Laws that could enable providers to acquire an EHR at low cost. In addition, local support and hosting could lower cost and provide support, especially for small providers with little or no IT staff.

As previously mentioned there is a significant need for data exchange services, warehousing, and analytics; but a natural extension of these might be to actually provide the quality measurement and reporting, public health surveillance, or other such functionality for the community.

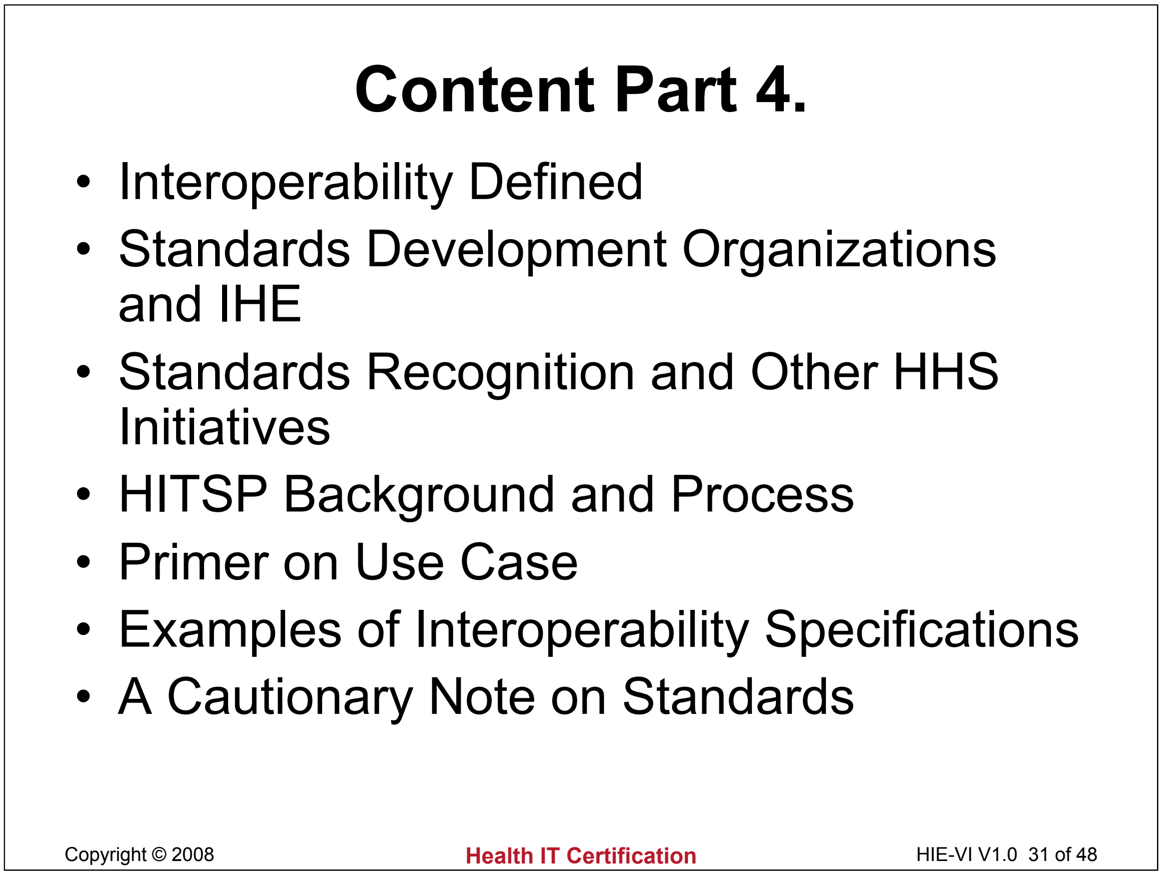
Certainly, creative HIEs are and will be finding many other “add on” lines of business – both to meet the interests of their stakeholders, but also to assist themselves in sustainability.



HIE Architectures

Part 4. Interoperability

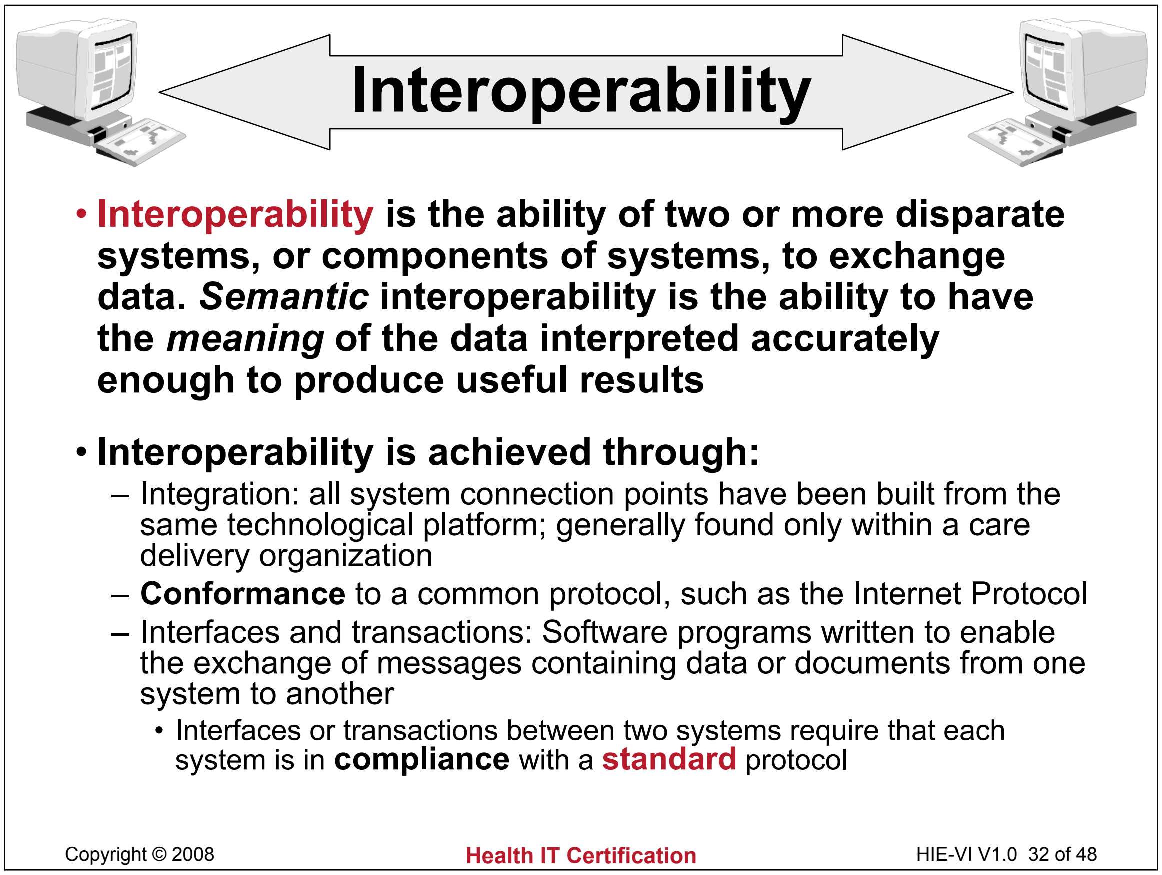
Much has been made of the need for standards to achieve interoperability within HIE. Part 4. of this course describes interoperability and describes how improvements in promoting interoperability are being achieved.



Content Part 4.

- Interoperability Defined
- Standards Development Organizations and IHE
- Standards Recognition and Other HHS Initiatives
- HITSP Background and Process
- Primer on Use Case
- Examples of Interoperability Specifications
- A Cautionary Note on Standards

Part 4. defines interoperability, provides an overview of standards setting processes and the federal government’s role, and provides specific information about efforts underway to promote standards for HIE.



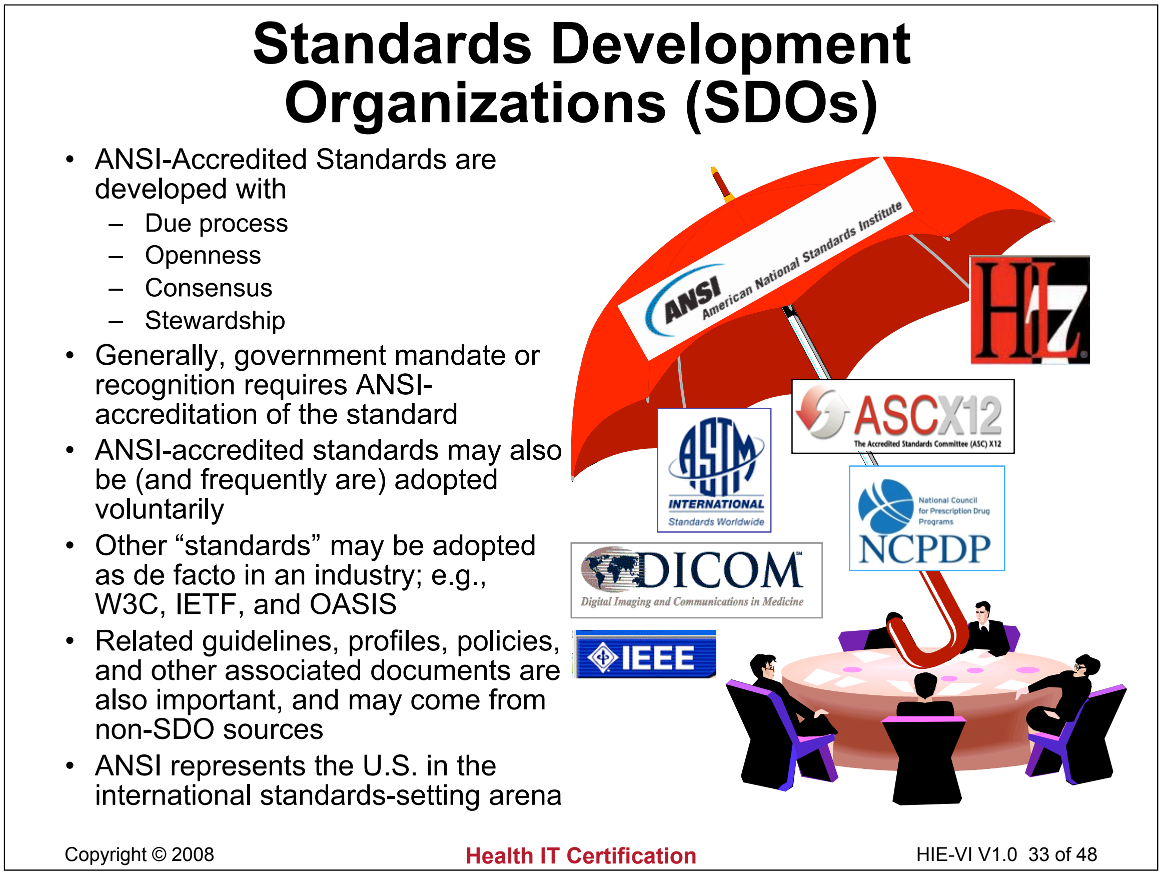
Interoperability

- **Interoperability is the ability of two or more disparate systems, or components of systems, to exchange data. *Semantic* interoperability is the ability to have the *meaning* of the data interpreted accurately enough to produce useful results**
- **Interoperability is achieved through:**
  - Integration: all system connection points have been built from the same technological platform; generally found only within a care delivery organization
  - **Conformance** to a common protocol, such as the Internet Protocol
  - Interfaces and transactions: Software programs written to enable the exchange of messages containing data or documents from one system to another
    - Interfaces or transactions between two systems require that each system is in **compliance** with a **standard** protocol

Health IT Certification HIE-VI V1.0 32 of 48

Interoperability is the ability of two or more disparate systems to exchange data. Issues associated with interoperability are not unique to health care, even though the healthcare industry may not have been able to come to terms with standards as readily as other industries – where standards are recognized as a means to support a competitive environment rather than restrict competition as some health information technology vendors may continue to perceive.

Interoperability, however, while perhaps simply defined, is not simple to achieve in any environment. Interoperability may be considered to have several flavors – from bland to robust! When all separate systems or applications are built upon the same technological platform, interoperability is quite robust (although still not necessarily perfect as different applications must address different workflows and processes that make some aspects of interoperability more difficult to achieve). Precise conformance to a common protocol achieve interoperability where systems or applications have not been built upon the same technological platform. Such precision in conformance, however, is often difficult to achieve, especially in an immature market. As a result, standard protocols are developed with some level of optionality to address competing interests, but resultant interfaces or transactions that result from their



Standards Development Organizations (SDOs)

- ANSI-Accredited Standards are developed with
  - Due process
  - Openness
  - Consensus
  - Stewardship
- Generally, government mandate or recognition requires ANSI-accreditation of the standard
- ANSI-accredited standards may also be (and frequently are) adopted voluntarily
- Other “standards” may be adopted as de facto in an industry; e.g., W3C, IETF, and OASIS
- Related guidelines, profiles, policies, and other associated documents are also important, and may come from non-SDO sources
- ANSI represents the U.S. in the international standards-setting arena

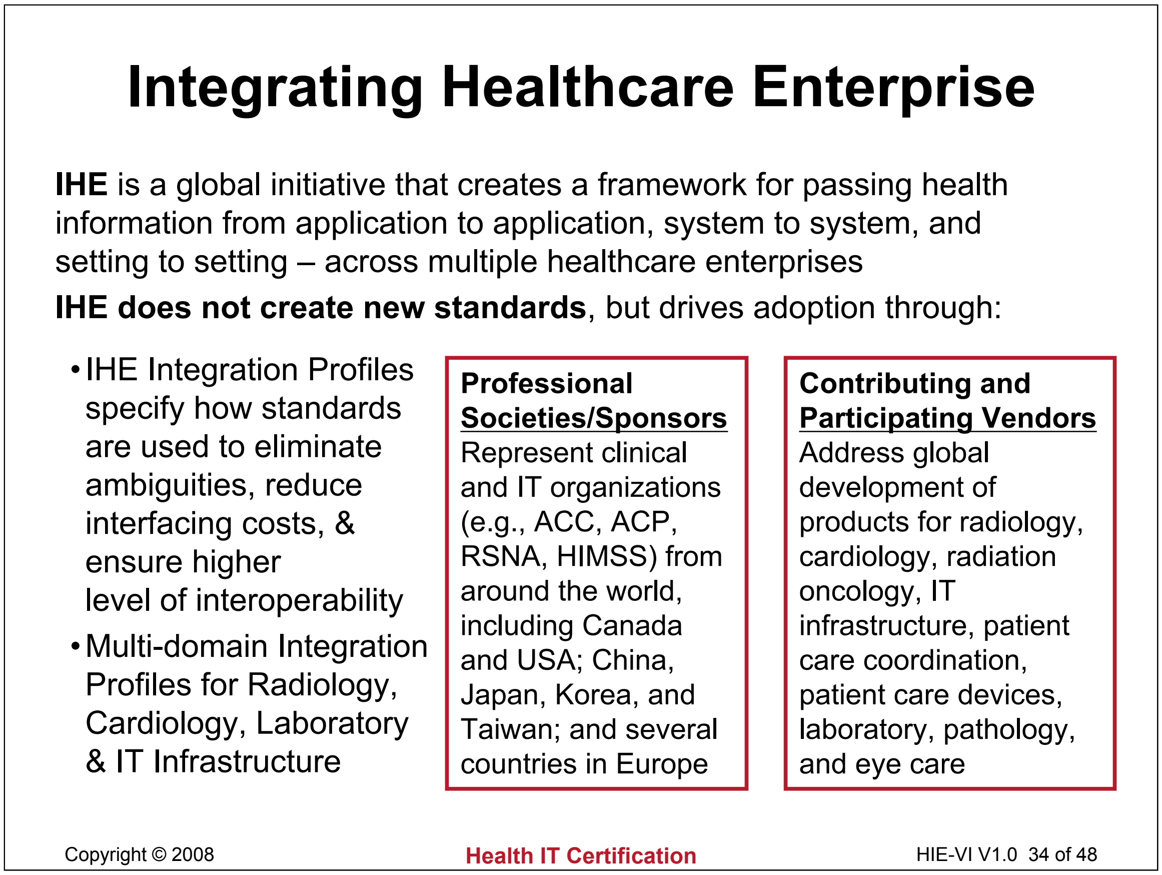
ANSI American National Standards Institute
HL7
ASC X12 The Accredited Standards Committee (ASC) X12
ASTM INTERNATIONAL Standards Worldwide
National Council for Prescription Drug Programs NCPDP
DICOM Digital Imaging and Communications in Medicine
IEEE

Copyright © 2008 Health IT Certification HIE-VI V1.0 33 of 48

There are several ways standards are developed and adopted:

- Ad hoc meetings of interested parties come together to agree on standard specifications where needed. This may be the most powerful form of standards setting because there is strong incentive and mutual agreement to use the standards. The World Wide Web Consortium (W3C), Internet Engineering Task Force (IETF) organized by the Internet Society (ISOC), and Organization for the Advancement of Structured Information Systems (OASIS) are the most applicable examples that provide leadership in WWW, Internet, and service oriented architecture (SOA) related standards.
- De facto standards exist where a single vendor controls a very large proportion of a market, making the product a market standard. A well-recognized example of this is Microsoft Windows. Of course, there can be Federal Trade Commission issues when this happens, and sometimes de facto standards are not necessarily in the best interest of the consumer.
- Government mandates may result in a standard. A good example is the HIPAA Privacy Standard. In general, however, the federal government prefers to adopt industry consensus standards where they exist rather than creating a new standard.
- Consensus standards are generally considered the most desirable because, at least in theory, they represent industry consensus.

Consensus-driven standards development organizations (SDOs) develop their standards in accordance with specific organizational structures and procedures to ensure that they truly represent industry consensus. The American National Standards Institute (ANSI) is not an SDO, but a body that accredits SDOs with respect to meeting the requirements for due process, openness, and consensus. (ANSI accredits many, though not all SDOs. Many of the ad hoc SDOs that have arisen out of industry need attest to a consensus process outside of this formal accreditation.) ANSI also creates internal Accredited Standards Committees (ASC) to meet a need not filled by an existing SDO. An example of this is ASC X12, which currently develops standards for financial and administrative transactions. European and international counterpart organizations to ANSI also exist (e.g., International Standards Organization [ISO]) and many of the SDOs work at the international level as well in order to ensure that products can be successfully marketed abroad.



Integrating Healthcare Enterprise

IHE is a global initiative that creates a framework for passing health information from application to application, system to system, and setting to setting – across multiple healthcare enterprises

IHE does not create new standards, but drives adoption through:

- IHE Integration Profiles specify how standards are used to eliminate ambiguities, reduce interfacing costs, & ensure higher level of interoperability
- Multi-domain Integration Profiles for Radiology, Cardiology, Laboratory & IT Infrastructure

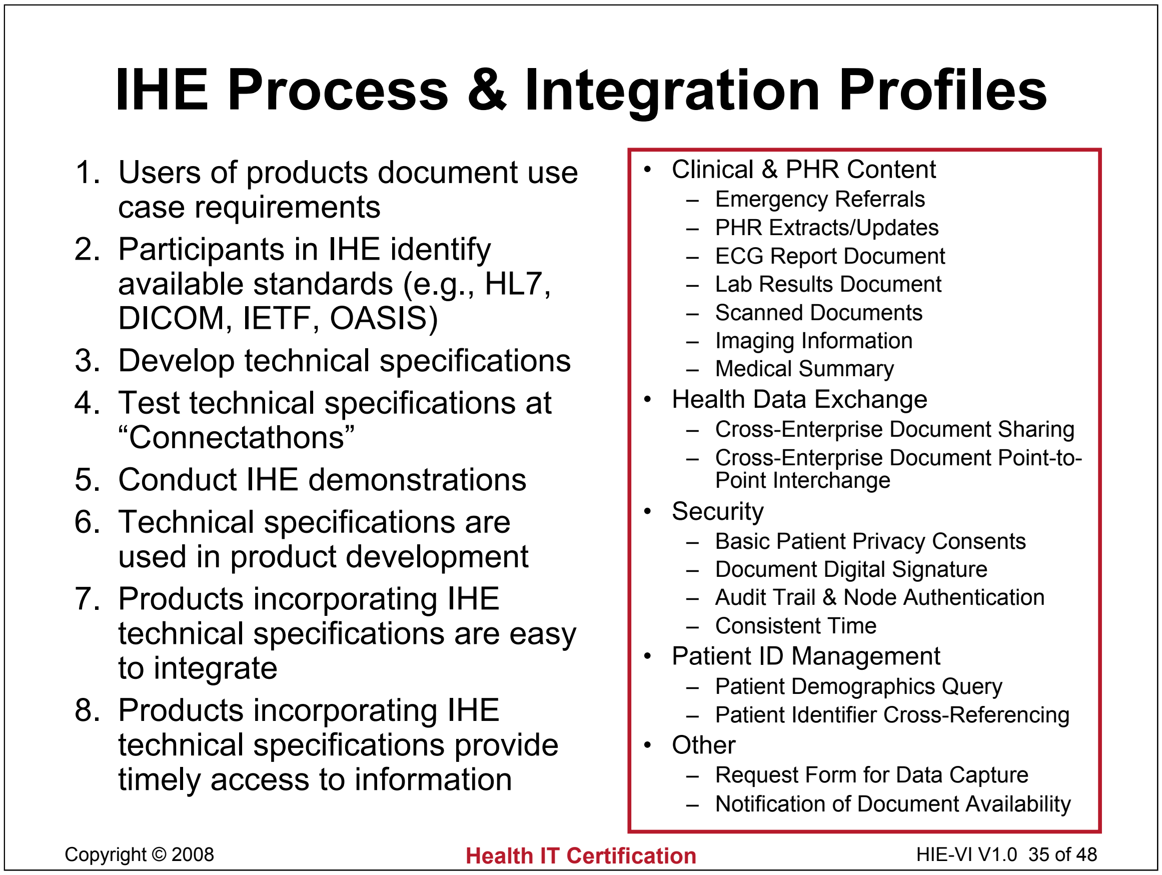
Professional **<u>Societies/Sponsors</u>**
Represent clinical and IT organizations (e.g., ACC, ACP, RSNA, HIMSS) from around the world, including Canada and USA; China, Japan, Korea, and Taiwan; and several countries in Europe

Contributing and **<u>Participating Vendors</u>**
Address global development of products for radiology, cardiology, radiation oncology, IT infrastructure, patient care coordination, patient care devices, laboratory, pathology, and eye care

In health care, many of the standards that have been developed were developed through a consensus process, but often with a fair amount of optionality in an effort to satisfy the broadest possible stakeholder constituency. The result is often a standard that is not as “standard” as it could be, or as is desired.

Several organizations representing users of products that need to be interoperable have been working together in an ad hoc manner to provide specification on how they would like to see certain standards used. These include, for example, the American College of Cardiology (ACC), American College of Physicians (ACP), the Radiological Society of North America (RSNA), and the Healthcare Information and Management Systems Society (HIMSS). The result has been the formation of the Integrating the Healthcare Enterprise (IHE), now an international effort to develop “integration profiles.” (See www/ihe.net.)

IHE does not produce base standards, hence they are not a standards development organization (SDO), but rather they produce descriptions of how base standards should be used to ensure that products can more seamlessly exchange data.



IHE Process & Integration Profiles

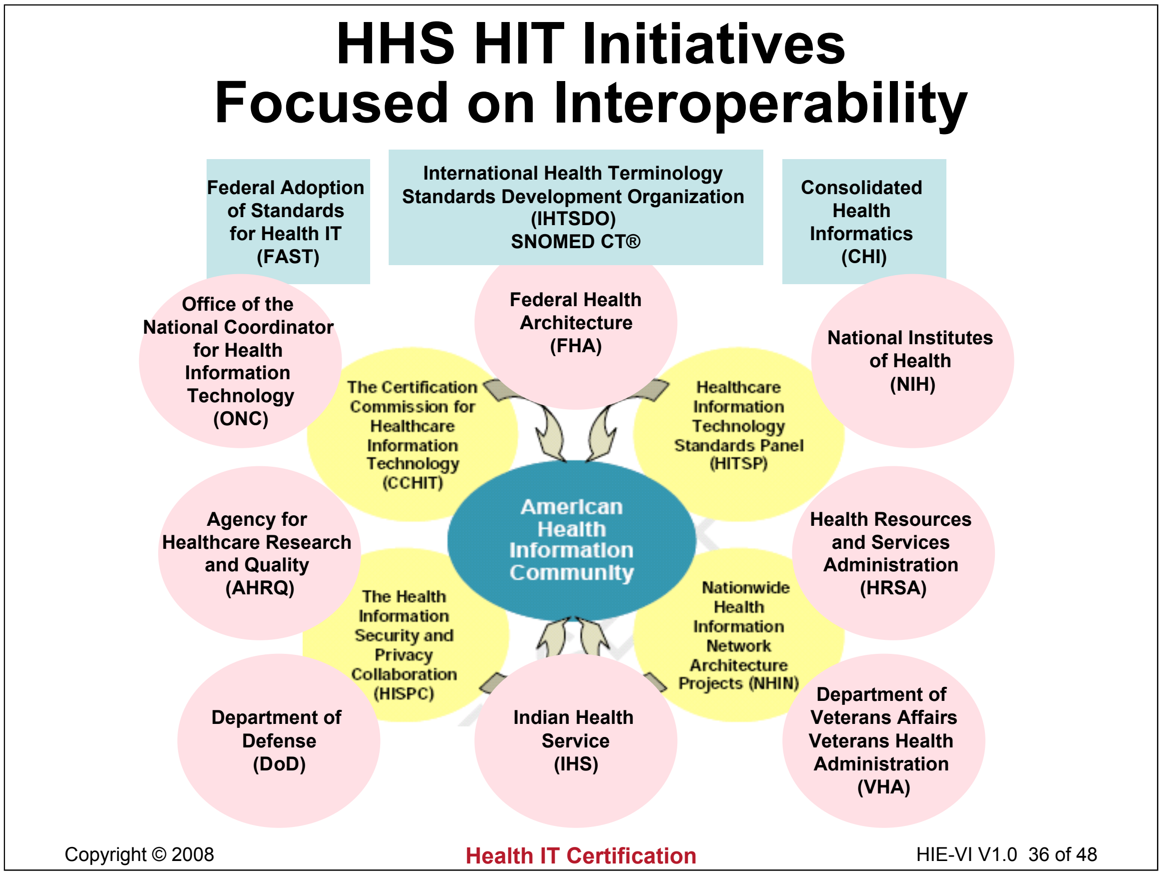
1. Users of products document use case requirements
2. Participants in IHE identify available standards (e.g., HL7, DICOM, IETF, OASIS)
3. Develop technical specifications
4. Test technical specifications at “Connectathons”
5. Conduct IHE demonstrations
6. Technical specifications are used in product development
7. Products incorporating IHE technical specifications are easy to integrate
8. Products incorporating IHE technical specifications provide timely access to information

- Clinical & PHR Content
  - Emergency Referrals
  - PHR Extracts/Updates
  - ECG Report Document
  - Lab Results Document
  - Scanned Documents
  - Imaging Information
  - Medical Summary
- Health Data Exchange
  - Cross-Enterprise Document Sharing
  - Cross-Enterprise Document Point-to-Point Interchange
- Security
  - Basic Patient Privacy Consents
  - Document Digital Signature
  - Audit Trail & Node Authentication
  - Consistent Time
- Patient ID Management
  - Patient Demographics Query
  - Patient Identifier Cross-Referencing
- Other
  - Request Form for Data Capture
  - Notification of Document Availability

Copyright © 2008 **Health IT Certification** HIE-VI V1.0 35 of 48

Today, IHE has done a lot to develop, test, and demonstrate the value of technical specifications that are now being adopted in products to make them easier to integrate, in turn providing more timely access to information.

IHE has developed technical specifications for clinical content, especially for information system connectivity with medical devices. An example is where an auto analyzer in lab contributes result data to a laboratory information system. IHE has also focused on inter-enterprise data exchanges, providing a number of technical specifications that support HIE.



HHS HIT Initiatives Focused on Interoperability

Federal Adoption of Standards for Health IT (FAST)

International Health Terminology Standards Development Organization (IHTSDO) SNOMED CT®

Consolidated Health Informatics (CHI)

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

Federal Health Architecture (FHA)

National Institutes of Health (NIH)

The Certification Commission for Healthcare Information Technology (CCHIT)

Healthcare Information Technology Standards Panel (HITSP)

American Health Information Community

Agency for Healthcare Research and Quality (AHRQ)

Health Resources and Services Administration (HRSA)

The Health Information Security and Privacy Collaboration (HISPC)

Nationwide Health Information Network Architecture Projects (NHIN)

Department of Defense (DoD)

Indian Health Service (IHS)

Department of Veterans Affairs Veterans Health Administration (VHA)

Copyright © 2008

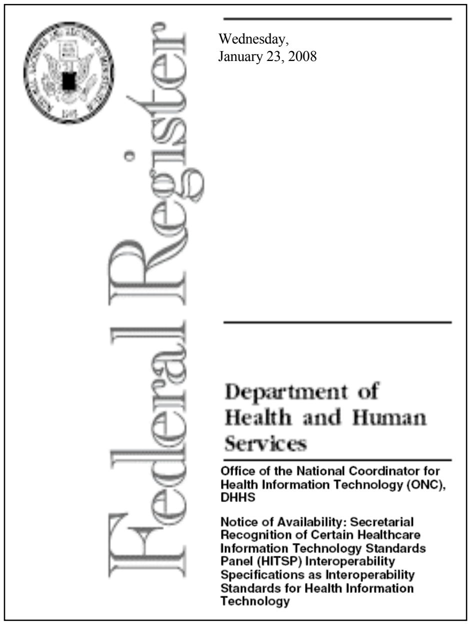
Health IT Certification

HIE-VI V1.0 36 of 48

The American Health Information Community (AHIC) was created by HHS Secretary Leavitt in 2005 to provide recommendations on how to make health records digital and interoperable, and assure that the privacy and security of those records are protected, in a smooth, market-led way. At the same time, the Department of Health and Human Services, through the Office of the National Coordinator for Health Information Technology (ONC) awarded contracts to (1) identify interoperability standards to facilitate the exchange of patient data (HITSP), (2) define a process for certifying that health IT products comply with appropriate standards (CCHIT), (3) develop a series of prototypes to establish the requirements of a nationwide health information network (NHIN), and(4) address interoperability among state privacy and security statutes (HISPC). These activities share the goal of widespread adoption of interoperable electronic health records within 10 years through public-private collaboration. In 2008, AHIC will be moving toward more of a private-sector advisory committee, intended to be self-sustainable in order to weather political changes.

In addition to AHIC and its four primary projects, the federal government has supported HIT initiatives and interoperability standards through several other means as well. Grants have been provided for a number of EHR and HIE projects through the Agency for Healthcare Research and Quality (AHRQ), Health Resources and Services Administration (HRSA), and other federal agencies. The Centers for Medicare and Medicaid Services (CMS) in its 8th Scope of Work supported the Doctors' Office Quality-Information Technology (DOQ-IT) initiative to help small and medium-sized primary care providers become more informed consumers as they purchased EHRs. The National Library of Medicine has acquired a license to use SNOMED at no cost to U.S. consumers. The Office of the National Coordinator for Health Information Technology (ONC) was formed to provide staff support to many of these initiatives, as well as tapping various National Institutes of Health (NIH) staff. Finally, the federal government looks to its own agencies to be early adopters of technology and standards, through the Federal Adoption of Standards for Health IT (FAST), Consolidated Health Informatics (CHI) initiative, and DOD, HIS, and VHA utilization for direct patient care.

Standards Recognition



Federal Register

Wednesday,
January 23, 2008

Department of
Health and Human
Services

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

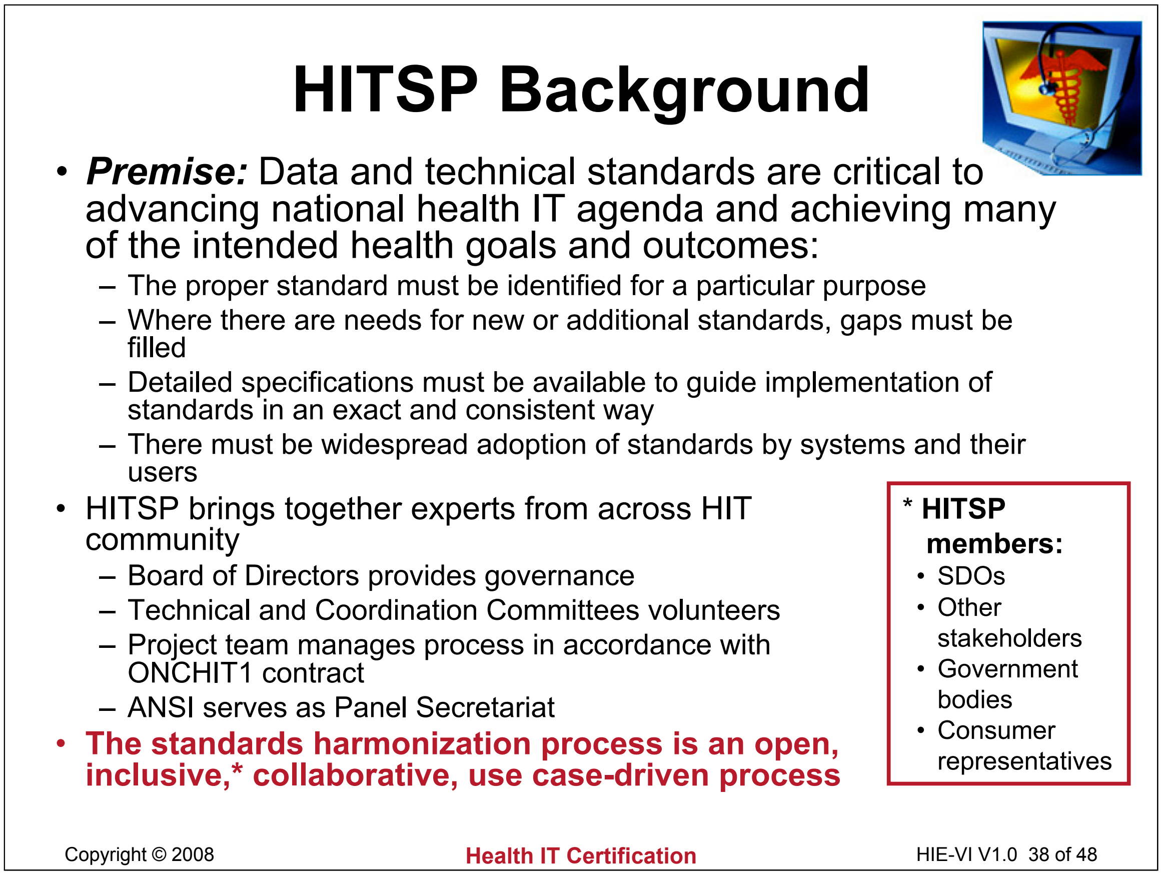
Notice of Availability: Secretarial Recognition of Certain Healthcare Information Technology Standards Panel (HITSP) Interoperability Specifications as Interoperability Standards for Health Information Technology

- Executive Order 13410, August 22, 2006, requires each Federal health agency to utilize products that meet recognized interoperability standards
- In order to recognize such standards, however, they needed to be created or made ready for recognition; and the Health Information Technology Standards Panel was created to do so
- On January 23, 2008, the Secretary of HHS officially provided recognition of certain HITSP “Interoperability Specifications.” The 30 standards include those addressing:
  – EHR Lab Results Reporting
  – Biosurveillance
  – Consumer Empowerment

For federal agencies to be required to adopt standards, an Executive Order 13410 was issued in 2006 requiring each federal health agency to utilize products that meet “recognized” interoperability standards. (http://www.whitehouse.gov/news/releases/2006/08/20060822-2.html)

In order to recognize such standards, however, they needed to be created or made ready for recognition; and this process was tasked to the Health Information Technology Standards Panel.

On January 23, 2008, the Secretary of HHS officially provided recognition of 30 HITSP “Interoperability Specifications” for use by federal agencies, including for EHR-lab results reporting, biosurveillance, and consumer empowerment (i.e., personal health records, such as the Veterans Administration’s MyHealtheVet personal health record system.)



HITSP Background

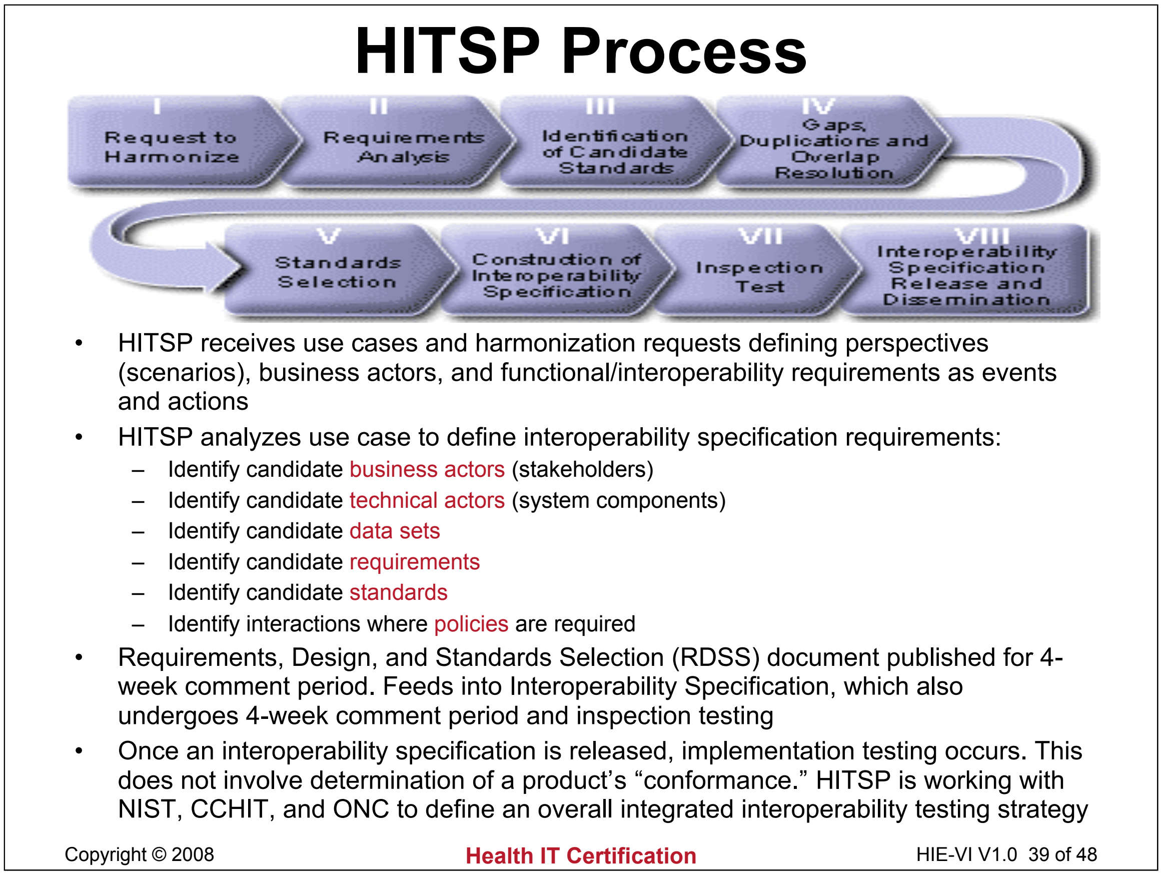
- ***Premise:*** Data and technical standards are critical to advancing national health IT agenda and achieving many of the intended health goals and outcomes:
  - The proper standard must be identified for a particular purpose
  - Where there are needs for new or additional standards, gaps must be filled
  - Detailed specifications must be available to guide implementation of standards in an exact and consistent way
  - There must be widespread adoption of standards by systems and their users
- HITSP brings together experts from across HIT community
  - Board of Directors provides governance
  - Technical and Coordination Committees volunteers
  - Project team manages process in accordance with ONCHIT1 contract
  - ANSI serves as Panel Secretariat
- **The standards harmonization process is an open, inclusive,* collaborative, use case-driven process**

* **HITSP members:**

- SDOs
- Other stakeholders
- Government bodies
- Consumer representatives

Copyright © 2008 **Health IT Certification** HIE-VI V1.0 38 of 48

The Healthcare Information Technology Standards Panel (HITSP) is a multi-stakeholder coordinating body designed to provide the process within which affected parties can identify, select, and harmonize standards for communicating information throughout the health care system. HITSP functions as a partnership of the public and private sectors and operates with a neutral and inclusive governance model administered by the American National Standards Institute (ANSI). ANSI, in cooperation with strategic partners HIMSS, Booz Allen Hamilton, and Advanced Technology Institute, was awarded the contract to advance this goal.



HITSP Process

I Request to Harmonize

II Requirements Analysis

III Identification of Candidate Standards

IV Gaps, Duplications and Overlap Resolution

V Standards Selection

VI Construction of Interoperability Specification

VII Inspection Test

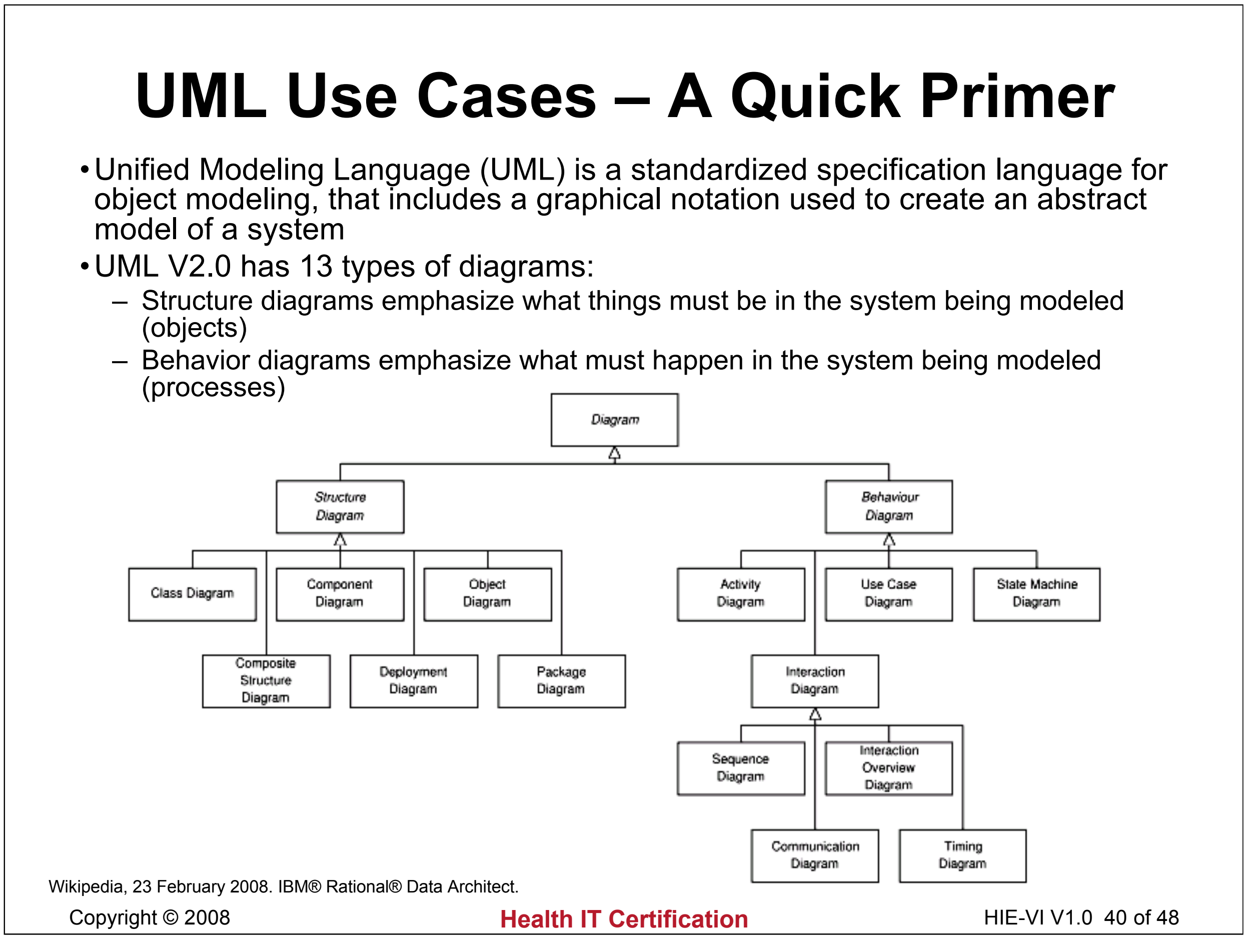
VIII Interoperability Specification Release and Dissemination

- HITSP receives use cases and harmonization requests defining perspectives (scenarios), business actors, and functional/interoperability requirements as events and actions
- HITSP analyzes use case to define interoperability specification requirements:
  - Identify candidate business actors (stakeholders)
  - Identify candidate technical actors (system components)
  - Identify candidate data sets
  - Identify candidate requirements
  - Identify candidate standards
  - Identify interactions where policies are required
- Requirements, Design, and Standards Selection (RDSS) document published for 4-week comment period. Feeds into Interoperability Specification, which also undergoes 4-week comment period and inspection testing
- Once an interoperability specification is released, implementation testing occurs. This does not involve determination of a product’s “conformance.” HITSP is working with NIST, CCHIT, and ONC to define an overall integrated interoperability testing strategy

Health IT Certification HIE-VI V1.0 39 of 48

AHIC, as the representative of public and private health sector stakeholders, identified the three use cases that drove the initial efforts of the HITSP. Nationwide public and private health sector priorities continue to focus the efforts of the HITSP. The use case driven HITSP harmonization process is implemented by formally chartered Technical Committees. The volunteers that comprise a Technical Committee follow an 8 step process, depicted on this slide.

Each HITSP Interoperability Specification (IS) is comprised of a suite of constructs that, taken as a whole, define how to integrate and constrain existing standards and specifications to satisfy the requirements imposed by a given use case. The IS groups specific actions and actors to describe the relevant context(s) for the use of the HITSP constructs that further identify and constrain standards where necessary.



UML Use Cases – A Quick Primer

- Unified Modeling Language (UML) is a standardized specification language for object modeling, that includes a graphical notation used to create an abstract model of a system
- UML V2.0 has 13 types of diagrams:
  - Structure diagrams emphasize what things must be in the system being modeled (objects)
  - Behavior diagrams emphasize what must happen in the system being modeled (processes)

Wikipedia, 23 February 2008. IBM® Rational® Data Architect.

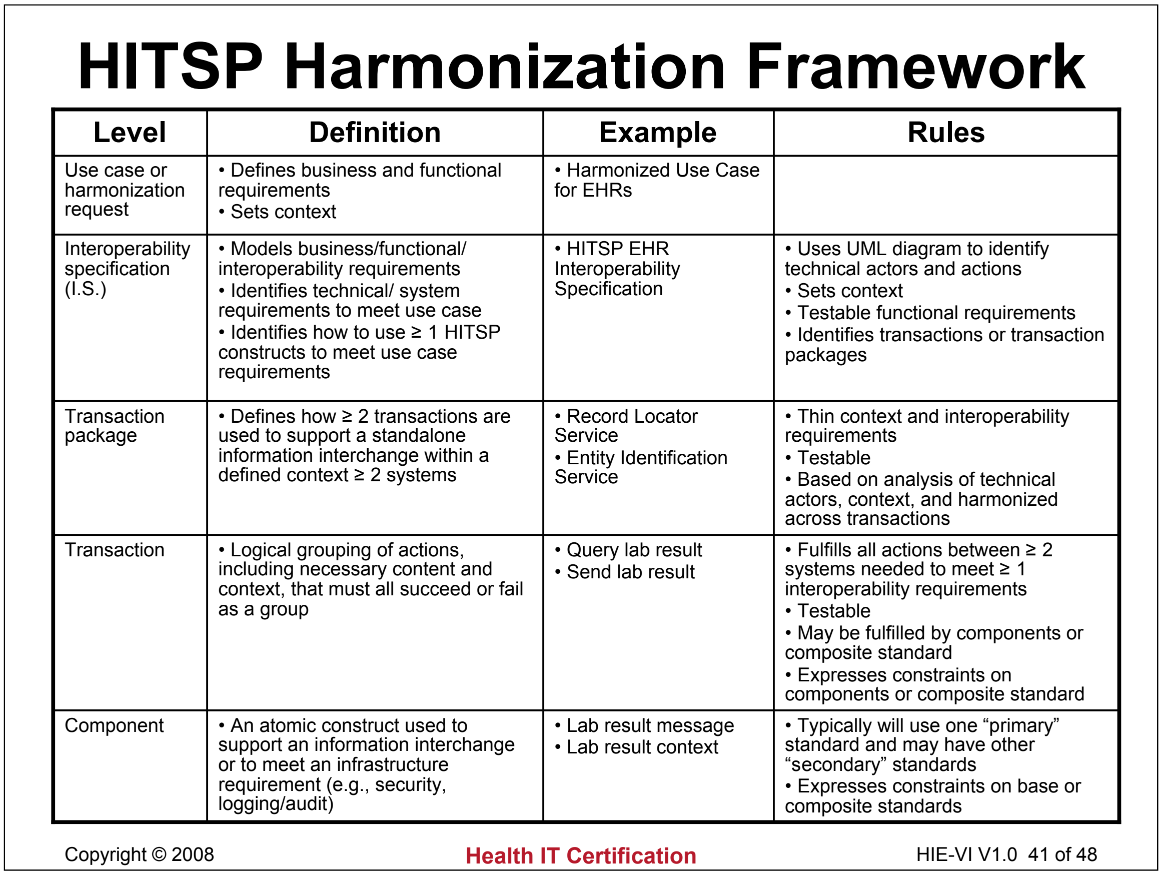
Health IT Certification HIE-VI V1.0 40 of 48

Use case modeling is used at the abstract level in business process mapping and in system analysis to identify, clarify, and organize system requirements in a technology free terminology and diagramming process. A use case organizes functional requirements, models the goals of user interactions, records paths (called *scenarios*) from trigger events to goals, describes one main flow of events (also called a basic course of action) and possibly other ones - called *exceptional* flows of events (or alternate courses of action). Uses cases are also multi-level, so that one use case can use the functionality of another use case.

A visual modeling technique for specifying use cases was first developed within the object-oriented (OO) community, as new programming techniques were developed for designing applications that could group tasks into objects capable of receiving messages, processing data, and sending messages to other objects. OO programming is also important for graphical user interface (GUI) design and as a bridge to complex relational database management systems. OO features have been added to C++ and other programming languages. Java is the most widely used OO language because it can run unchanged on many different platforms. Other commercially important OO languages are Visual Basic .NET and C# for Microsoft's .NET platform.

Unified Modeling Language (UML) is a standardized specification language for use case modeling, often co-authored by systems analysts and end users. Within systems engineering, detailed requirements may be captured in SysML requirement diagrams or similar mechanisms.

This slide illustrates the UML diagramming technique as well as identifies the 13 types of more detailed diagrams that may be used within use case modeling. While use case modeling may not appear complex, a full use case schema becomes very complex when applied to the design of relational and federated databases, and when converted to an XML Schema Definition (XSD), supplanting Data Type Definitions (DTDs) in XML. IBM's Rational Data Architect is the software tool most commonly used to create use case models and is the tool HL7 has adopted to describe its Reference Information Model (RIM) for its V3.0 standards.



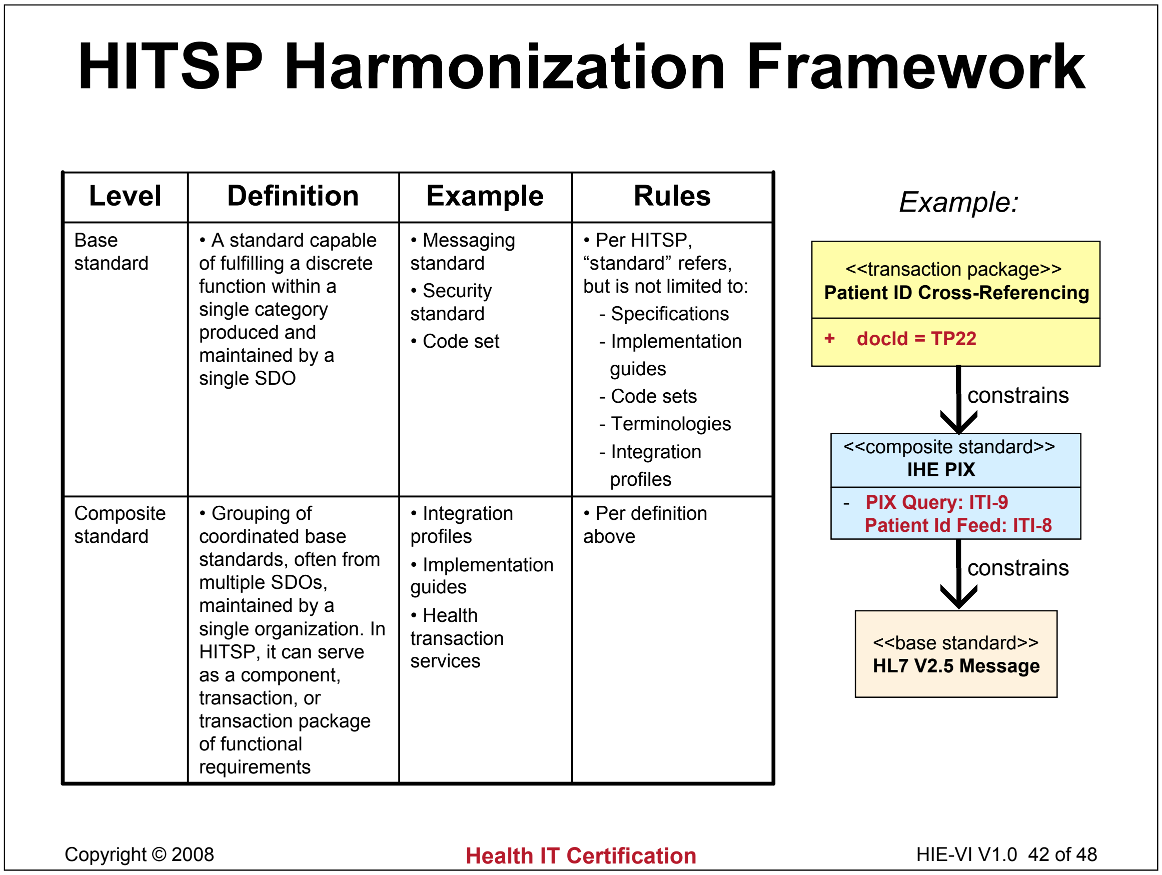
HITSP Harmonization Framework

Level	Definition	Example	Rules
Use case or harmonization request	• Defines business and functional requirements • Sets context	• Harmonized Use Case for EHRs	
Interoperability specification (I.S.)	• Models business/functional/ interoperability requirements • Identifies technical/ system requirements to meet use case • Identifies how to use ≥ 1 HITSP constructs to meet use case requirements	• HITSP EHR Interoperability Specification	• Uses UML diagram to identify technical actors and actions • Sets context • Testable functional requirements • Identifies transactions or transaction packages
Transaction package	• Defines how ≥ 2 transactions are used to support a standalone information interchange within a defined context ≥ 2 systems	• Record Locator Service • Entity Identification Service	• Thin context and interoperability requirements • Testable • Based on analysis of technical actors, context, and harmonized across transactions
Transaction	• Logical grouping of actions, including necessary content and context, that must all succeed or fail as a group	• Query lab result • Send lab result	• Fulfills all actions between ≥ 2 systems needed to meet ≥ 1 interoperability requirements • Testable • May be fulfilled by components or composite standard • Expresses constraints on components or composite standard
Component	• An atomic construct used to support an information interchange or to meet an infrastructure requirement (e.g., security, logging/audit)	• Lab result message • Lab result context	• Typically will use one “primary” standard and may have other “secondary” standards • Expresses constraints on base or composite standards

Copyright © 2008 Health IT Certification HIE-VI V1.0 41 of 48

HITSP has developed a Harmonization Framework (published September 18, 2007, www.hitsp.org) to describe how it evaluates standards and develops recommendations for harmonization.

HITSP uses use case modeling to develop its interoperability specifications (ISs). In addition to ISs that model the business requirements and technical/system requirements, there are three other types of HITSP constructs, each more specific and detailed than the next to further define transactions, actions, and specific interchange requirements. These are Transaction Packages (TP), Transactions (T), and Components (CO) as defined here.



HITSP Harmonization Framework

Level	Definition	Example	Rules
Base standard	• A standard capable of fulfilling a discrete function within a single category produced and maintained by a single SDO	• Messaging standard • Security standard • Code set	• Per HITSP, "standard" refers, but is not limited to: - Specifications - Implementation guides - Code sets - Terminologies - Integration profiles
Composite standard	• Grouping of coordinated base standards, often from multiple SDOs, maintained by a single organization. In HITSP, it can serve as a component, transaction, or transaction package of functional requirements	• Integration profiles • Implementation guides • Health transaction services	• Per definition above

Example:

<<transaction package>>
Patient ID Cross-Referencing

+ docId = TP22

constrains

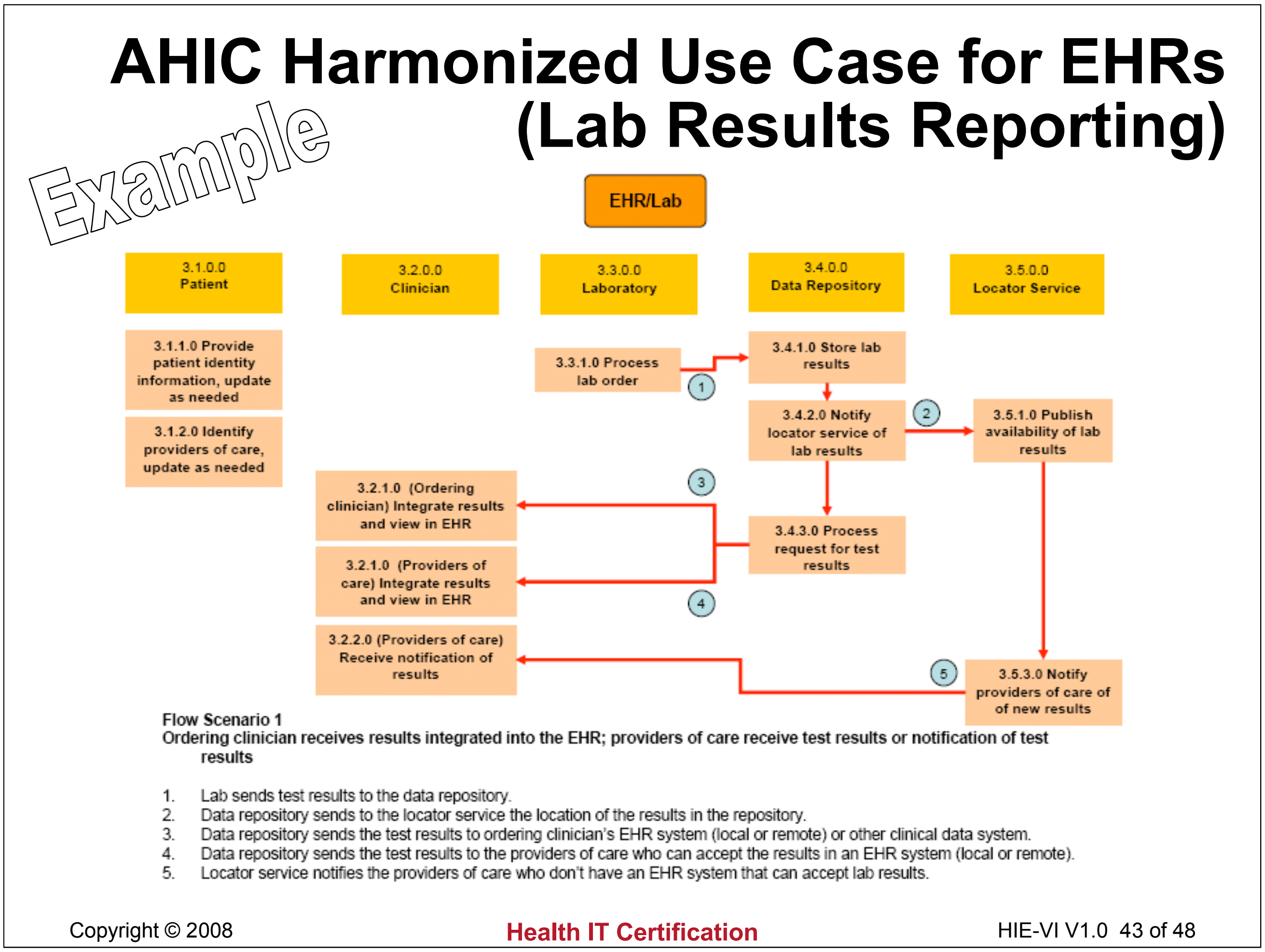
<<composite standard>>
IHE PIX

- PIX Query: ITI-9
Patient Id Feed: ITI-8

constrains

<<base standard>>
HL7 V2.5 Message

Ultimately, HITSP identifies base standards and composite standards from the harmonization process. For example, a transaction package may be patient identification cross referencing, which uses the IHE Patient Identifier Cross Referencing (PIX) integration profile to further specify the HL7 V2.5 Message relative to patient identification.



AHIC Harmonized Use Case for EHRs (Lab Results Reporting)

Example
EHR/Lab
3.1.0.0 Patient
3.2.0.0 Clinician
3.3.0.0 Laboratory
3.4.0.0 Data Repository
3.5.0.0 Locator Service
3.1.1.0 Provide patient identity information, update as needed
3.1.2.0 Identify providers of care, update as needed
3.3.1.0 Process lab order
3.4.1.0 Store lab results
3.4.2.0 Notify locator service of lab results
3.5.1.0 Publish availability of lab results
3.2.1.0 (Ordering clinician) Integrate results and view in EHR
3.2.1.0 (Providers of care) Integrate results and view in EHR
3.4.3.0 Process request for test results
3.2.2.0 (Providers of care) Receive notification of results
3.5.3.0 Notify providers of care of of new results
1
2
3
4
5

Flow Scenario 1

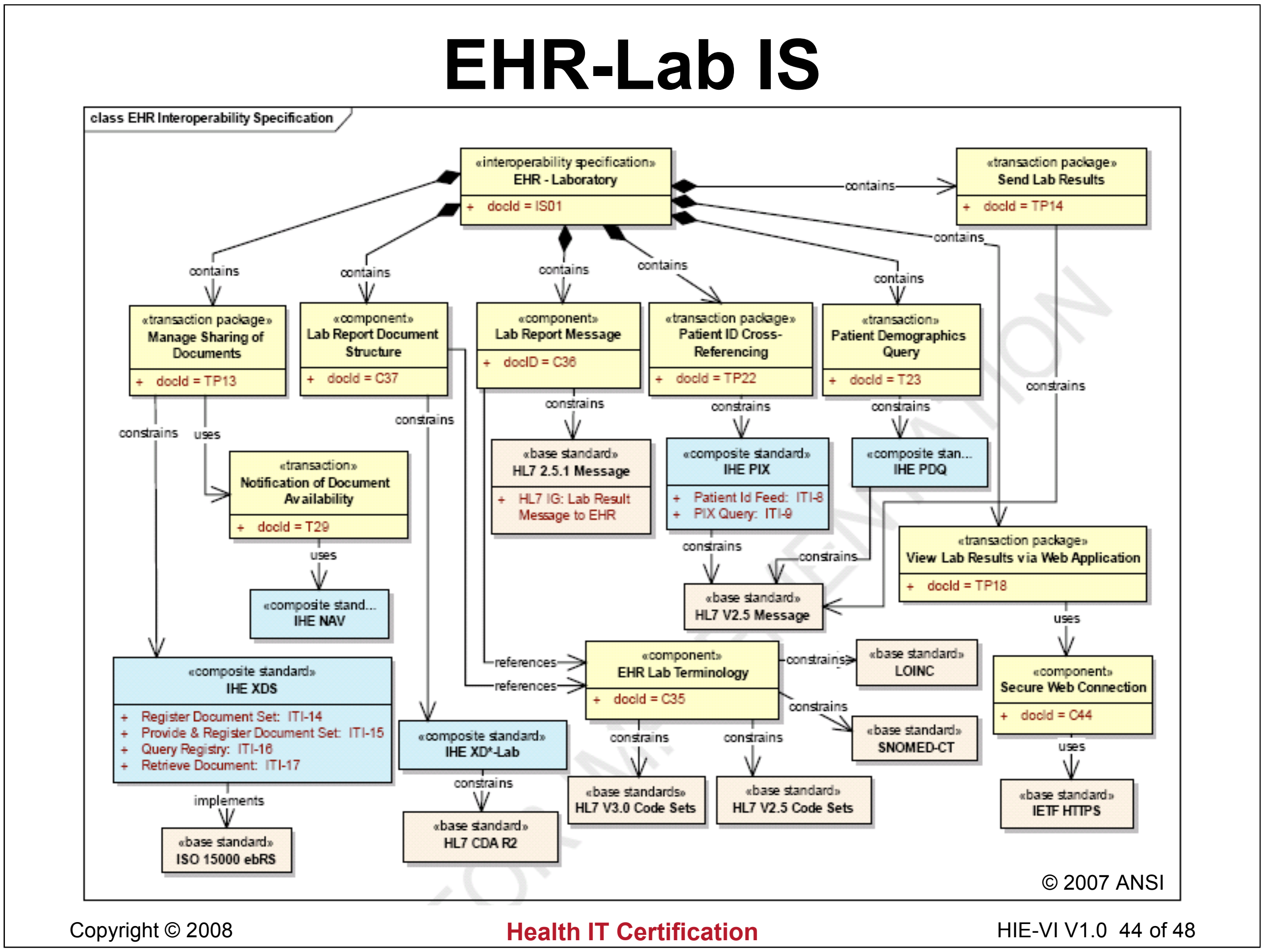
Ordering clinician receives results integrated into the EHR; providers of care receive test results or notification of test results

1. Lab sends test results to the data repository.
2. Data repository sends to the locator service the location of the results in the repository.
3. Data repository sends the test results to ordering clinician's EHR system (local or remote) or other clinical data system.
4. Data repository sends the test results to the providers of care who can accept the results in an EHR system (local or remote).
5. Locator service notifies the providers of care who don't have an EHR system that can accept lab results.

Health IT Certification

HIE-VI V1.0 43 of 48

The use case illustrated here is from the AHIC (www.hhs.gov/healthit/usecases/) and is intended to illustrate lab results reporting to an EHR within a NHIN environment. This use case was then taken by HITSP and developed into an Interoperability Specification.



EHR-Lab IS

class EHR Interoperability Specification

«interoperability specification»
EHR - Laboratory
+ docId = IS01

«transaction package»
Send Lab Results
+ docId = TP14

«transaction package»
Manage Sharing of Documents
+ docId = TP13

«component»
Lab Report Document Structure
+ docId = C37

«component»
Lab Report Message
+ docID = C36

«transaction package»
Patient ID Cross-Referencing
+ docId = TP22

«transaction»
Patient Demographics Query
+ docId = T23

«transaction»
Notification of Document Availability
+ docId = T29

«composite stand...
IHE NAV

«base standard»
HL7 2.5.1 Message
+ HL7 IG: Lab Result Message to EHR

«composite standard»
IHE PIX
+ Patient Id Feed: ITI-8
+ PIX Query: ITI-9

«composite stan...
IHE PDQ

«transaction package»
View Lab Results via Web Application
+ docId = TP18

«base standard»
HL7 V2.5 Message

«composite standard»
IHE XDS
+ Register Document Set: ITI-14
+ Provide & Register Document Set: ITI-15
+ Query Registry: ITI-16
+ Retrieve Document: ITI-17

«composite standard»
IHE XD*-Lab

«component»
EHR Lab Terminology
+ docId = C35

«base standard»
LOINC

«base standard»
SNOMED-CT

«component»
Secure Web Connection
+ docId = C44

«base standard»
ISO 15000 ebRS

«base standard»
HL7 CDA R2

«base standards»
HL7 V3.0 Code Sets

«base standard»
HL7 V2.5 Code Sets

«base standard»
IETF HTTPS

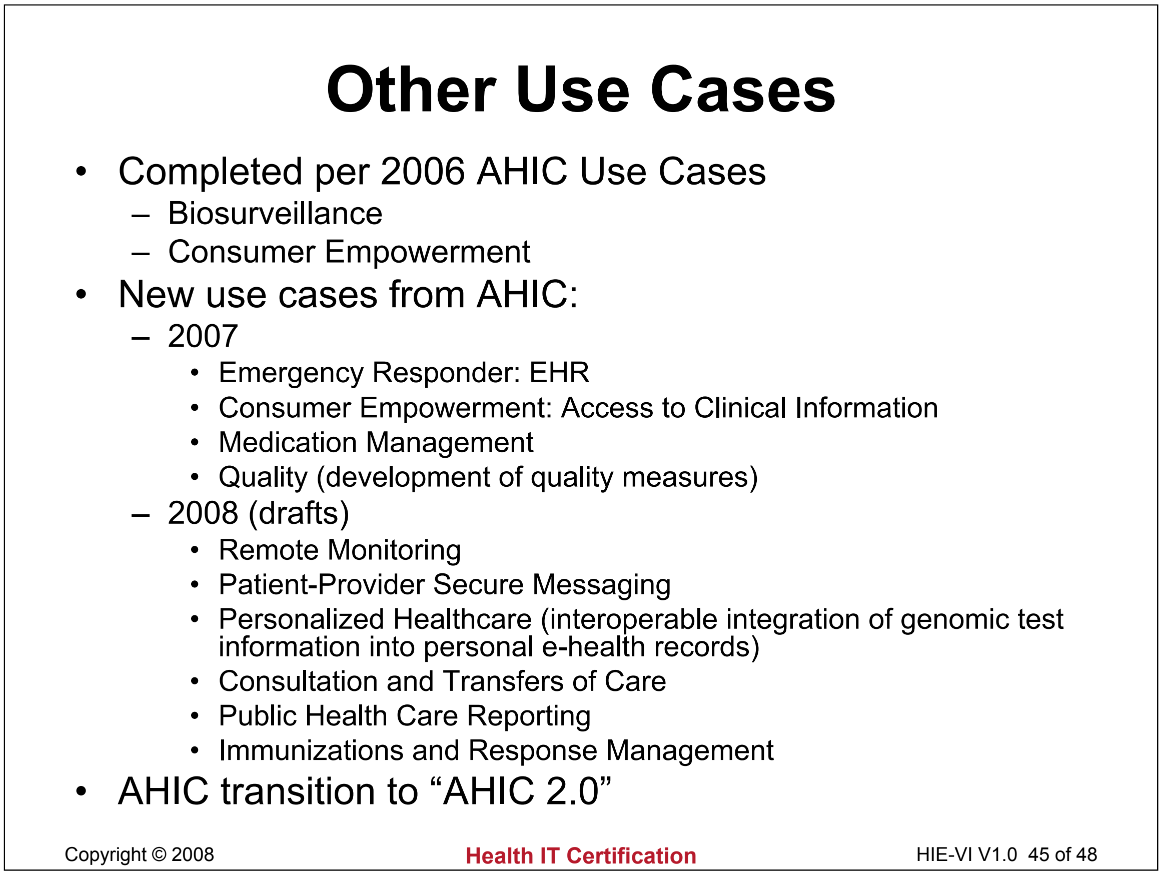
© 2007 ANSI

Copyright © 2008

Health IT Certification

The EHR-Lab Interoperability Specification (IS) in full is depicted here. (It is noted that this material was copied from the HITSP EHR Lab Results Reporting Interoperability Specification. HITSP documents indicate that content may be copied, without permission from ANSI, in an unaltered format.)

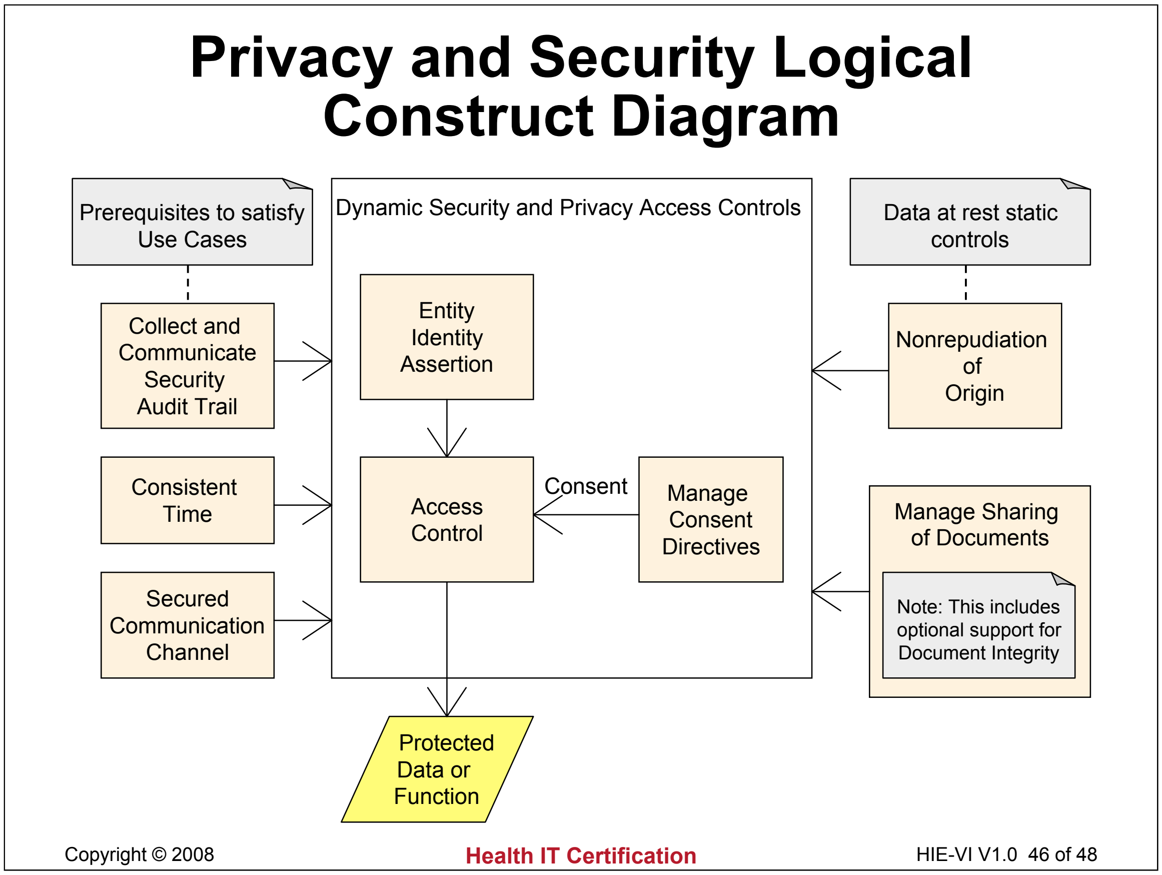
The EHR-LAB IS includes several transaction packages, transactions, and components, including the Manage Sharing of Documents (TP), Lab Report Document Structure (C), Lab Report Message (C), Patient ID Cross-Referencing (TP), Patient Demographics Query (T), Notification of Document Availability (T), View Lab Results via Web Application (TP), EHR Lab Terminology (C), and Secure Web Connection (C). In addition there are composite standards from IHE and base standards from HL7, LOINC, ISO, SNOMED, and IETF. HITSP notes that for readability, not all composite standards (e.g., Unified Code for Units of Measure [UCUM]) or other regulatory mandates, such as HIPAA and CLIA, are included in this figure.



Other Use Cases

- Completed per 2006 AHIC Use Cases
  - Biosurveillance
  - Consumer Empowerment
- New use cases from AHIC:
  - 2007
    - Emergency Responder: EHR
    - Consumer Empowerment: Access to Clinical Information
    - Medication Management
    - Quality (development of quality measures)
  - 2008 (drafts)
    - Remote Monitoring
    - Patient-Provider Secure Messaging
    - Personalized Healthcare (interoperable integration of genomic test information into personal e-health records)
    - Consultation and Transfers of Care
    - Public Health Care Reporting
    - Immunizations and Response Management
- AHIC transition to “AHIC 2.0”

Other uses cases the HITSP has addressed include biosurveillance and consumer empowerment. It is starting work on additional use cases as developed by AHIC. As AHIC transitions to an independent entity, additional use cases are likely to emerge, or other sources of use cases may be utilized. Several of the currently available and draft use cases will be explored in more depth in the remaining courses in this program.



Privacy and Security Logical Construct Diagram

Prerequisites to satisfy Use Cases

Collect and Communicate Security Audit Trail

Consistent Time

Secured Communication Channel

Dynamic Security and Privacy Access Controls

Entity Identity Assertion

Access Control

Consent

Manage Consent Directives

Protected Data or Function

Data at rest static controls

Nonrepudiation of Origin

Manage Sharing of Documents

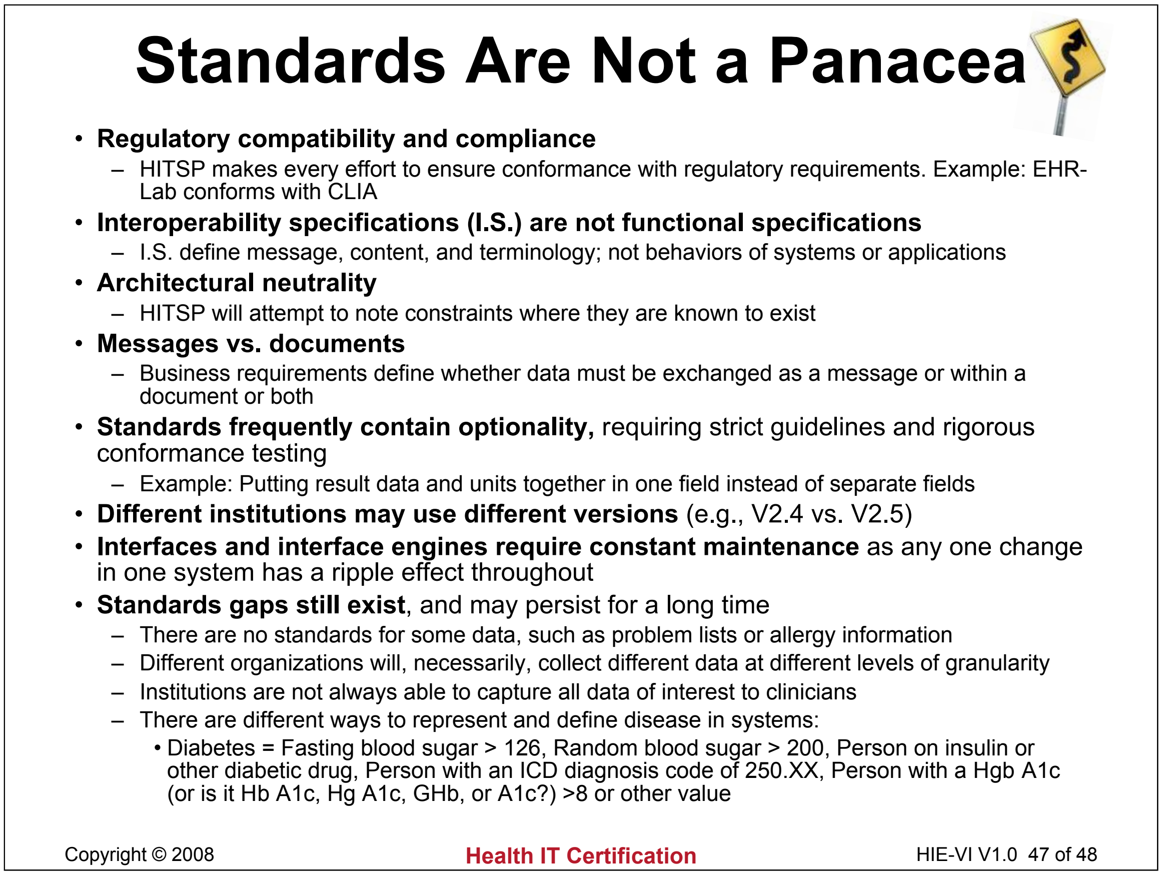
Note: This includes optional support for Document Integrity

Copyright © 2008 Health IT Certification HIE-VI V1.0 46 of 48

Because privacy and security cross all use cases, HITSP has developed a Security and Privacy Technical Note to provide the context for the HITSP Security and Privacy Constructs, based on the initial AHIC Use Cases. It observes that it has not attempted to resolve privacy or security policy issues, risk management, healthcare application functionality, operating systems functionality, physical control specifications, or other low-level specifications. Rather, the constructs described in the Security and Privacy Technical Note are intended to support a wide variety of security and privacy policies and technical frameworks, including core concepts from many common state laws as well as federal laws and regulations, including:

- HIPAA Privacy Regulations (45 CFR § 160 and 164 Part E)
- HIPAA Security Regulations (45 CFR § 160 and 164 Part C)
- Confidentiality of Alcohol and Drug Abuse Patient Records (42 CFR Part 2)
- Family Education Rights and Privacy Act (FERPA)
- Privacy Act of 1974
- Right to Financial Privacy Act (1978)
- Privacy Protection Act of 1980
- Electronic Communications Privacy Act (1986)
- Communications Assistance for Law Enforcement Act of 1994
- Telecommunications Act of 1996
- Financial Modernization Act (Gramm-Leach-Bliley Act) (2000)
- Emergency Supplemental Appropriations Act for Defense, the Global War on Terror and Tsunami Relief (Real ID Act) (2005)

The Technical Note associated with the Privacy and Security Logical Construct Diagram identifies selected standards and corresponding implementation guidance. In the Diagram, the Dynamic Security and Privacy Access Controls represent the relationship of the constructs to the use and disclosure of individually identifiable health information within the context of the AHIC Use Cases. The boxes on the left of the diagram represent prerequisites to these dynamic security and privacy access controls, while the boxes on the right of the diagram are static controls (applicable to data at rest).



Standards Are Not a Panacea

- **Regulatory compatibility and compliance**
  - HITSP makes every effort to ensure conformance with regulatory requirements. Example: EHR-Lab conforms with CLIA
- **Interoperability specifications (I.S.) are not functional specifications**
  - I.S. define message, content, and terminology; not behaviors of systems or applications
- **Architectural neutrality**
  - HITSP will attempt to note constraints where they are known to exist
- **Messages vs. documents**
  - Business requirements define whether data must be exchanged as a message or within a document or both
- **Standards frequently contain optionality,** requiring strict guidelines and rigorous conformance testing
  - Example: Putting result data and units together in one field instead of separate fields
- **Different institutions may use different versions** (e.g., V2.4 vs. V2.5)
- **Interfaces and interface engines require constant maintenance** as any one change in one system has a ripple effect throughout
- **Standards gaps still exist**, and may persist for a long time
  - There are no standards for some data, such as problem lists or allergy information
  - Different organizations will, necessarily, collect different data at different levels of granularity
  - Institutions are not always able to capture all data of interest to clinicians
  - There are different ways to represent and define disease in systems:
    - Diabetes = Fasting blood sugar > 126, Random blood sugar > 200, Person on insulin or other diabetic drug, Person with an ICD diagnosis code of 250.XX, Person with a Hgb A1c (or is it Hb A1c, Hg A1c, GHb, or A1c?) >8 or other value

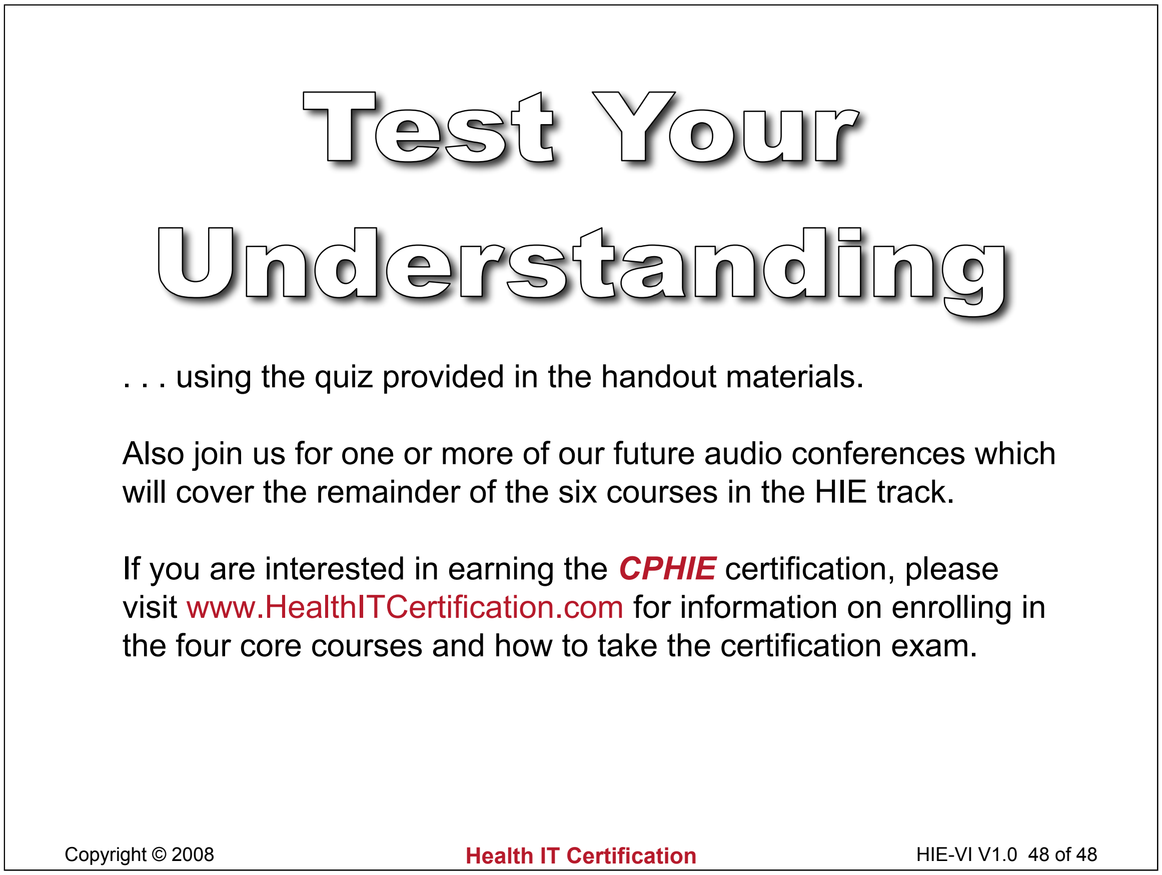
Copyright © 2008 Health IT Certification HIE-VI V1.0 47 of 48

Each of the HITSP interoperability specifications includes a section on "technical assumptions and scope," including, for example, cautionary notes that interoperability specifications are not functional specifications and that the interoperability specifications are intended to be architecturally neutral. Many in the industry are literally craving for solutions that fill all unmet needs.

Standards are not a remedy for all ills. Atif Zafar, MD, Associate Professor of Medicine, Indiana University School of Medicine, and Academic Staff, AHRQ, National Resource Center for Health IT, also identifies a number of issues that organizations must address that are not resolved by standards alone. Something as simple as system performance, for example, is a big factor in HIE acceptance – but cannot be solved solely with standards. Database and network performance must be well-managed. For example, he points out that despite having fast servers and wide network bandwidths, if a transaction-based database configuration is used instead of caching frequently used results, response time waiting for every result will be slow. This is especially a word of caution for those considering the inconsistent database (or point-to-point) approach to a federated architecture.

Part of HITSP's work is also to identify standards gaps. As these gaps are being filled, however, the ability to overcome issues must be addressed. It may be necessary to use a master synonym dictionary, for example, if terms or abbreviations cannot be standardized to everyone's satisfaction. However, moving to achieve greater standardization is also important, or filling the gaps in standards will be meaningless.

Finally, keeping up-to-date on what is happening nationally is important; but it must be recognized that just because a standard has been put forth or recognized by the federal government does not mean it will suddenly appear in every HIT product. Vendors need time to incorporate new standards into their product suite. Vendors can also be stymied by the laws of supply and demand. If a standard is not backward compatible and buyers do not want to rip out all their legacy systems and replace them with new systems, what economic incentive is there for the vendor to supply new product? Tools are becoming available for new technology to be overlaid on top older technology, but even this requires enhancement to products that the industry must demand.



Test Your Understanding

. . . using the quiz provided in the handout materials.

Also join us for one or more of our future audio conferences which will cover the remainder of the six courses in the HIE track.

If you are interested in earning the ***CPHIE*** certification, please visit www.HealthITCertification.com for information on enrolling in the four core courses and how to take the certification exam.

This course has studied the HIE architectures and their technology. Use the quiz in the handout materials to test your understanding of the content just presented. Answers are provided following the quiz.