Data Stewardship

Course VII.
Content for CPHIE

 Health IT Certification

Welcome to the Health IT Certification program on Health Information Exchange (HIE) Architectures. This is the third 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
VI – HIE Architecture
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

Allen E. Briskin, JD
Attorney, Davis Wright Tremaine, LLP
Co-author, *Guide to Establishing a Regional Health Organization*
San Francisco, CA

Harry L. Reynolds, Jr.
Vice President of HIPAA and Information Compliance Officer
Blue Cross & Blue Shield Of North Carolina, Inc.; Member, National Committee on Vital and Health Statistics (NCVHS); Chair, Committee on Operating Rules for Information Exchange (CORE), CAQH
Durham, NC

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:
  - Describe uses and users of health data in a health information exchange (HIE), recognizing the benefits and potential harms of data sharing
  - Discuss uses and users of health data in an HIE within the context of HIPAA protections
  - Define and describe the importance of data stewardship
  - Prepare to apply added measures of privacy and security protections to data sharing within an HIE
  - Prepare to manage the quality of the data exchanged within an HIE for all authorized uses

Objectives of this Course emphasize the importance of not only data protection but also the ability to assure the quality of data, certainly for treatment and payment purposes, but for quality measurement, reporting, and improvement, healthcare research, public health, and other authorized uses. The Course reviews both benefits and potential harms that may arise from enhanced data sharing, and the need to address not only where HIPAA provides protections for data sharing and where there may deficiencies or additional protections that are necessary and appropriate, but additional aspects of data stewardship that are critically important in improving the overall healthcare delivery system and the value of HIE.

Topics

Part 1. Data Uses and Users within an HIE

Part 2. HIE and HIPAA, State Law, and Other Legal Matters

Part 3. Information Practices

Part 4. Data Stewardship Solutions

Topics covered in this Course on Data Stewardship intend to strike a balance that will enable benefits of HIE to be achieved while protecting privacy, and assuring confidentiality, data integrity, and data availability. HIE enables many more uses and users of health data than when such data were housed in inaccessible paper charts. As a consequence, the importance of data stewardship must be stressed. In general, it is believed that HIPAA affords a baseline set of data stewardship principles, but that enhanced uses, more users, and greater risk through electronic capabilities require both greater attention to the HIPAA standards as well additional protections. Finally, while many are focused on privacy aspects, managing the quality of the data can be as great a need – especially as data are more widely dispersed and used directly in patient care, quality improvement, and research.

Data Stewardship

Part 1. Data Uses and Users within an HIE

Uses and users of data within an HIE are certainly more in number and may also be broader in scope than in any given provider, payer, or other organization using health data. In fact, many HIEs are looking to supply new uses of data as sources of revenue with which to sustain themselves. In addition, there are managers of the HIE that are separate and apart from the members of the workforce within typical user organizations. All of these data uses and users must be addressed with respect to their role in data stewardship.

Content Part 1.

- Definition of Data Stewardship
- Benefits and Potential Harms in Uses of Health Data Enabled Through an HIE
- Uses of Health Data
  - Treatment, Payment, and Operations
  - Quality, Research, and Marketing
- Users of Health Data
  - Covered Entities and Organized Health Care Arrangements
  - Business Associates and their Agents
  - Organizations with No HIPAA Relationship

The first Part of this Course sets the context for data stewardship, by defining data stewardship and describing issues associated with uses and users of health data in an HIE. This Part of the Course also uses the context of HIPAA protections to discuss these uses and users and to emphasize where HIPAA protections exist and where specific state laws and/or individual HIEs may afford stronger protections. It also stresses the importance of appreciating the balance that must be struck between protections and usability.

Data Stewardship

- **Stewardship** . . . Is personal responsibility for taking care of something one does not own
  - Duality of ownership in health information
- **Data stewardship** (corporate) is management of the corporation's data assets in order to improve their reusability, accessibility, and quality. Data stewardship needs are especially recognized when using data warehouses for data mining
- **Health data stewardship** (AMIA) "encompasses the responsibilities and accountabilities associated with managing, collecting, viewing, storing, sharing, disclosing, or otherwise making use of personal health information"

 Health IT Certification

Data stewardship is an important concept when considering how any organization should manage its data assets. Stewardship, as defined in the *Random House Webster's College Dictionary*, refers to the responsibility for taking care of something one does not own. For example, a bank is a steward of the funds an individual deposits in the bank. "The Case for Data Stewardship" (William Laurent, *DM Review*, February 2005) describes data stewardship as the management of an organization's data assets. This is especially important when there is a duality of ownership in the data. Data ownership is a particularly sensitive issue in health care because there is no federal law establishing precise ownership rights or responsibilities. Adele Waller, in "Legal Aspects of Computer-based Patient Records and Record Systems," IOM, 1991, describes the fact that most law concerning ownership of medical records is found in state licensure regulations and even in case law. At least with respect to the admissibility of medical records as evidence in a court of law, medical records compiled about patients and their treatment are generally believed to form the business records for the treating organization. As such, they are subject to the Federal Rules of Evidence. Waller further notes, however, it is generally accepted that patients have a qualified property interest in the information contained in the record – that is, they have the right to authorize disclosure of the information.

Data stewardship has become increasingly important – not only to ensure privacy protection but also to ensure that the data used to make decisions are sound and to ensure that any data used are properly maintained and retained. The Sarbanes-Oxley Act and the debacles of several publicly-traded companies raised the Nation's consciousness about how data are handled. Within health care, the importance of health data stewardship has arisen also because of concerns about handling data – especially in light of the fact that automated collection and enhanced data mining tools potentially make electronic health data more vulnerable to risk – again, not only in terms of privacy protections which are of utmost importance, but also in the quality of data with which health-related business and clinical decisions are increasingly being made. Safran, et al, in "Toward a National Framework for the Secondary Use of Health Data," *Journal of the American Medical Informatics Association*, February 2007, provide a definition of health data stewardship. Many have concerns about how well privacy of health information can be protected in the new world of automation in general and HIE in particular.

Is Anything Private Anymore?

- **Google Street View** (online mapping, used by employers to monitor employee smoking)
- **Fast Lane** (toll booth cameras, often used by divorce attorneys as well as toll authorities)
- **Discount cards** (save you money while collecting buying patterns)

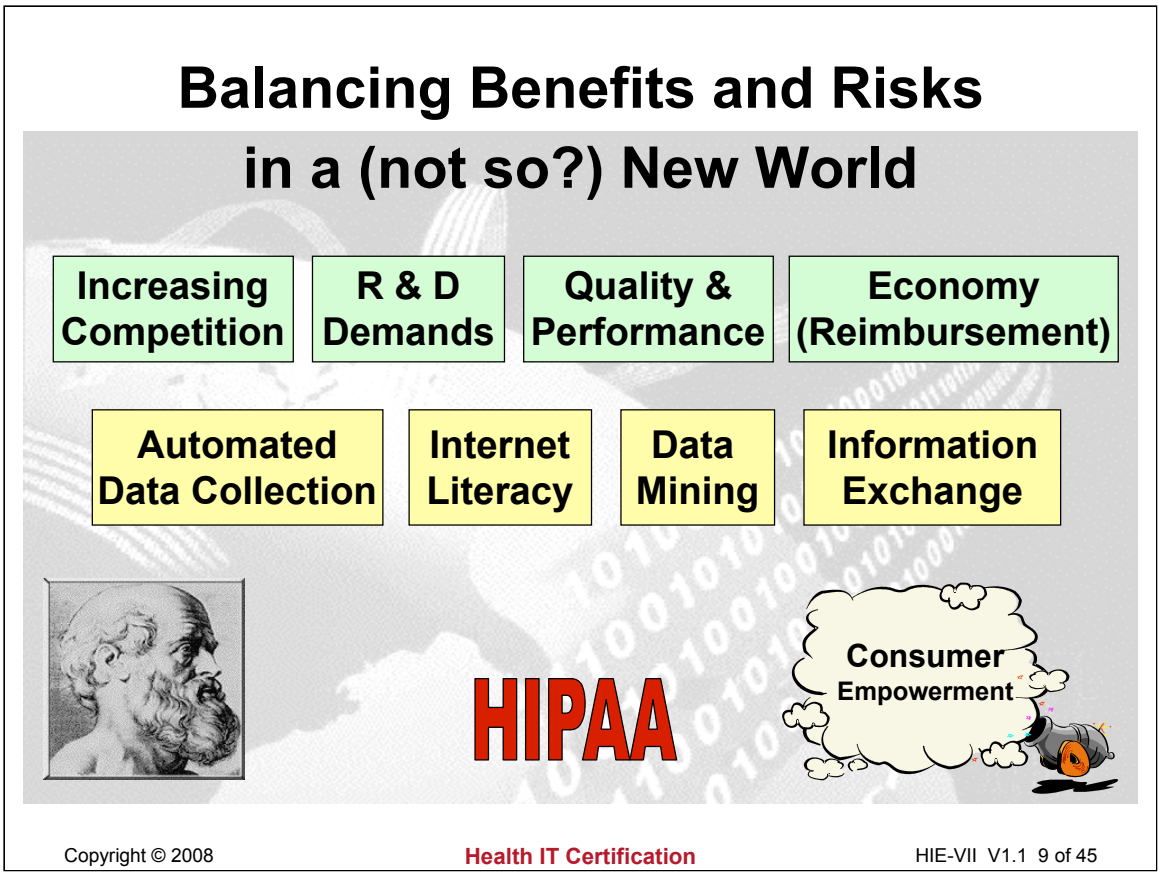
Identity theft
Insurance coverage
Mortgages/loans
Social consequences
Employment
Government
Marketing
Compromised care:
21% of consumers have withheld information from providers due to privacy concerns, Harris Interactive, January 2007

Who is the Data Steward?

In a survey of 169 people in the CareSpark HIE region, March 2006, 78% believed they personally were responsible for their health data stewardship.

In light of increasing concerns about loss of privacy in all aspects of our lives, a key question may be “who is the data steward?” for any given set of data. In fact, recent studies have suggested that many individuals believe they alone must be responsible for their health data stewardship.

While many people participate voluntarily in social networking sites and use discount cards at grocery stores, many are also becoming increasingly concerned about loss of privacy in all aspects of their lives, and especially with respect to health data – where there are potential discriminatory consequences. Many individuals cite potential risks for identity theft in general, and medical identity theft where someone uses their insurance information to acquire healthcare services; inability to get health, life, or other insurance coverage, mortgages, or loans; social consequences where family and friends are concerned; loss of employment; potential government action; and targeted marketing that may further enhance risk of health data misuse. Although many individuals do not cite the potential risk of compromised care, a Harris Interactive poll taken in January 2007 identified that 21% of consumers say they have withheld information from their providers because of worries the information might be disclosed. This puts these individuals at risk for compromised care because lack of complete information could result in medical errors, or lack of trust could result in not seeking care at all for an illness or injury.



Privacy has always been a concern in health care, even from the days of Hippocrates. However, heightened privacy concerns in general have spilled over into health care with concerns that could set off potentially disastrous effects. HIPAA may address some, but not all of these concerns. For example, automated data collection has enabled much more use of health data – to both benefit patient care and to potentially put individuals at risk from widespread data dissemination. Consumers are much more Internet literate, and both value and fear its power. As a result of Internet use, many consumers have come to expect opt-in and opt-out capabilities – for any information use. While perhaps not directly apparent to all consumers, data mining techniques have become extremely sophisticated – such that new patterns of health information can lead to potentially new treatments, but also grave concerns about linking health data to employment and other data. There has always been a sense of "power" when data are held by an organization or individual, but now information may be becoming the new currency in certain aspects of our lives – and there have been concerns expressed about health disparities associated with access to providers with or without HIT, and potentially in the future, in an HIE or not.

So technology can change our world in many ways. In a world with increasing competition, whether among treating organizations or pharmaceutical manufacturers – IT can support quality initiatives that ensure new drugs are working properly, but also increase cost of health care through aggressive marketing of brand name drugs. Research and development, whether to treat new diseases or develop better information technology products, also adds value and risk. Consumers want more information on the quality and performance of their providers, but providers want the data to accurately represent their performance and consumers may wonder that, if their data are used to substantiate such information – what other uses may be made of the data? Finally, when the cost of healthcare continues to escalate and reimbursement continues to be stressed, the economics of health data uses – for good and bad – are clearly becoming more visible.

What is PHI?

- ***Protected*** health information (**PHI**), under HIPAA, is individually identifiable health information held by or for a HIPAA covered entity (health plans, clearinghouses, and providers who use HIPAA transactions)
- ***Personal*** health information is ***any*** individually identifiable health information. When held outside of a HIPAA covered entity, it is not protected under HIPAA

What is TPO?

45 CFR

§ 164.502 Uses and disclosures of protected health information: general rules.

(1) *Permitted uses and disclosures.* A covered entity is permitted to use or disclose protected health information as follows:

(i) To the individual;

(ii) For treatment, payment, or health care operations, as permitted by and in compliance with § 164.506;

Uncertainty

Fear

Doubt

Copyright © 2008 Health IT Certification HIE-VII V1.1 10 of 45

In considering what health information exchanged within an HIE may or may not be protected under HIPAA, it is helpful to distinguish between protected health information (PHI) as defined by HIPAA and personal health information that may be outside of legal protections. PHI is clearly captured by providers, and payers clearly have access to PHI, but outside of the covered entity and business associate status, personal health information is conceivably available to many others.

Within the construct of HIPAA, PHI is able to be used and disclosed, within certain boundaries, for what has come to be referred to as "TPO" – for treatment, payment, and health care operations. Treatment is defined within HIPAA as the provision, coordination, or management of health care by one or more providers, including coordination or management of health care with a third party, consultation between providers relating to a patient, or referral of a patient for health care from one provider to another. Payment refers to the activities by health plan to obtain premiums or determine responsibility for coverage. It also refers to the activities of a provider or health plan obtaining/providing reimbursement for health care; determination of eligibility; risk adjustment; billing, claims management, collections; review for medical necessity; utilization review; and certain disclosures to consumer reporting.

HIPAA's standard permitting use and disclosure of TPO enables sharing of health data without authorization or consent among treating providers and with payers. However, Bill Braithwaite, MD, PhD, of Health Information Policy Consulting, observes that uncertainty (about how to interpret HIPAA requirements and lack of a standard set of technology to implement), fear (of violating laws that are not well understood), and doubt (as to whether exchange partners can be trusted) may be resulting in conservative approaches to legal advice, new and non-uniform more stringent state laws, and the potential to impede HIE and HIT initiatives.

In the "New World". . .

- **Non-covered providers** are increasing in number. Will these providers participate in HIE?
  - How will these providers prove their value?
  - Will these providers comply with principles of HIPAA?
- **Health plans** conduct case management and disease management directly with patients
  - How will they define minimum necessary?
  - Will providers accept that they "may rely on a requested disclosure as the minimum necessary for the stated purpose when the information is requested by another covered entity"? (45 CFR §164.514(d)(3)(iii)(B))
- **Organizations with no HIPAA relationship** may have an interest in HIEs, for example, commercial PHR vendors, personal trainers, banks

A new world is also emerging, where not only are HIEs supporting data sharing, but roles are blurring and changing. A surprising, and increasing, number of providers fall out of the HIPAA covered entity definition when they do not use the HIPAA financial and administrative transactions, perhaps because these providers are no longer accepting Medicare and file paper claims for other patients; are chiropractics, dentists, physical therapists and other specialty treatment providers who frequently require direct payment; or when they make special arrangements to treat patients for a fixed fee over the course of a year (referred to as "concierge" providers, or "cash-only" providers by the American Academy of Family Practice). Even though these providers may adhere to the principles of HIPAA, the federal government has no compliance authority over them.

Health plans are also starting to provide case management and disease management services more directly to individuals who hold policies. Although within the HIPAA definition of "payment," these functions often require more information than is available via claims, and some individuals may be surprised at this role and how much information a payer may have about them. Recently, for instance, some providers were surprised to learn that health plans were receiving not only what lab tests had been charged, but the results of the tests were being sent to them from the commercial labs performing the tests. In addition, although minimum necessary does not apply to disclosures to the individual or for treatment, minimum necessary can be applied to "payment." Many covered providers express concern that payers ask for more than is minimum necessary, and may not accept that HIPAA's minimum necessary standard does permit covered entities to define what they believe to be minimum necessary, and that when health information is exchanged between covered entities, it is acceptable to rely on the requesting covered entity for the request to be minimum necessary under HIPAA.

Health Care Operations

"any of the following activities of the covered entity to the extent that the activities are related to covered functions:

(1) conducting **quality assessment and improvement activities** . . .;

(2) reviewing the competence or qualifications of healthcare professionals . . .;

(3) underwriting, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits . . .;

(4) conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;

(5) business planning and development . . .; and

(6) business management and general administrative activities of the entity" (45 CFR §164.501)

For example,
Does an architectural firm need access to PHI to understand how many rooms should be designed with enlarged doors to accommodate a hospital's new bariatric program?

Of special interest to HIEs and especially the federal government in its efforts to adopt a nationwide health information network (NHIN) is the use of such structures to improve the quality of health care and drive healthcare value. Some HIEs have explicitly formed as a result of earlier collaborative efforts to address quality improvement. However, many also view the HIPAA definition of health care operations, incorporating quality activities, as somewhat of a slippery slope, where some believe that HIPAA may be too permissive.

Quality Assessment & Improvement

- "Outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose; population-based activities relating to improving health or reducing costs, protocol development, case management and care coordination, contacting of healthcare providers and patients with information about treatment alternatives . . ." (45 CFR §164.501)

Ethical & Regulatory Issues of QI

QI finds Vioxx linked to heart attacks. Product recalled.

Research

- "A systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge." (45 CFR §164.501; 45 CFR 46, The Common Rule)

Marketing

- Communications other than "face-to-face made by a covered entity to an individual; or promotional gift of nominal value provided by a covered entity" (45 CFR §164.508(a)(3))

How would you feel if an ad for a stent appeared next to the CT scan of your heart?

Many have expressed concerns about data stewardship not only in relationship to health care operations in general, but quality activities in particular, especially as they may slide into research and possibly even into marketing.

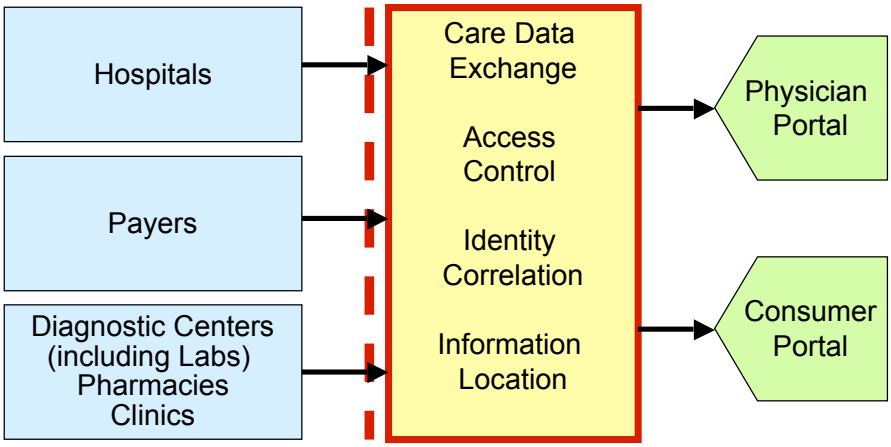
The Hastings Center was contracted in 2007 by the Agency for Healthcare Research and Quality (AHRQ) to conduct a project looking at the ethical and regulatory issues associated with healthcare quality improvement. The study looked at organizational responsibility for quality improvement, informed participation, publication of quality improvement findings, implications of HIPAA on quality improvement activities, practical and ethical issues of organized healthcare arrangements (OHCA), as defined by HIPAA, and other collaboratives on quality improvement, accountability for conducting quality improvement projects, and the issue of when a given project is quality improvement or research. Overall, the Hastings Center report provides suggestions and case studies for promising strategies that should provide a framework of key concepts and practices to ensure responsible implementation of quality activities and also protect persons used as subjects of research. For instance, the Hastings Center has suggested that an organization conducting both quality and research activities may want to look at joint oversight for these activities.

Certainly the question of when does a quality improvement study become research needs to be addressed – both from the standpoint of ensuring that quality studies can provide benefit but also that quality studies do not endanger individuals. For example, it was a quality improvement study in a large healthcare provider organization that led to the identification that the drug Vioxx appeared to be associated with increasing risk for heart attack. As HIEs enable quality improvement studies on larger pools of data, the likelihood of identifying such findings will only increase.

There are also concerns that large pools of data collected for quality activities may be used for marketing or other purposes unanticipated by individuals, or that cash-strapped organizations may view marketing as a means to acquire HIT. It is these potential uses of personal health information that many individuals fear.

Case Study

Santa Barbara County Care Data Exchange oldest RHIO
Until it Shut Down March 15, 2007



Vision and technology issues solved
Privacy concerns and ongoing costs insurmountable

 Health IT Certification HIE-VII V1.1 14 of 45

Perhaps the most telling result of concerns reflecting "uncertainty, fear, and doubt" about HIPAA and privacy was the closure of the high-profile Santa Barbara County Care Data Exchange (SBCCDE). Although there were ongoing cost issues, many cite insurmountable privacy concerns as the cause of few providers willing to sign up to participate in the HIE and hence the inability to sustain itself (*Healthcare IT News*, March 16, 2007). Although not explicitly documented, concerns have been expressed that the ability to only view information and not retrieve data into the data users' systems (as evidence of information review or for future reference) was a significant workflow issue and factor resulting in lack of interest on the part of providers.

There are lessons to be learned from the Santa Barbara experience: Their vision of enabling data exchange among competing organizations and the technology infrastructure to support access control, identity correlation, and information location put them well ahead of their peers ("Moving Toward Electronic Health Information Exchange: Interim Report on the Santa Barbara County Data Exchange," California HealthCare Foundation, July 2003; "Santa Barbara Blueprint: A Regional Health Data Network Takes the Plunge," Michael Schrader, *Journal of AHIMA*, May 2004). Certainly the fact that CalRHIO announced a few days after the announcement of SBCCDE's closing that CalRHIO had selected its technology partners to connect communities and the entire state with a suite of affordable, secure, privacy-protected services does not suggest that an HIE cannot succeed in California. One observer of the CalRHIO project noted, however, that "I hope that our national perpetual state of fear does not hamstring data-sharing efforts." (Greg Wenneson in "Does Santa Barbara RHIO shutdown affect California HIE Efforts?" *Healthcare IT News*, March 16, 2007)

Data Stewardship

Part 2. HIE and HIPAA, State Law, and Other Legal Matters

 Health IT Certification

So in this new world, HIPAA remains an important set of data stewardship principles, but may need enhancements.

Content Part 2.

- Does HIPAA Provide Context for HIE?
- Legal Agreements
- State Laws and HIEs
- Potential Liability Concerns and Risk Mitigation Strategies

The second Part of this Course looks more closely at the relationship of HIEs to HIPAA and what other legal concerns there may be and what measures could be taken to address these.

Does HIPAA Provide Context, or Not?

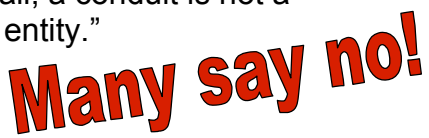
- HIPAA provides a backdrop for how HIEs deal with privacy and security
  - Many covered entities are involved
- But most HIEs are not ***directly*** subject to HIPAA's requirements
  - Most HIEs are not covered entities, or even OHCAs
  - Does the business associate relationship apply?
  - Is the business associate relationship strong enough?
  - How are non-covered entity providers and others included in the data sharing process?
- Whether applicable or not, is HIPAA enough a decade after it was written?
  - Is applicability a matter of interpretation?
  - Does HIPAA need to be updated to be more explicit?

While many covered entities and business associates assume that HIPAA covers all aspects of dealing with protected health information (PHI), many have pointed out that HIEs are generally not covered entities, or even organized health care arrangements (OHCA) as defined by HIPAA. Instead, many – though not all – HIEs consider themselves business associates of the covered entities they serve, and the covered entities either have uni-lateral business associate agreements with them or data sharing agreements that provide more universal business associate coverage. However, as was pointed out in the previous Part, not all participants in an HIE may be covered entities. And while the burden of defining who is a covered entity and who is a business associate strictly speaking falls upon covered entities, not all covered entity participants in an HIE may realize this responsibility or be aware that some of their counterpart providers are not covered entities!

It is not feasible for this Course to definitively answer the questions posed here – only legislators or regulators are able to do so. However, HIPAA does establish some context for consideration – if only to identify what individuals, covered entities, or HIE structures may decide to do on their own as more of a "best practice."

Is an HIE a Conduit?

- OCR FAQ:
  - "The Privacy Rule does not require a covered entity to enter into business associate contracts with organizations, such as the US Postal Service, certain private couriers and their electronic equivalents that act merely as conduits for protected health information."
  - A conduit is described as "an organization that transports information but does not access it other than on a random or infrequent basis as necessary for the performance of the transportation services or as required by law."
  - Further, "since no disclosure is intended by the covered entity, and the probability of exposure of any particular protected health information to a conduit is very small, a conduit is not a business associate of the covered entity."



 Health IT Certification

In addition to the issue of whether an HIE is a covered entity or business associate, there may be reason to believe that an HIE is a conduit, especially if its architecture is solely that of a switch. Many HIEs that form with a federated architecture have stressed that they retain no health information. The response to a Frequently Asked Question (FAQ) posted on the HHS Office for Civil Rights (OCR) web site clearly describes a conduit, but obviously does not explicitly mention an HIE as an example. Some HIEs consider themselves only a conduit and not a business associate, especially when the HIE uses a federated or switch architecture.

Many covered entities, however, are uncomfortable with this view and want to strengthen the relationship through contractual obligations.

Legal Agreements

- Business Associate Contract
  - Requirement of both HIPAA Privacy and Security Rules when covered entities use other businesses to perform work for them
- Data Use Agreement
  - A requirement of HIPAA for a party to use a limited data set (i.e., data that are partially but not fully de-identified) for research, public health, or health care operations.
- Data Sharing Agreement
  - Agreement among parties who will share data, usually indicating the criteria for data access, whether or not there are any conditions for certain types of use, specific (privacy, security, and other technical) standards with which the data sharing must conform, and whether the data may be de-identified
- Participation Agreement
  - Agreement that specifies the terms of the relationship between parties in an HIE and the roles, rights, and responsibilities of each party to the HIE. Signing of this agreement usually means that each participant will adhere to the policies and procedures of the HIE

There are a number of legal agreements that may be used to support exchange of data within an HIE. The business associate contract is the basic HIPAA agreement for covered entities to use when engaging other parties to perform work for them. A business associate, as defined by HIPAA, is a person who, on behalf of a covered entity or OHCA but other than in the capacity of a member of the workforce, performs or assists in the performance of a function involving the use or disclosure of individually identifiable health information; or provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services that involves the disclosure of individually identifiable health information from the covered entity, or from another business associate of the covered entity to the person (45 CFR §160.103). A data use agreement is another HIPAA requirement when a “limited data set” is exchanged with another party for research, public health, or health care operations. The limited data set is individually identifiable health information from which most but not all HIPAA-specified identifiers have been removed (45 CFR §164.512(e)(4)).

Many HIEs have adopted a data sharing agreement and/or participation agreement (HIE Enterprise Integration Strategy: Templates for Planning, Assessing & Document, www.calrhio.org/?cridx=408). These agreements may be construed as broader than the HIPAA business associate contract. They address many issues associated with the exchange of information in addition to privacy and security. It is not clear whether it is necessary to have both a data sharing agreement and a participation agreement, or if one tends to be established between entities and another is an agreement with patients, but obviously any agreements should be put into place by a qualified attorney advising the HIE specifically.

State HIE Laws

www.ncsl.org/programs/health/forum/hitch/HIE_networks.htm

- A number of states are addressing legislation relating to various issues associated with HIEs, including:
  - Support for their formation, creation of statewide networks
  - Grants, low or no-cost loans, contracts, other funding sources
  - Consent and other privacy and security requirements, including conforming language among state's statutes
  - Health reform that may be enabled by HIE
  - Requirements for adoption of EHR
  - Appropriating funds for pilot PHR projects
  - Definition of an HIE as a "health care facility" for licensure purposes
  - Data set requirements

 Health IT Certification

Many states have started introducing bills and enacting statutes –to help support the formation of HIEs, promote their sustainability, and assure their value, as well as to address some of the potential legal issues that newly forming HIEs may face.

The National Conference of State Legislatures provides a web site that tracks state legislation by state, bill, status, and topics included. Fully 18 states enacted one or more pieces of legislation in 2007 relating to one or more of the topics identified here, and several others have pending legislation or legislation that failed but may be re-introduced in the future. This is obviously a very active issue for states.

Other Legal Matters

- Most common potential liability for HIEs is likely:
  - Negligence
    - General negligence
    - Negligent hiring, retention, training, and supervision
    - Invasion of privacy and/or emotional distress
  - Contract claims
    - Breach of contract
    - Breach of warranties
- Practical considerations
  - Data integrity
  - Service provider issues
  - Patient restrictions in data use
  - Quality of care issues
- Legal risk mitigation and limitation strategies
  - Arbitration clauses in contracts
  - Jurisdiction and venue specifications if an HIE operates in multiple states
  - Disclaimers or limitations on liability
  - Indemnity for damages provisions in contracts
  - Waivers of liability from patients (based on that an HIE is only a passive conduit in the exchange)
  - Insurance
  - Immunity legislation (also based on the belief that an HIE is a passive conduit)

 Health IT Certification

Several members of the American Health Lawyer's Association published an article (Anning D., et al, "Blame it on the RHIO: Potential Liability Concerns with Electronic Health Information Exchange," *Health Lawyers News*, June 2006) describing potential liability concerns with HIEs. Although they identified issues of HIPAA compliance, privacy and security, intellectual property, tax-emption, labor and employment, antitrust, anti-kickback and self-referral, and liability issues as potential concerns, they acknowledged that the most likely legal issues facing HIEs would be liability for negligence and contract claims. They also identified a number of risk mitigation and limitation strategies that either HIEs could adopt themselves in contracts or lobby to have addressed in state legislation.

In addition, the authors of the article observe that there are some practical considerations that HIEs should consider as they develop data sharing and participation agreements. They observe, for example, that the data exchanged by an HIE is only as good as the data from the source systems, so that HIEs should be indemnified against data corruption that arises from these other sources. They also suggest that potential problems with mis-matching patients, inaccessibility to data due to service disruption, erroneous information from poor software design, etc. could result in injury to patients, so that HIEs might want to seek indemnification from their vendors and waivers of liability from data users and patients for errors that are the fault of third-party vendors and outside the control of the HIE. The more options given to patients to restrict access to some or all of their information can also result in increased exposure of risk from improper disclosure, so again the authors suggest seeking a waiver from data users and patients for improper disclosures that are the fault of service providers. Finally, the authors observe that quality of care ultimately rests with the provider and that providers must not abdicate their responsibility to appropriately interview patients and patients must not abdicate their responsibility to provide full medical histories – and that these conditions should be clearly stated in any usage of an HIE, with potential use of indemnification from providers and waivers of liability from patients.

Certainly while all of these matters are of concern and should be attended to when HIEs are forming, the extent to which legal clauses can or will be implemented will need to be studied by each HIE.

Data Stewardship

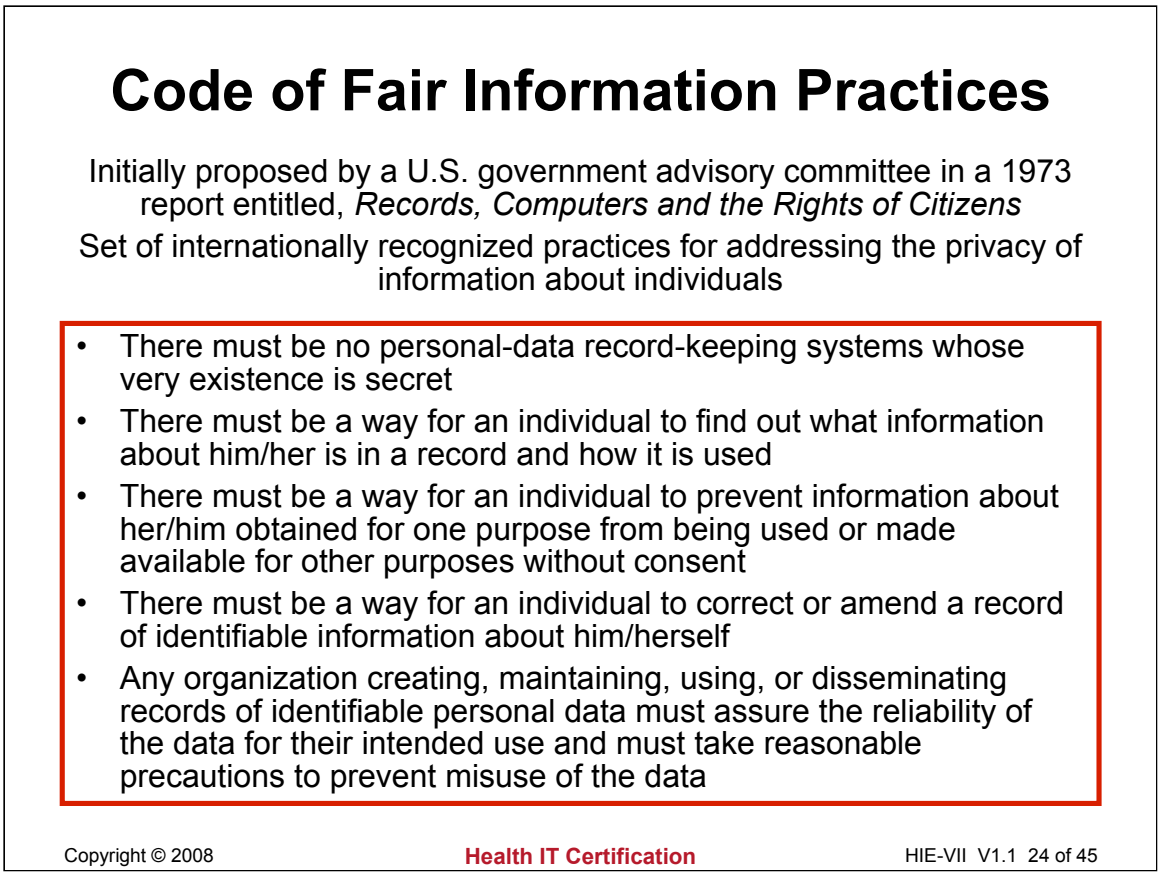
Part 3. Information Practices

With a backdrop of enhanced opportunities for uses and potential misuses of health data within an HIE and potential legal arrangements that may afford protections, it is also important to consider ways HIEs can immediately improve their information practices.

Content Part 3.

- Fair Information Practices
- Health Data Stewardship
  - Connecting for Health
  - American Medical Informatics Association
  - AHRQ RFI on a National Data Stewardship Entity
  - National Committee on Vital and Health Statistics Recommendations to ONC

Part 3 of this Course describes Fair Information Practices and provides references for guidance on health data stewardship.



HIEs need trusting relationships, or data sources will not be willing to share the data they hold and individuals will lose faith in the healthcare delivery system. Participants in an HIE must agree to follow certain information sharing policies and procedures. As seen in the previous section, it is advisable to have these agreements in writing. The agreements, however, should be the minimum necessary so they do not add burdensome processes that are costly and reduce the likelihood of participation. The agreements should reflect the local culture – which varies significantly between states and even within regions of a state, recognizing, however, that ultimately an HIE might be connecting with a nationwide health information network and will need to follow the minimum necessary requirements for participation in that construct. HIE agreements should also be based upon mutually agreed upon principles and these principles should be enforceable and enforced.

The principles in the Code of Fair Information Practices (FIPs) are those that have existed for many years and are internationally recognized. Certainly they were an important reference in formulating HIPAA's Privacy Rule, although some believe that the HIPAA Privacy Rule did not go even as far as the Code of FIP would suggest. For example, some would claim that the ability to use health information for treatment, payment, and a myriad of healthcare operations (TPO), even with a notice of privacy practices to that effect, is more than intended under FIPs. Bob Gellman in his "Fair Information Practices: A Basic History," January 4, 2008, observes that critics of FIPs can be found on both sides. "Some in the privacy community believe that FIPs are too weak, allow too many exemptions, do not require a privacy agency, fail to account for the weaknesses of self-regulation, and have not kept pace with information technology. Critics from a business perspective often prefer to limit FIPs to reduced elements of notice, consent, and accountability. They complain that other elements are unworkable, expensive, or inconsistent with openness or free speech principles." Different HIEs will likely weigh in differently on the specifics of these principles, and especially as some state laws may become more stringent than HIPAA, although in general FIPs are certainly best practices for privacy and security approaches to be adopted.

Health Data Stewardship

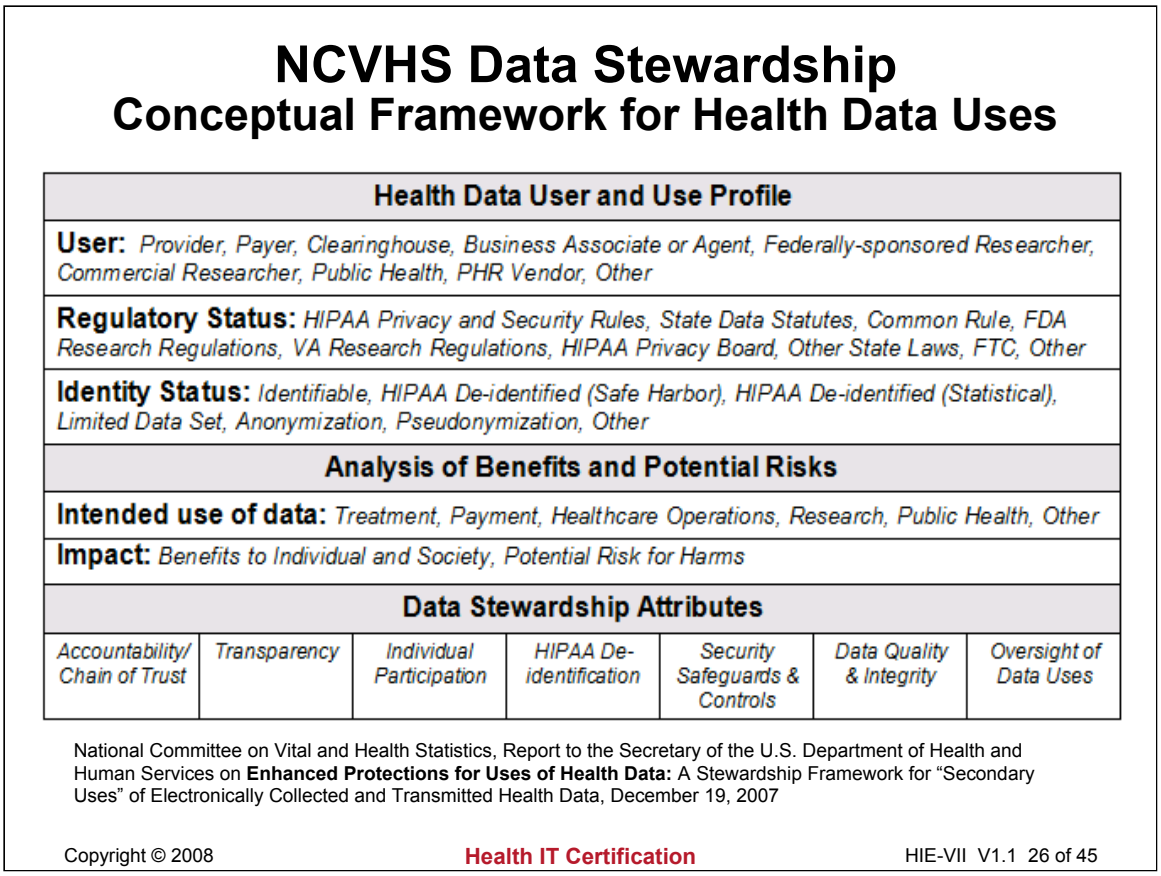
Connecting for Health Common Framework – Privacy Principles

1. Openness and transparency
2. Purpose specification and minimization
3. Collection limitation
4. Use limitation
5. Individual participation and control
6. Data integrity and quality
7. Security safeguards and controls
8. Accountability and oversight
9. Remedies

American Medical Informatics Association – Proposed Data Stewardship Principles

- Accountability (including governance, oversight, and regulations)
- Openness and transparency (including structure, processing and delivery of data, and business processes and practices)
- Note to patients
- Privacy and security (including data quality, de-identification, and costs of re-identification)
- Granularity of patient consent
- Permitted uses and disclosures (including data aggregation and analyses)
- Enforcement and remedies

Two organizations that are thought leaders in HIE and uses of health data have proposed principles that perhaps enhance and update the Fair Information Practices, or at least relate them more closely to HIEs.



As evidence of the federal government's interest in addressing privacy concerns, the Office of the National Coordinator (ONC) on Health Information Technology asked the National Committee on Vital and Health Statistics (NCVHS) in 2007 to make recommendations relative to needed protections for uses of health data envisioned to be performed or aided by a nationwide health information network (NHIN). NCVHS delivered the Report to the Secretary of the U.S. Department of Health and Human Services Enhanced Protections for Uses of Health Data: A Stewardship Framework for "Secondary Uses" of Electronically Collected and Transmitted Health Data on December 19, 2007.

The NCVHS Data Stewardship Conceptual Framework for Health Data Uses is a tool intended to outline how any organization (whether covered entity, business associate, company outside of the scope of HIPAA) may approach evaluation of its intended uses of health data and recognize where it may need to enhance its data stewardship processes. *For example, a business associate of a payer, that is covered by HIPAA, and wishes to use identifiable data for quality measurement under HIPAA's permitted uses for healthcare operations, should describe the benefits of this use and consider the potential risk for harms, then consider how it addresses each of the data stewardship attributes. In some areas, the user may believe it provides appropriate data stewardship, but in other cases may believe there are opportunities for improved transparency, stronger security controls, etc.*

Data Stewardship

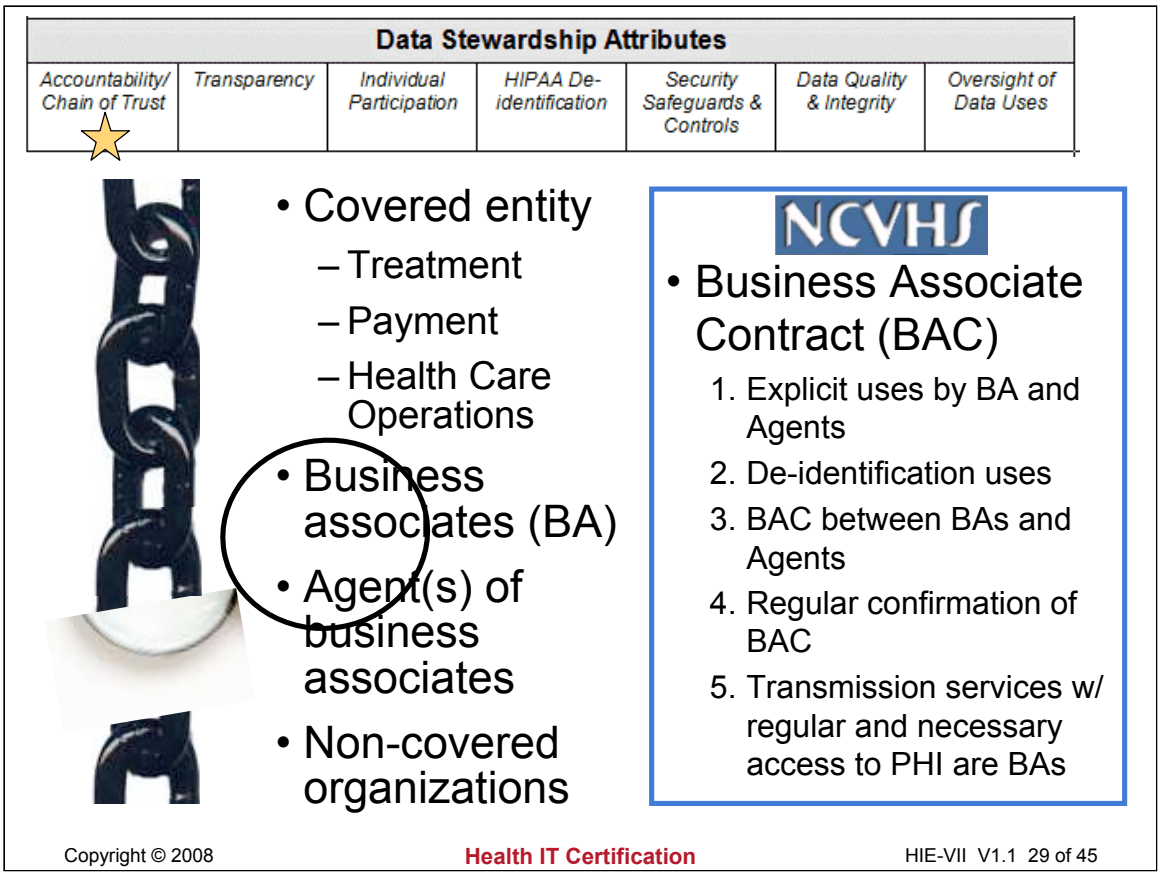
Part 4. Data Stewardship Solutions

The principles of health data stewardship, whether espoused through Fair Information Practices, HIPAA, or more recent public and private sector initiatives, provide important solutions for HIEs to consider adopting.

Content Part 4.

- Accountability/Chain of Trust
- Transparency
- Individual Participation
- HIPAA De-Identification
- Security Safeguards and Controls
- Data Quality and Integrity
- Oversight of Data Uses

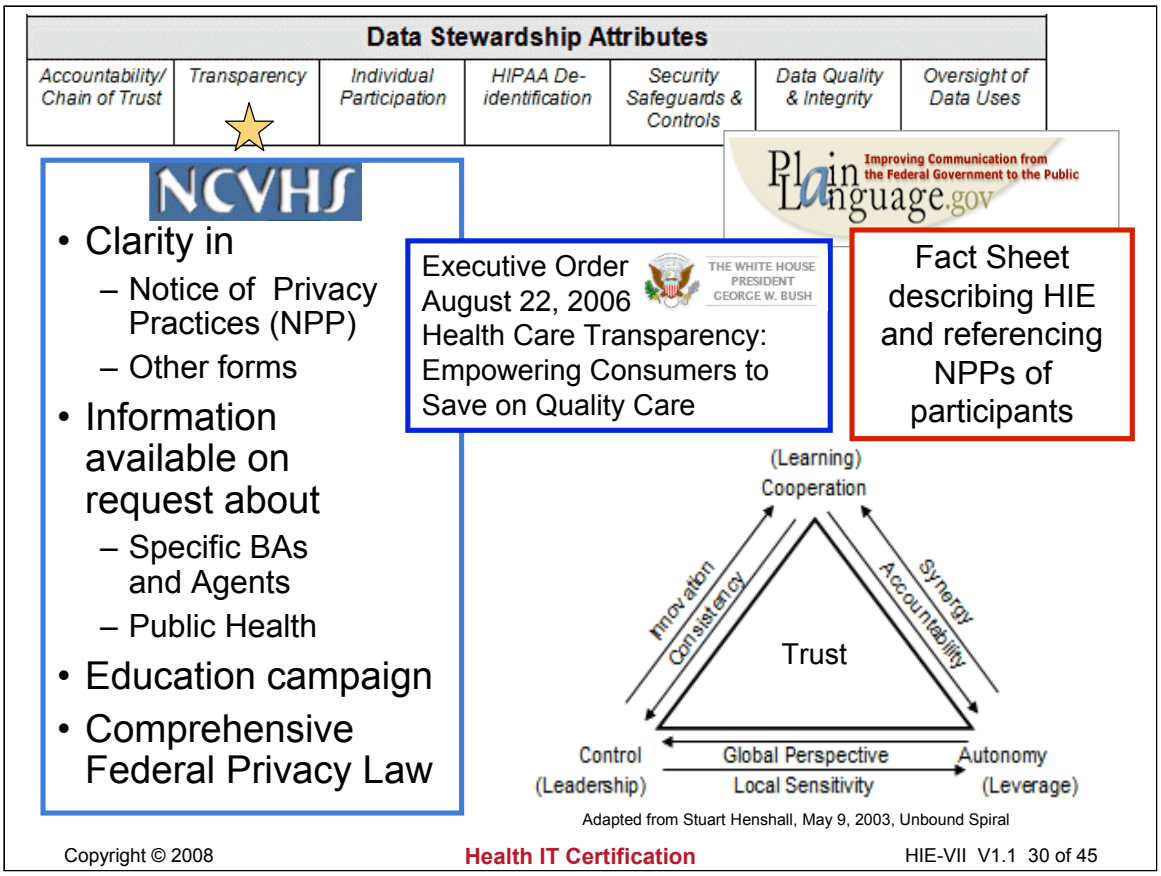
Topics covered in Part 4 identify a variety of approaches that have been proposed – both by the National Committee on Vital and Health Statistics (NCVHS) and other industry experts – to address health data stewardship.



Chain of trust is a concept frequently used in the security community to describe that a uniform level of security is applied at every "link" in the chain where information passes from one party to another. Security, then, is only as strong as the weakest link in the chain. Steve Fox, of Pepper Hamilton LLP, observes that "verification of uniformity at each link is necessary for optimal protection of transmitted data, and that a 'chain of trust' agreement is a proxy for actual physical confirmation before and after each and every transmittal." Chain of trust and its associated accountability are important concepts for all parties to an HIE.

Tasked with making "practically possible" recommendations that could be accomplished within 18 months, essentially not requiring regulatory change or new legislation, NCVHS recommended that the chain of trust between covered entities, their business associates, and agents of business associates be strengthened. This could be accomplished by CMS establishing precedence in its own business associate and other agreements, as well as others voluntarily requiring:

1. More explicit statements of uses of health data by the business associate, where today most business associate contracts (BAC) merely reference a vague statement of "permitted and required uses and disclosures of PHI."
2. That the BAC explicitly describe if PHI will be de-identified and what uses may be made of the de-identified data.
3. That the BAC include a specification of what agents the business associate will use and that a BAC must exist between the business associate and its agents. BACs today acknowledge that there may be agents of the business associate and that they must agree to the "same restrictions and conditions that apply to the business associate," but there is no requirement for identification of or contracts with these agents.
4. Regular review and confirmation that the BAC is up-to-date. This is recommended to ensure that changes necessitated by either party to a BAC get addressed in a timely manner and to provide the ability for the covered entity to identify all users of PHI to anyone upon request (see next slide).
5. Organizations that serve as conduits, but have regular and necessary access to PHIs be considered business associates – which would be an explicit directive that HIEs are business associates.



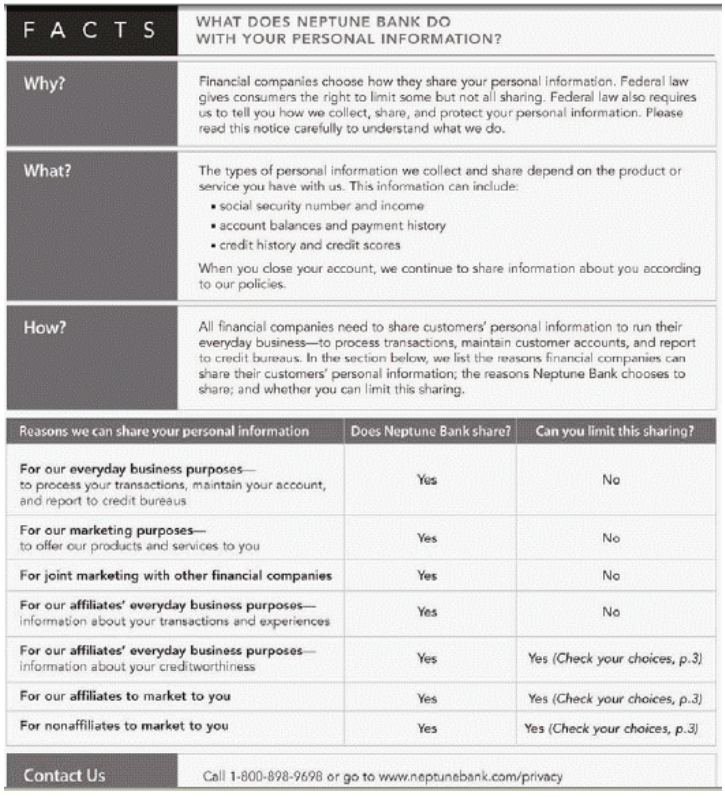
The federal government has been promoting transparency in many industries, and in health care, especially in pricing, quality, HIT standards, and options for quality and efficiency. In its hearings conducted to develop data stewardship recommendations, NCVHS also heard that trust requires transparency. Transparency is not the sole factor that garners trust, but is a critical component. A blog posting about trust requiring transparency observed that "humans gain trust by interacting and 'getting to know' people. Transparent technologies that make it easy to see what people and companies are up to (in a sense the opposite of firewalls – though not suggesting they not be used) are what help trust." President Reagan has been quoted as saying, "trust, but verify." Trust models often describe a tradeoff between control and autonomy, but another blogger on Unbound Spiral suggests a model that introduces a third point of cooperation, and still another blogger suggested replacing control, autonomy, and cooperation with leadership, leverage, and learning respectively, suggesting that when there is the context and discipline to ask questions, there is leadership, understanding, and leverage.

Whatever trust model a given HIE may ascribe to, the notion of trust through leadership, learning, and leverage are important to suggest that these have probably not been the hallmarks of HIPAA documents, which to date have largely been massive legal missals few read or can understand. NCVHS recommendations, therefore, call for transparency in the form of clear language for the notice of privacy practices and other administrative forms required to be used in compliance with HIPAA (and presumably extending to fact sheets and other documents describing HIEs to individuals), the ability to identify business associates and their agents to individuals upon request, and an educational campaign to dispel the uncertainty, fear, and doubt that seem to arise from the HIPAA Privacy and Security Rules. And while not immediately actionable, NCVHS reiterated call for comprehensive federal privacy law that would broaden the scope of HIPAA and address more Fair Information Practices tenets.

Could the healthcare industry do this?

- GLBA Privacy Notices:
  - Too lengthy
  - Dense in content
  - Complex language
  - Consumers neither read nor understood
- Response:
  - Multi-Agency Form Development Project

Evolution of a Prototype Financial Privacy Notice, Kleimann Communication Group, Inc., Feb. 28, 2006



F A C T S — **WHAT DOES NEPTUNE BANK DO WITH YOUR PERSONAL INFORMATION?**

Why? Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do.

What? The types of personal information we collect and share depend on the product or service you have with us. This information can include:

- social security number and income
- account balances and payment history
- credit history and credit scores

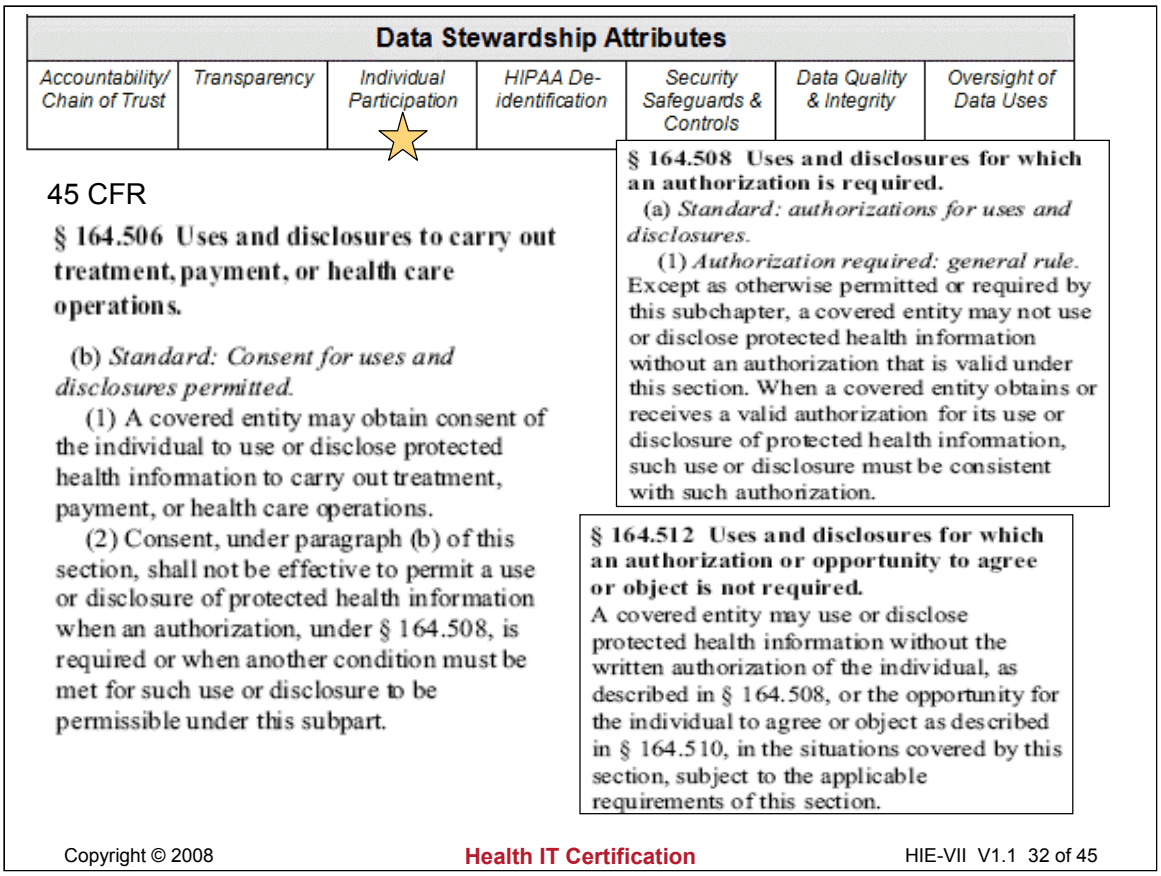
When you close your account, we continue to share information about you according to our policies.

How? All financial companies need to share customers' personal information to run their everyday business—to process transactions, maintain customer accounts, and report to credit bureaus. In the section below, we list the reasons financial companies can share their customers' personal information; the reasons Neptune Bank chooses to share; and whether you can limit this sharing.

Reasons we can share your personal information	Does Neptune Bank share?	Can you limit this sharing?
For our everyday business purposes— to process your transactions, maintain your account, and report to credit bureaus	Yes	No
For our marketing purposes— to offer our products and services to you	Yes	No
For joint marketing with other financial companies	Yes	No
For our affiliates' everyday business purposes— information about your transactions and experiences	Yes	No
For our affiliates' everyday business purposes— information about your creditworthiness	Yes	Yes *(Check your choices, p.3)*
For our affiliates to market to you	Yes	Yes *(Check your choices, p.3)*
For nonaffiliates to market to you	Yes	Yes *(Check your choices, p.3)*

Contact Us — Call 1-800-898-9698 or go to www.neptunebank.com/privacy

Clarifying language in the notice of privacy practices required by HIPAA would not be without precedence. In fact, the financial services sector, in reviewing compliance with the Gramm Leach Bliley Act (GLBA), observed that the privacy notices it requires were too long, dense in content, complex in language, and difficult to read and understand. This review resulted in a multi-agency project to develop a prototype financial privacy notice, such as illustrated here. A review of the privacy notices you get from your own financial institutions may reveal that some significant changes have already been made! Of course, the challenge still remains to get people to read the notice to begin with.



Certainly, whether it is a notice of privacy practices (NPP), an authorization form for uses and disclosures of PHI (with the valid elements required by HIPAA), or a consent for uses and disclosures to carry out TPO that may be required by state laws or individual covered entities or HIEs, there should be attention to clarity of language.

A number of states and covered entities are very concerned that wrongful disclosures will be made, even within the context of TPO. They believe that not requiring a consent or authorization for release of information for any purpose may be viewed as a lax practice. Certainly part of transparency is that individuals should have a greater “say” over use and disclosure of their personal health information. Hence a number of states and organizations have instituted statutes or policies (respectively) that would require consent or authorization for some or all uses and disclosures for TPO. In fact, many point to §164.506(b) as enabling such consent.

Interestingly, however, students of HIPAA may recall that §164.506(b) was modified after the initial dissemination of the Privacy Rule containing stricter consent requirements was found to be unworkable. Examples commonly cited at the time were the inability for an ill person to send a spouse or relative to the drug store to pick up a prescription without supplying written consent, or the inability for a pharmacy to call a provider about an illegible prescription, drug contraindication, or formulary issue without the consent of the patient. Of course, such consent could be facilitated by automated consent management functionality, but could still present problems when an unanticipated exchange of data is not addressed and confusion ensues.

What some states or organizations may not be clear about, as well, is that the consent as described in HIPAA is not considered to be a substitute for an authorization, when an authorization is required by HIPAA. HIEs that adopt a consent requirement should be clear about when consent is required and when authorization is required.

Authorization / Consent

- Authorization as used in the **HIPAA Privacy Rule** is the granting of formal written permission (using a valid authorization form) for uses and disclosures of protected health information (PHI) **for which an authorization is required** by the HIPAA Privacy Rule (45 CFR §164.508)
- Authorization as used in the **HIPAA Security Rule** refers to the policies and procedures for granting ***access*** to electronic PHI that are consistent with the applicable requirements of the Privacy Rule (45 CFR §164.308(3))

- **Consent** as used in the HIPAA Privacy Rule is the granting of permission to use or disclose PHI **for TPO**, but . . .
  - **Consent is not effective to permit a use or disclosure of PHI when an authorization is required or other condition must be met**
    (45 CFR §164.506(b)(2))
- **Informed consent** is the permission required for
  - A provider to administer care and/or treatment or perform surgery and/or other medical procedures, explaining benefits and risks and enabling an informed decision
  - A researcher to involve a human being as a subject in a research study covered by the Common Rule or HIPAA's Privacy Board requirements

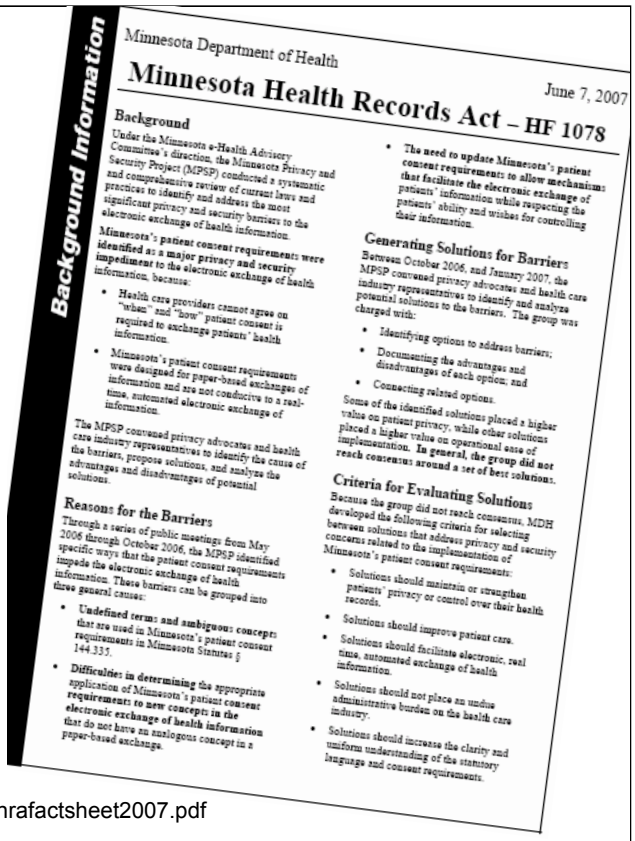
Consent and authorization are not only distinguished within HIPAA, but also in the broader context of informed consent for performing healthcare procedures that carry risk or that are required to conduct research. The AMA Office of the General Counsel (last updated May 7, 2007) provides a definition of informed consent as a communication that is both ethically and statutorily required by all states for specific medical interventions. Informed consent within the context of research is described by the Protection of Human Subjects regulation (a.k.a. the Common Rule) at 45 CFR §46.101, requiring an informed consent (or waiver by an Institutional Review Board) for "all research involving human subjects conducted, supported, or otherwise subject to regulation by any federal department or agency which takes appropriate administrative action to make the policy applicable to such research." HIPAA also requires either an authorization for research or a waiver by a Privacy Board where the research may not be subject to the Common Rule (45 CFR §164.512(i)).

At Issue

"Minnesota's patient consent requirements were identified as a major privacy and security impediment to the electronic exchange of health information"

Connecting for Health Common Framework

- Model Privacy Policies and Procedures for Health Information Exchange
- Notification and Consent When Using a Record Locator Service



Background Information

Minnesota Department of Health

June 7, 2007

Minnesota Health Records Act – HF 1078

Background

Under the Minnesota e-Health Advisory Committee's direction, the Minnesota Privacy and Security Project (MPSP) conducted a systematic and comprehensive review of current laws and practices to identify and address the most significant privacy and security barriers to the electronic exchange of health information.

Minnesota's patient consent requirements were identified as a major privacy and security impediment to the electronic exchange of health information, because:

- Health care providers cannot agree on "when" and "how" patient consent is required to exchange patients' health information.
- Minnesota's patient consent requirements were designed for paper-based exchanges of information and are not conducive to a real-time, automated electronic exchange of information.

The MPSP convened privacy advocates and health care industry representatives to identify the cause of the barriers, propose solutions, and analyze the advantages and disadvantages of potential solutions.

Reasons for the Barriers

Through a series of public meetings from May 2006 through October 2006, the MPSP identified specific ways that the patient consent requirements impede the electronic exchange of health information. These barriers can be grouped into three general causes:

- **Undefined terms and ambiguous concepts** that are used in Minnesota's patient consent requirements in Minnesota Statutes § 144.335.
- **Difficulties in determining** the appropriate application of Minnesota's patient consent **requirements to new concepts in the electronic exchange of health information** that do not have an analogous concept in a paper-based exchange.
- **The need to update Minnesota's patient consent requirements to allow mechanisms** that facilitate the electronic exchange of patients' information while respecting the patients' ability and wishes for controlling their information.

Generating Solutions for Barriers

Between October 2006, and January 2007, the MPSP convened privacy advocates and health care industry representatives to identify and analyze potential solutions to the barriers. The group was charged with:

- Identifying options to address barriers;
- Documenting the advantages and disadvantages of each option; and
- Connecting related options.

Some of the identified solutions placed a higher value on patient privacy, while other solutions placed a higher value on operational ease of implementation. **In general, the group did not reach consensus around a set of best solutions.**

Criteria for Evaluating Solutions

Because the group did not reach consensus, MDH developed the following criteria for selecting between solutions that address privacy and security concerns related to the implementation of Minnesota's patient consent requirements:

- Solutions should maintain or strengthen patients' privacy or control over their health records.
- Solutions should improve patient care.
- Solutions should facilitate electronic, real time, automated exchange of health information.
- Solutions should not place an undue administrative burden on the health care industry.
- Solutions should increase the clarity and uniform understanding of the statutory language and consent requirements.

http://www.health.state.mn.us/e-health/mpsp/hrafactsheet2007.pdf

Minnesota is an example of a state that for many years has had much stricter requirements for consent to exchange health information. It now recognizes that it is facing barriers to exchange of health information within an HIE environment as a result and issued a fact sheet describing how it would go about evaluating solutions to these issues.

Connecting for Health's Common Framework (www.connectingforhealth.org) provides model privacy policies and procedures for HIEs with respect to notification and consent when using a record locator service.

Opt-in / Opt-Out

- Only mention of "opportunity" within HIPAA is at

45 CFR
§ 164.502 Uses and disclosures of protected health information: general rules.

(1) *Permitted uses and disclosures.* A covered entity is permitted to use or disclose protected health information as follows:

(v) Pursuant to an agreement under, or as otherwise permitted by, § 164.510; →

- HIPAA also includes right to request restrictions of uses and disclosures (at 45 CFR §164.522)

45 CFR
§ 164.510 Uses and disclosures requiring an opportunity for the individual to agree or to object.

A covered entity may use or disclose protected health information, provided that the individual is informed in advance of the use or disclosure and has the opportunity to agree to or prohibit or restrict the use or disclosure, in accordance with the applicable requirements of this section. The covered entity may orally inform the individual of and obtain the individual's oral agreement or objection to a use or disclosure permitted by this section.

(a) *Standard: use and disclosure for facility directories.*

(b) *Standard: uses and disclosures for involvement in the individual's care and notification purposes.*

 Health IT Certification

Many HIEs are interested in obtaining consent – as permitted by HIPAA for TPO – and using the construct established in the Internet and e-commerce, that is, giving individuals the opportunity to opt in or opt out.

Interestingly, whether HIPAA actually addresses opt in or opt out is very much a matter of interpretation. Some suggest that HIPAA's "opportunity to agree or to object" is essentially opt in or opt out. Some also point to the right given individuals to request restrictions (which some suggest is an opportunity to opt out). Others, however, disagree with these interpretations – suggesting that neither the opportunity or restriction standards address consent, especially since opportunity to agree or object is only afforded relative to inclusion in facility directories and involvement in the individual's care and for notification purposes.

E-Consent for HIE?

Opt in: requires action or affirmation by an individual for inclusion; default is exclusion

Opt out: requires action or affirmation for exclusion; default is inclusion

- No legislation/regulation in U.S. specifically requires opt-in or opt-out for e-marketing, although . . .

  Federal Trade Commission (FTC) should exercise its authority to ensure that privacy policies on web sites collecting personal health information fully inform users of the uses that will be made and the organizations do not engage in misleading advertising or other deceptive trade practices

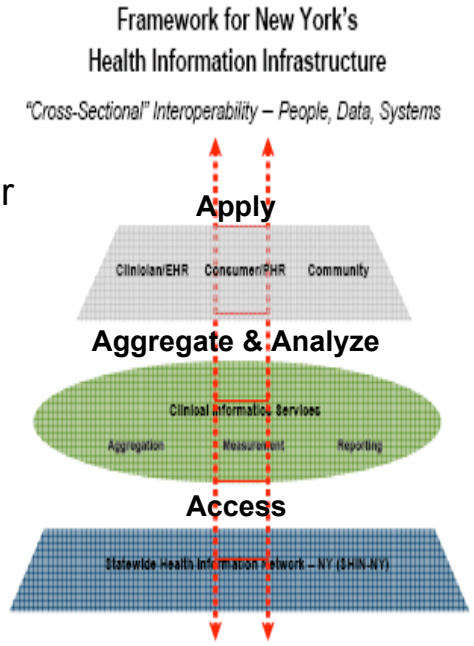
- UK Privacy and Electronic Communications Regulations 2003 specifically address opt in and opt out as applicable to organizations that send out marketing by telephone, fax, automated calling systems, email, messaging services (SMS, MMS), or any other form of electronic communication

More often than not, HIEs are looking to adopt a patient-consent model of affording opt in or opt out. The definitions provided here, commonly used within the e-commerce community, are important – not only to consider for adopting within an HIE, but also to recognize that these capabilities must be carefully planned, and may be mutually exclusive. Many HIEs discuss opt in and opt out as if both processes can exist and an individual decides whether to opt in or opt out. In reality, most HIEs that have adopted a patient-consent management process have done so using the opt out structure because it is technically easier to manage and less confusing to individuals. (Technical aspects of consent management, also suggesting a "quilted" approach through a "Consent Wizard," are described in the CPHIE Course VI: HIE Architectures.)

Because of the many organizations that may hold personal health information that are not subject to HIPAA, NCVHS has recommended that, in the absence of legislation making such organizations covered entities under HIPAA, that the Federal Trade Commission use its authority to ensure that privacy policies on web sites collecting personal health information fully inform users of the uses that will be made of their personal health information, and that the organizations do not engage in misleading advertising or other deceptive trade practices with respect to uses of personal health information. It is observed that many other countries have more stringent laws with respect to privacy and electronic communications.

New York Case Study

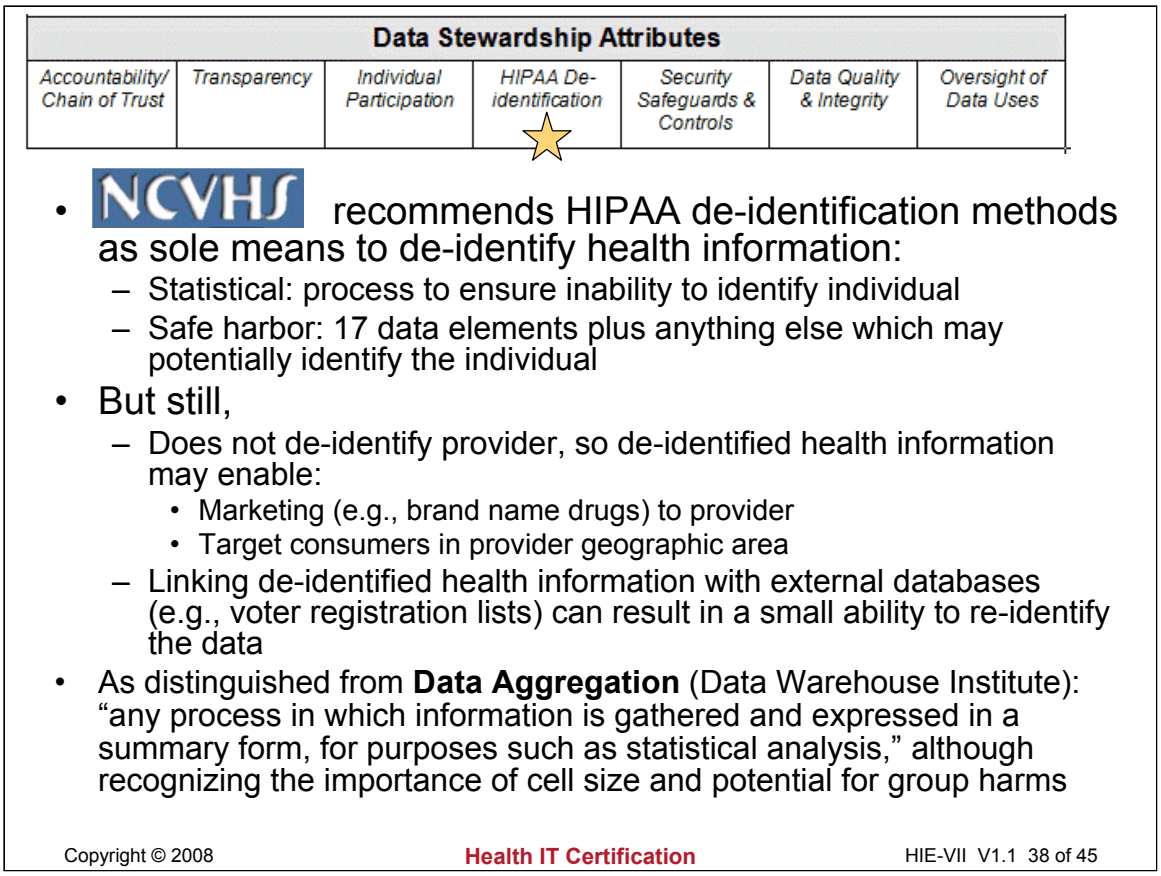
- **Up-Loading Data**
  - Same as other data storage and management arrangements
- Affirmative **Consent** for Uses of Health Information
  - Level 1: Expected by consumer
    - Treatment
    - Quality Improvement & Disease Management
  - Level 2: Less Expected
    - Research
    - Marketing
- Sensitive Health Information
- Standard Consent Form - Durability and Revocability
- Consumer Engagement and Access



A model for consent within an HIE is being developed for the RHIOs that participate in the Statewide Health Information Network for New York (SHIN-NY). New York recently issued draft Standardized Consumer Consent Policies and Procedures for RHIOs. Under these rules, each provider and payer organization participating in a RHIO must obtain an affirmative consent from the consumer that specifically references the RHIO prior to accessing her/his personal health information. However, healthcare providers may "upload" patient information to a RHIO without patient consent – as it is believed that healthcare providers routinely enter into data storage and management arrangements with EHR hosting vendors, outsourced data centers, and other technology companies today, and that uploading data to a RHIO is no different.

Within the SHIN-NY, permissible uses of health information fall into two categories: Level 1 uses are likely to be expected by the consumer and bring the consumer direct personal benefit. These have less stringent consent requirements. Any entity accessing information for Level 1 uses must have had a relationship with the individual who is the subject of the information and the information must pertain to such relationship. Level 2 uses are those less likely to be anticipated by the consumer or to bring direct personal benefit. Higher restrictions will be in place for Level 2 uses. Certain uses of information exchanged within the RHIO will be prohibited, including underwriting, discrimination, or others as designated by the State. Finally, RHIOs must have limitations on re-use and disclosure that provide protections identical to those provided under HIPAA. With respect to sensitive health information, NY permits a single consent except for information from designated substance abuse providers that are subject to current Federal Law. In addition to these requirements, SHIN-NY expects all RHIOs to use a State-approved consent form, that they be durable and revocable, and that RHIOs must comply with consumer education, engagement, and access standards.

On March 29, 2008, New York Governor David A. Paterson announced $105 million in grant awards to 19 leading community-based HIT projects, hoping to "begin to repair our fragmented delivery systems by making sure that accurate patient information is quickly available so that we can improve health care quality and efficiency." Lori M. Evans, Deputy Commissioner of the Office of HIT Transformation noted: "In order for EHRs and new quality tools to realize their potential, they must be interoperable. Achieving interoperability is as much a function of trust and collaboration among stakeholders and helping clinicians learn how to use information as the technology [itself]."



Many organizations de-identify health information in order to more freely use it. Although some would suggest that the value of de-identified information is minimal after all HIPAA identifiers have been removed, there are still concerns that the HIPAA requirements for de-identification may not be followed to the letter, and that even when followed, may still afford linking ability with information from other databases to re-identify the data. In making its data stewardship recommendations, NCVHS heard testimony concerning the ability to de-identify data and other forms of data-identity protection that may be applied to PHI. Although NCVHS intends to continue to study the issue further, it did recommend that the HIPAA definition of de-identification be the sole means to de-identify health information.

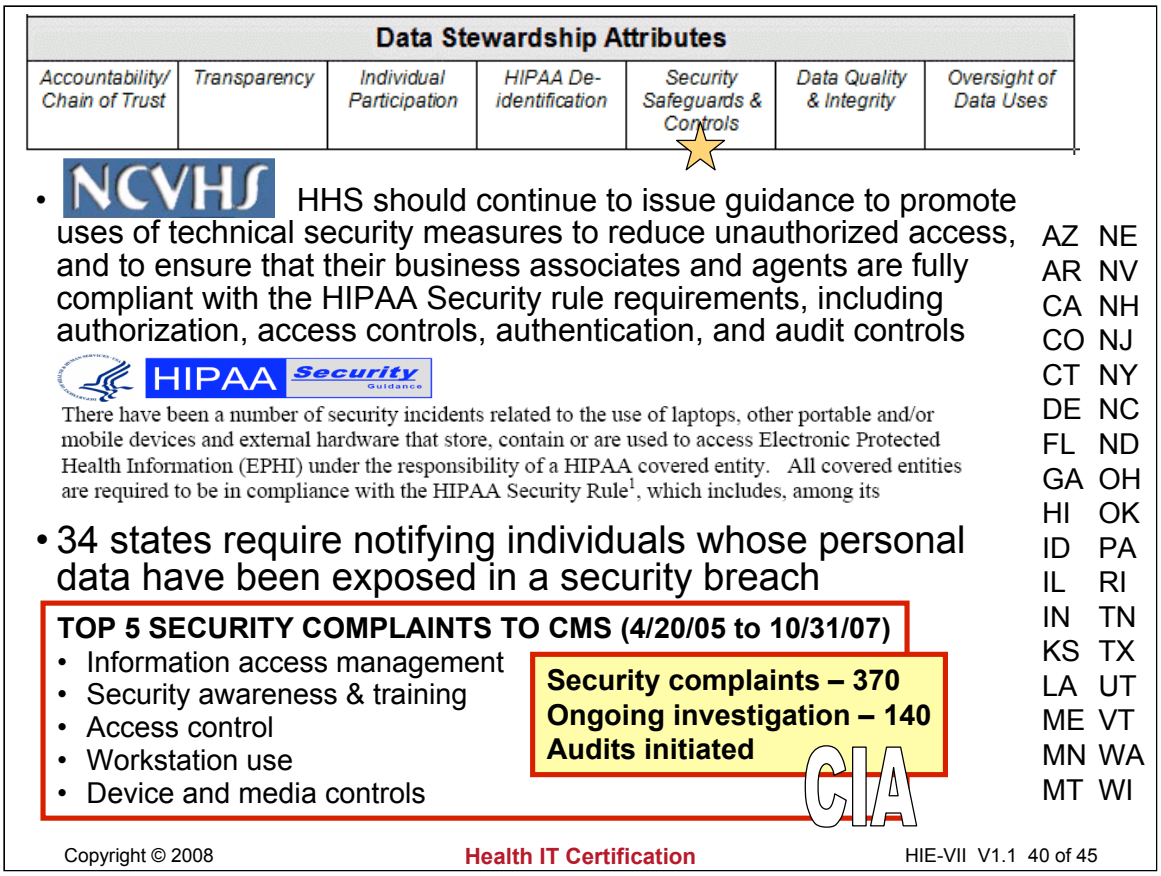
Data aggregation, by virtue of processing data, may also render data de-identifiable, although testifiers to NCVHS observed that cell size matters in such data aggregation. If there is only one person in the community who is over 100 years old, it is very difficult to render that person de-identified in most data aggregations. In addition, concerns about group harms from aggregated data were identified. Although not a function of HIT or HIE, group harm may be the cause of privacy concerns. For example, suggesting that people of a certain ethnicity may be more likely to acquire a certain disease can put the entire population of such persons at risk for discrimination – although many would also counter that without recognizing such a fact there would also be increased harm to the group from not taking appropriate precautions to lessen the chance for acquiring the disease.

Other Forms Retain Ability to Identify

These afford protection to PHI where use and disclosure of PHI is permitted but where extra precautions are desirable, such as for public health uses

- **Anonymization** (Health Information Technology Standards Panel): a process of "removal and aggregation requirements for data variables submitted to a biosurveillance information system, in accordance with the HIPAA Privacy Rule 45 CFR §164.519(b), 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** (Health Information Technology Standards Panel): "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."

Other forms of identity protection are being sought. Two that are commonly used within the public health community are anonymization and pseudonymization. Both have been recognized as standard processes by the Health Information Technology Standards Panel (HITSP). Both methods protect identity while still enabling re-identification by a trusted party. The public health community is using these processes to add protection, since disclosures to public health are permitted under HIPAA (45 CFR §164.512(b)).



Certainly a key element of health data stewardship not only relates to privacy-related protections, but security as well. Again, much of security is focused on ensuring confidentiality, although it must be remembered that security measures should also be directed to protecting the integrity of the data (i.e., keeping it from alteration) and the availability of the data (i.e., ensuring that is not destroyed and that it can be accessed in a timely manner as authorized and needed). This is commonly referred to as the CIA (confidentiality, integrity, and availability) of security. The Centers for Medicare and Medicaid Services (CMS), as the body designated within the Department of Health and Human Services (HHS) to administer the HIPAA Security Rule, has not received many security complaints, but recognizes that many security issues are not always observable to the general public. It also recognizes that security of data in general as well as health data in particular is increasingly making headlines – whether it is a stolen laptop, peeks at a movie star's health records, or erroneously faxing PHI to a bank. As a result, it has decided to initiate security audits. In addition, 34 states have stepped up their efforts to both draw attention to security matters and to provide a means for the public to mitigate potential harm from data security incidents through enacting data breach reporting requirements (Wernick, Alan, Data Theft and State Law: When Data Breaches Occur, 34 States Require Organizations to Speak Up, *Journal of AHIMA*, November-December 2006).

NCVHS' data stewardship recommendations recommend that CMS continue to draw attention and provide greater guidance to the industry on HIPAA security requirements.

eHealthConnecticut

- Treatment allowed uses are enforced through typical role-based access referencing functional role
- Policy table shows allowed use between sensitivity classes and functional role
- All clinical documents are published with subset of confidentiality codes, indicating type of data only, not status of consent at moment
- Consent acts are captured and managed as indicated

IHE BPPC

Consent Policy Table	Care Mgmt	Clinical Mgmt	Clinical Care	Privileged Care	Personal Care
Subject of care	Y	Y	Y	Y	Y
Subject of care agent	Y	Y	Y	Y	Y
Personal health professional	Y	Y	Y	Y	Y
Privileged health professional	Y	Y	Y	Y	Y
Health professional	Y	Y	Y	Special	Special
	Y	Y	Y	Special	N
	Y	Y	Special	N	N

HL7 CDA Document

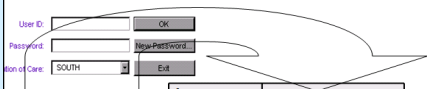
Content of Document

Privacy details

XDS Metadata

Role	Department	Applications	Screens/ Data Elements/ Other Conditions	Role Privileges							Context Privileges
				R	W	P	S	BTG	T	A	D	Location/ Time
Chaplain	*Pastoral Care*	*Directory*	*-Patient name -Room-bed -Religion*	X								*Chaplain office/Any time*
Clerk - Billing	*Patient Accounting*	*Billing System*	*-Demographics -Insurance -Charges -Dx/Proc Codes*	X	X	X						*Patient Accounting Department/ Day shift*
Clerk - Coding	*Medical Records*	*Encoder*	*-Entire medical records as assigned*	X	X							*HIM Department Day shift*

* Read/View, Write &Correct, Print, Sign, Break-The-Glass, Transmit, System Administration, Delete

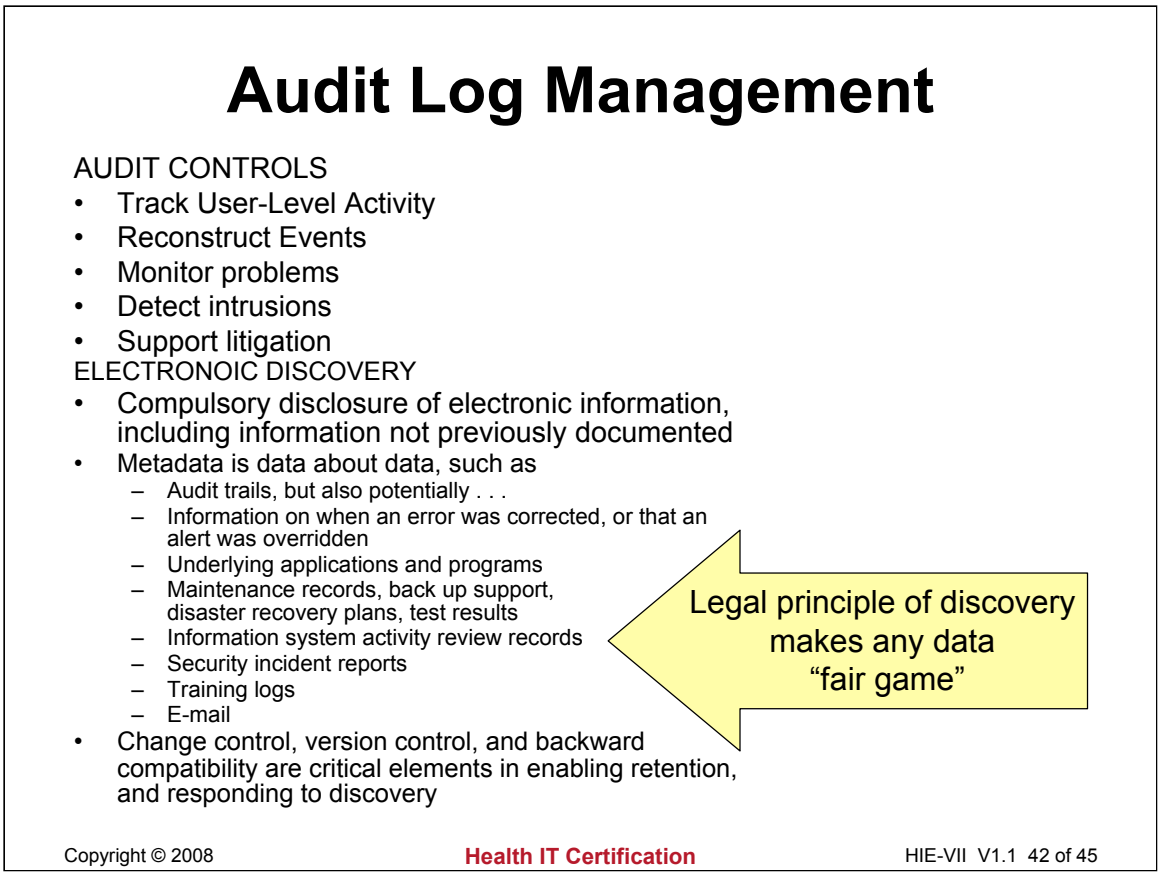


Minimum Necessary
Classes of Users
Categories of PHI
Conditions of Access

Access Control	Assigns Privileges
User-based	To each user
Role-based	To classes of users to categories of PHI
Context-based	Based on conditions

eHealthConnecticut is an organization preparing the state of Connecticut for HIE by establishing a collaboration forum, educating stakeholders, adopting standards, certifying technology providers, and producing annual statewide progress reports. It is enabling e-prescribing for its Medicaid patients and hospital and physician sharing of laboratory and medication information. It is also implementing a statewide database of clinical quality and cost information for public reporting of provider performance, having applied for recognition by the federal government as a Chartered Value Exchange. In part, this data aggregation project enables an incentive program for providers to spur adoption of HIT (www.ehealthconnecticut.org).

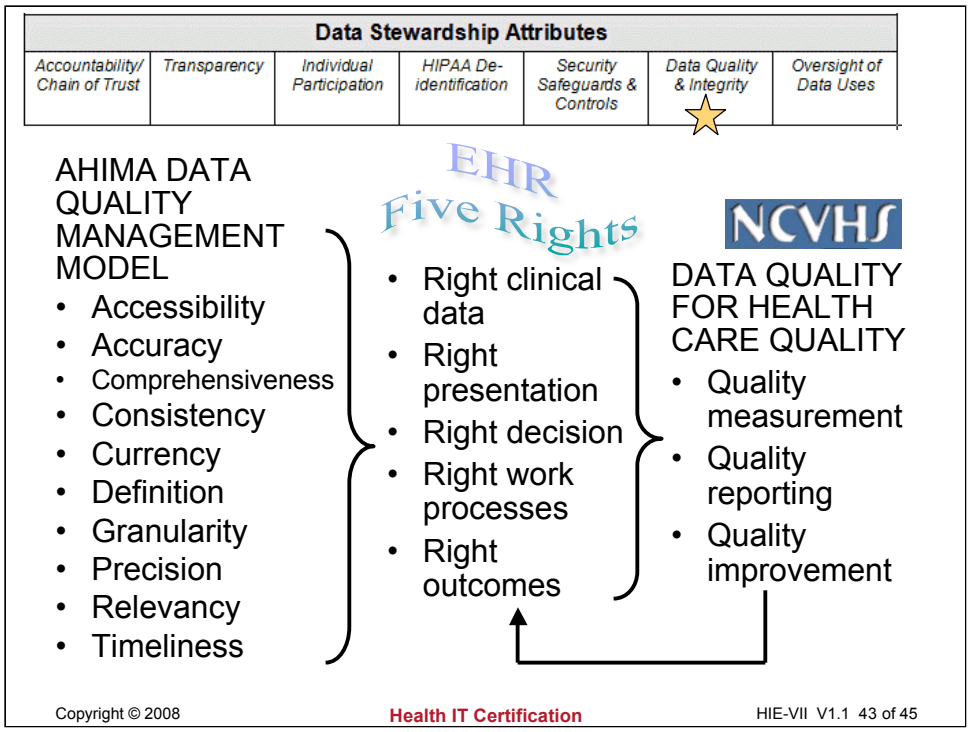
eHealthConnecticut was also cited in a presentation by John Moehrke and Lori Fourquet, conducted at the IHE Educational Workshop in 2007, for its successful use of a security consent matrix. Integrating the Healthcare Enterprise (IHE, www.ihe.net) is a global initiative that brings together healthcare information technology stakeholders to implement standards for communicating patient information efficiently throughout and among healthcare enterprises by developing a framework for interoperability. IHE is not a standards development organization, but develops profiles for best practices in adopting standards. It has developed a Basic Patient Privacy Consent (BPPC) profile to record patient privacy consents and to mark documents with patient privacy consent information when these documents are published in accordance with the Cross-Enterprise Document Sharing (XDS) integration profile, which is based on Health Level Seven (HL7) Clinical Document Architecture (CDA). The intent is to enable an HIE to develop a set of privacy policies and implement them with access control mechanisms supported by their HIT and electronic health record (EHR) systems. Patients can be made aware of the privacy policies and have an opportunity to selectively control access to their health information.



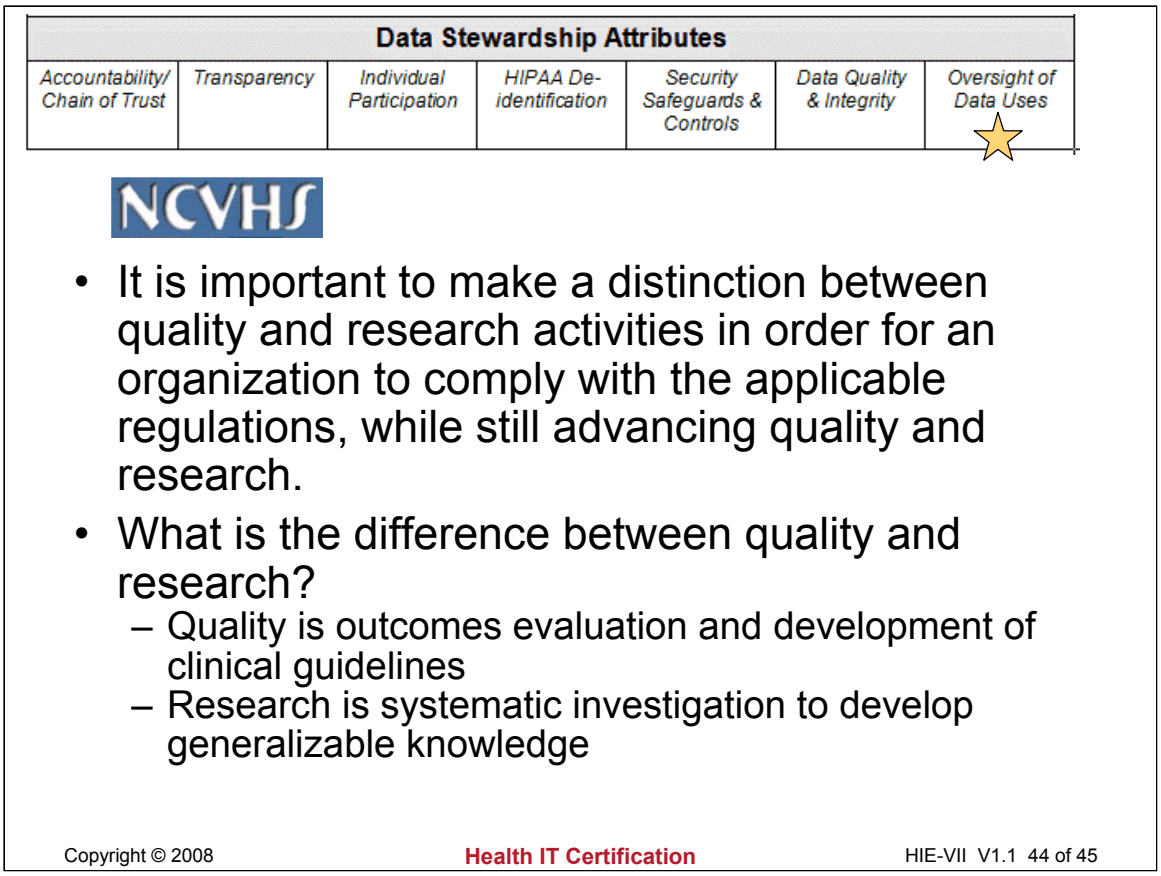
Audit controls are also security controls that support individual participation. Audit logs can be used to identify who and when any action was taken on electronic data, and are critical in:

- Tracking User-Level Activity by capturing and recording access information for all devices, applications, and servers to ensure that individuals are held accountable for their actions
- Reconstructing Events leading to a potential incident following a network event
- Monitoring Problems, providing early warnings of anomalies and threats, providing time to remediate issues prior to a system failure, improving system availability
- Detecting intrusions: Logs from devices such as the IDS, firewalls, and externally facing web servers provide early warnings of a breach or performance issue
- Supporting litigation: The ability to provide a detailed accounting of an event will enhance the ability to demonstrate a violation of IT policies. This is useful when considering response options related to internal sanctions; and detailed records will facilitate legal proceedings. (It must be remembered, however, that the HIPAA Privacy Rule's requirement for accounting for disclosures does not require that all audit log data be disclosed to the individual. This is because covered entities are only required to account for disclosures *other than* disclosures to carry out treatment, payment, and healthcare operations; to provide individuals protected health information about themselves; incident to a use or disclosure otherwise permitted or required; pursuant to an authorization; for the facility's directory or to persons involved in the individual's care or other notification purposes; for national security; to correctional institutions or law enforcement officials as provided for in the Rule; and as part of a limited data set.)

Audit logs, however, have increased in importance since amendments to the Federal Rules of Civil Procedure for electronic discovery went into effect on December 1, 2006 (and several states have also adopted such rules or are planning to follow suit). Often referred to as "e-discovery" rules, these rules make all electronically stored information subject to being called into court in the face of litigation or pending litigation. For the healthcare industry, this means significantly more information than has traditionally been kept between the pages of a medical record folder. "Metadata," or data about data, may include virtually anything.



Because many HIEs are supported by or interested in supporting quality measurement, reporting, and improvement, the data they maintain not only must be privacy protected and secured, but must be meaningful. NCVHS included recommendations on data quality in its data stewardship guidance to ONC, including that precision, accuracy, reliability, completeness, and meaning of data used for quality measurements, reporting, and improvement as well as other uses of health data should be assured. NCVHS has also made previous recommendations for adoption of standard vocabularies (see also CPHIE Course VI: HIE Architectures).



For many uses of health data relating to quality and research activities, there is a clear distinction. However, several testifiers at hearings held by the NCVHS in its deliberations about health data stewardship guidance indicated that there are times when the distinction between quality and research activities is not clear. NCVHS offered an initial set of recommendations – that quality measurement, reporting, and improvement remain within the scope of healthcare operations when conducted by covered entities or their business associates and under the accountability and data stewardship principles inherent in HIPAA. Although it will be holding additional hearings to further study this issue, NCVHS observed that there may be a desire for a wider role for individuals in deciding whether to permit their health data to be used for quality activities, and there needs to be appropriate shepherding of quality improvement findings into research when applicable. The Hastings Center report, referenced earlier, also describes a joint quality-research oversight process that has been used successfully in certain organizations. Each organization and HIE needs to study uses and users of the health data exchanged to determine appropriate strategies.

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.

 Health IT Certification

This course has studied the landscape of data stewardship, drawing lessons from other industries, emphasizing the importance of HIPAA, but also recognizing that in the new world of HIT and HIE, there are new concerns and potential new strategies that are needed.

Use the quiz in the handout materials to test your understanding of the content just presented. Answers are provided following the quiz.