



NHII Privacy Architecture

Kathleen Connor
Fox Systems
September 2006

What is Happening

Interoperability for Safe Exchange of Healthcare Information

- Regional Health Information Organizations (RHIO's) are gathering steam throughout the health care industry
- These collaborations seek to share pertinent information within a geographical area to enhance administration and provision of health care services. This presentation will explore the technology and safe guards each organization should be aware of as the drive to participate in a RHIO grows
- State Medicaid agencies have the opportunity to shape the development of these groups in their area and leverage the information exchanged in the administration of the state's program.

Key HIT Legislation

Current strong contenders with important privacy implications:

- Senate S. 1418 *Wired for Health Care Quality Act*
 - Sponsored by Sens. Michael Enzi, R-Wyo.; Edward Kennedy, D-Mass.; Bill Frist, R-Tenn.; and Hillary Clinton, D-N.Y.
 - <http://www.cbo.gov/ftpdocs/65xx/doc6585/s1418.pdf>
- House H.R.4157 *Health Information Technology Promotion Act of 2005*
 - Sponsored by Rep. Nancy Johnson

Senate 1418 Privacy Provisions

- Section 4: Ensuring Privacy and Security
- Would not affect scope, substance or applicability of
 1. HIPAA
 2. Sections 1171 – 1179 of the Social Security Act inclusive of 1175, basis for 42 CFR Part 2
 3. Any regulation issued pursuant to these sections

HR 4157 Privacy Provisions

- Section 4 Uniform Health Information Laws and Regulations: HHS to compare State and Federal security and confidentiality laws to determine
 - Degree to which state laws vary among states and with the federal laws
 - How any variance may adversely impact security and confidentiality of individually identifiable health information and electronic exchange among states, federal government and private entities
 - Pros and cons of current laws for purposes of protecting individually identifiable health information vs. timely & efficient exchanges of health information to improve quality of care and availability of health information for medical decisions
 - HHS must report to Congress a determination as to whether state and federal security and confidentiality standards should conform to create a single set of national standards, and what those should be.

EHR & PHR Privacy Issues

- Once a provider is given access to PHR data, that data is open to HIPAA disclosures
- Payers are accessing and using payment data for non-payment purposes (e.g., health analytics to profile enrollee's risk) by creating pseudo clinical data
- Payers are affiliating with banks, which assert exemption from HIPAA, to send 835s and handle HSA claims
- Employers are requesting voluntary participation in care management programs for reduced premiums – If employees Opt-in, then employer has access to PHI

My Privacy Nightmares

BlueCross, Cerner Plan Tennessee EMR Database

May 26, 2005



[BlueCross BlueShield of Tennessee](#) and [Cerner](#) have collaborated to create a database of patient medical records that eventually might contain all of the state's health records, [MSNBC/Nashville Business Journal](#) reports. The deal is intended to help reduce costs and improve care.

The database will eliminate the need for physicians to rerun certain tests, and it will allow them to find out which medication a patient is taking, [MSNBC/Nashville Business Journal](#) reports.

If the state approves the database, it will be launched this summer and cover BlueCross' 700,000 [TennCare](#) beneficiaries. By the end of the year, the database could be available to the remaining TennCare managed care organizations, and next year it could be open to all commercial insurance patients. The database will be the largest of its kind nationwide, covering the insurer's 2.8 million commercial and Medicaid beneficiaries in the state, [MSNBC/Nashville Business Journal](#) reports.

BlueCross will pay Cerner a per-member, per-month fee to host the database. The information will be compiled from the insurer's records, public health department data and other sources, [MSNBC/Nashville Business Journal](#) reports.

Scott Vogel, president of the Healthcare Information and Management Systems Society's Tennessee chapter, said the deal could dominate the market in the state, but other stakeholders could get involved if their databases are interoperable (Moore, [MSNBC/Nashville Business Journal](#), 5/22).

All TennCare Beneficiaries To Get Electronic Records

July 07, 2005



Shared Health, a subsidiary of [BlueCross BlueShield of Tennessee](#), on Wednesday signed a contract to create electronic health records for one million TennCare beneficiaries, the [Tennessean](#) reports. The project, which is called Community Connection, is expected to be the largest of its kind in the country (Pack, [Tennessean](#), 7/7).

TennCare beneficiaries' medical records will be available via a secure Web site, and any physician in the state who accepts TennCare patients will be able to access the records. About 700,000 TennCare enrollees currently have EHRs, and another 300,000 will have EHRs by the end of the year.

The project was tested in four Tennessee communities prior to Shared Health's decision to implement it statewide. Bill Steverson, BlueCross BlueShield's public affairs director, said physicians who tested the program were enthusiastic about it, [Government Health IT](#) reports (Ferris, [Government Health IT](#), 7/6).

BlueCross BlueShield officials estimate that the EHRs will save \$3 to \$4 for every dollar invested in the Community Connection project ([Government Health IT](#), 7/6).

AHA Releases Advisory on Concerns Over JCAHO Data Mining

November 03, 2005



The [American Hospital Association](#) sent an advisory brief to its members about its concerns over the [Joint Commission on Accreditation of Healthcare Organizations](#) selling data to third parties that was collected for accreditation purposes, [Modern Healthcare](#) reports.

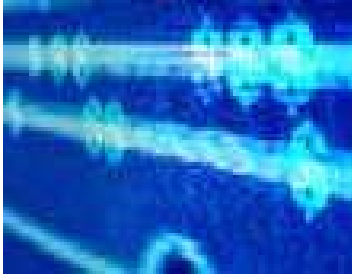
JCAHO in May contracted with the [Blue Cross and Blue Shield Association](#) to provide hospital-specific data analyses to more than 12 BCBS plans in several states. JCAHO also demanded that hospitals beginning in 2006 provide patient-specific data to the organization's ORYX quality-improvement program (Conn, [Modern Healthcare](#), 11/2).

The AHA in its advisory said JCAHO's plan to collect data for use unrelated to accreditation raises HIPAA compliance issues and that the AHA would seek guidance from HHS on privacy issues, [AHA News](#) reports. The AHA also said JCAHO's new data-mining program is a duplication of the Hospital Quality Alliance's program and would cause a conflict of interest ([AHA News](#), 11/2).

JCAHO officials were not immediately available for comment, [Modern Healthcare](#) reports ([Modern Healthcare](#), 11/2).

Visa, Blue Cross and Blue Shield Association To Offer Health Debit Cards

November 22, 2005



[Visa](#) and the [Blue Cross and Blue Shield Association](#) on Monday announced they are partnering to offer a co-branded debit card for health-related costs, the [San Francisco Chronicle](#) reports.

According to the *Chronicle*, the venture is "part of a shift in health care to get consumers to assume a greater decision-making and financial role in their medical care."

Only members with flexible savings accounts or health savings accounts, which are part of high-deductible plans, can use the debit card. Blue Cross and Blue Shield companies in four states - Idaho, Louisiana, New Jersey and South Carolina - so far have agreed to offer the debit card to members.

The Visa card contains only account information, and a Visa spokesperson said the co-branded cards have the same protections as credit cards.

Other health insurers also are partnering with credit card companies. [UnitedHealth Group](#), which created its own bank, last year began offering members [MasterCard](#) debit cards that contain information about a member's coverage and co-payments. UnitedHealth Group also is piloting a card that includes a member's medical records information, the *Chronicle* reports (Colliver, *San Francisco Chronicle*, 11/22).

Empire Blue Cross To Offer American Express Health Care Payment Card

December 01, 2005



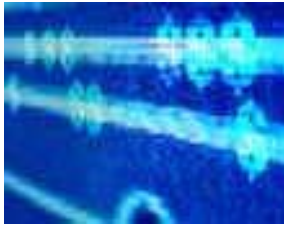
[Empire Blue Cross](#) in New York state will offer its Empire Total Blue members an [American Express](#) HealthPay Plus payment card, which will permit integrated claims processing and easier access to health savings account funds, the Albany [Business Review](#) reports.

Approved members will be able to use the HealthPay Plus payment card at participating provider offices to pay deductibles or other expenses. Empire and American Express will process the remaining payment and claims. Empire will begin distributing the cards in early 2006, the *Business Review* reports (*Albany Business Review*, 11/30).

[Visa](#) and the [Blue Cross and Blue Shield Association](#) last week announced they are partnering to offer a co-branded debit card for health-related costs, and [UnitedHealth Group](#), which created its own bank, last year began offering members [MasterCard](#) debit cards that contain information about a member's coverage and copayments. UnitedHealth Group also is piloting a card that includes a member's medical record information ([iHealthBeat](#), 11/22).

BCBS To Create Bank for Health Savings Accounts

December 05, 2005



The [Blue Cross and Blue Shield Association](#) plans to charter a bank to manage enrollees' health savings accounts directly, the *Wall Street Journal* reports. The move follows the creation in November of a jointly branded debit card with [Visa](#) for accounts linked to health plans (Fuhrmans, *Wall Street Journal*, 12/5).

The association, which is expected to announce the move on Monday, is planning to begin bank operations by summer, pending regulatory approval (Vrana, [Los Angeles Times](#), 12/5). Blue Healthcare Bank is intended to simplify the administration of HSAs and similar plans offered by Blue Cross insurers throughout the U.S., according to Scott Serota, president and CEO of the association (*USA Today*, 12/5). Until now, BCBS insurers have partnered with established banks to handle the savings accounts that members use to pay their out-of-

pocket expenses.

BCBS executives noted that Blue Healthcare Bank, which currently has the support of 31 of 39 locally operated BCBS companies, could help decrease transaction costs for the health plans. [UnitedHealth Group](#) is the only other major health insurer that has formed its own bank (*Wall Street Journal*, 12/5).

Blue Healthcare Bank will offer debit cards for health care costs and credit lines if enrollees' costs exceed their savings. It will not provide mortgages or other types of commercial lending. Glenn Melnick, health care financing expert with [Rand](#), said that the move is logical, adding, "With the growth of HSAs, there should be \$10 [billion] to \$20 billion in those accounts by 2010, and the insurers are hoping to hold on to that money. It's a growing market" (*Los Angeles Times*, 12/5).

Serota said, "We're not getting into the banking business per se. This is about the sole function to support health care transactions, a business we know a lot about." However, some analysts said that health insurers lack the "critical mass" and "expertise" to compete with established banks, the *Journal* reports (*Wall Street Journal*, 12/5).

Payer Health Analytics

Parallax *i*® is a fully integrated, web-based **total health and productivity decision support tool allowing employers to track and evaluate the effectiveness of programs that impact group health results**. Parallax *i* is designed to capture and compare information derived from multiple data sources for integrated health and productivity reporting and analysis. Data querying and access is straightforward, allowing you to quickly understand cost and utilization patterns and assess opportunities for cost savings. Because Parallax *i* integrates individual program attributes into one central data repository, experience can be viewed across the entire spectrum of the health care delivery system. Performance of each program can be viewed individually and holistically, assessing how employees access or utilize benefits across various offerings. By understanding what is really driving specific experience, you can understand how risks relate to one another and implement the right intervention programs and best practices. Employers have used Parallax *i* to:

- quantify the changes in plan costs and identify the drivers of expense;
- determine the quality of care being provided to employees;
- identify potential areas of excess care or unfavorable pricing;
- assess the performance of their carriers and networks;
- evaluate the need for, or performance of, specialty and carve-out benefit programs;
- structure future plan designs consistent with organizational strategy;
- forecast costs and establish budgets for future periods;
- present to senior management benefit plan results and rationale for change;
- prepare mandated financial reporting;
- evaluate the diagnostic causes of health-related claims, occupational injuries, and lost time;
- identify the interventions expected to have the most impact on a specific employee population, and;

detect the individuals most likely to become high cost claimants in the near future, and facilitate early case management.

<http://www.ingenix.com/content/attachments/ParallaxiBrochure.pdf>

House Panel Passes Bill To Require Electronic Health Records for FEHBP Members

The House Government Reform [Subcommittee on the Federal Workforce and Agency Organization](#) on Wednesday passed a bill (HR 4859) that would authorize the [Office of Personnel Management](#) to require health insurers to establish two forms of electronic health records for the [Federal Employee Health Benefits](#)

[Program](#), *CongressDaily* reports.

The first form of EHRs would include information currently tracked by health insurers -- such as hospital and physician visits, claims information and prescription drug records -- and FEHBP members could access them within four years of passage of the legislation. The second form of EHR would include personal health information -- such as medical history, symptoms and diet - - and FEHBP members would administer them.

The bill, co-sponsored by subcommittee Chair Jon Porter (R-Nev.) and Rep. William Clay (D-Mo.), would require health insurers to comply with medical privacy rules established under the 1996 Health Insurance Portability and Accountability Act in the administration of the EHRs (*CongressDaily*, 9/14). Under the legislation, health insurers would cover the cost of the establishment of the EHRs and could not pass the cost to FEHBP members through higher premiums. The bill also would require health insurers to provide grants to physicians to implement EHRs through a new trust fund established with private donations.

Some Concerns

[America's Health Insurance Plans](#) has asked Porter to delay the legislation until health insurers develop standards for EHRs and the systems used to store and transmit them. AHIP President Karen Ignagni said that the bill would lead to the establishment of a number of different EHR "models and make standardization and interoperability very difficult to achieve." Rep. Danny Davis (D-Ill.) said that the legislation should include more privacy protections, such as a requirement that health insurers inform FEHBP members in the event their EHRs are unlawfully obtained (Wayne, CQ *Today*, 9/13).

Medicaid Confidentiality Standards are on the “HIT” List

- **FEDERAL MEDICAID CONFIDENTIALITY STANDARDS:**
- **The federal Medicaid confidential data standard is established by §1902(a)(7) of the Social Security Act (42 USC §1396a(a)(7)). The law requires that a “State plan for medical assistance must: (7) provide safeguards which restrict the use or disclosure of information concerning applicants and recipients to purposes directly connected with the administration of the plan.” This statutory requirement is implemented in regulations at 42 CFR §431.300 et seq.. 42 CFR §431.302 defines Medicaid program administration to include:**
 - **(A) Establishing Eligibility;**
 - **(B) Determining the amount of Medical Assistance;**
 - **(C) Providing services for recipients; and**
 - **(D) Conducting or assisting an investigation, prosecution, or civil or criminal proceeding related to the administration of the plan.**

42 CFR is Considered an Obstruction and Obsolete

- Generally only permits disclosures and use of patient records as permitted by regulation. (§ 2.13) Limits "any" disclosure made under the regulations to "information which is necessary to carry out the purpose of the disclosure."
- Requires minimum necessary disclosures (§ 2.13)
- Permits disclosure without consent for medical emergencies (§ 2.51)
- Must document disclosure in record (*breaking the glass provision*)
- Permits disclosures with written consent (§2.33)
- Consent must contain specific elements (§ 2..31)
- Most importantly, perhaps, is that it allows the individual to specify the name or title of the individual *or the organization* to which the disclosure is to be made.
- Must specify when consent expires –can be a date, event or condition—but can last no longer than reasonably necessary to serve the purpose for which it is given
- Regulation includes sample consent
- Consent can contain additional elements
- Each disclosure made with the patient's written consent must be accompanied by a written statement that info. is protected by 42 CFR part 2 and that recipient is prohibited from making further disclosure unless further disclosure is expressly permitted by the written consent of the subject of the info. (§ 2.32)
- Regulation specifies exact required language (§ 2.32)

HIV-AIDs

- **MEDICAID HIV CONFIDENTIALITY RESTRICTIONS:**
- **The Health Care Financing Administration (HCFA) also has issued a State Operations Letter #91-32, regarding the confidentiality and release of Medicaid data concerning persons with AIDS.**
- ***The letter establishes that sharing of claims data regarding AIDS patients with other state agencies is a violation of federal privacy safeguards.*** The operations letter notes that while it is a legitimate public health concern to engage in disease prevalence surveillance, federal law and regulations permit disclosure of information concerning Medicaid applicants or recipients, including AIDS data, only for purposes directly related to State Medicaid plan administration.
- **Accordingly, state health departments seeking recipient information for reasons unrelated to administration of the Medicaid program must rely on provider compliance with State reporting requirements. Medicaid data cannot be released for such purposes, including accurate counting of AIDS cases.** The HCFA suggests that as an alternative to the release of patient identifying information, Medicaid agencies may provide summary data, including recipient counts and expenditures

Privacy issues with EHRs and PHRs

- Only privacy requirements for RHIOs and their non-HIPAA related participants are by business associate agreements – e.g., providers/payers may access PHI for patients/persons who are not under their care/coverage
- Support for consents required by 42 CFR and other more stringent state laws are deemed infeasible, burdensome, obstacles to care management, barriers to care coordination, and impediments to measuring quality
- Clear need for privacy architecture like other countries

Privacy and HIT Standards

- Protecting privacy and confidentiality of personally identifiable health data is *not* a technical issue – it's a policy issue
- Other countries with NHIs have far more stringent requirements around patient's control of disclosure – e.g., Canada, UK, AU, and NL
- Standards have an impact on supporting privacy – e.g., EHRs Functional Model support of 42 CFR and state specific privacy law may reduce the need for uniformity

HL7 International Privacy Architecture

- Recent meeting with 30 international experts on privacy policies and supportive technologies
- CA, NL, DE, UK, AU, US
- Compared National HIE architectures, delivery systems, and privacy policies
- *Complex Consent Policies are being supported*
 - *At the record, encounter, or data element level*
 - *Can mask provider, diagnosis, condition, service, demographics*
 - *Patient can authorize access to masked information*

Supporting Patient Consent

- Policy, Standards, and Technical Support for Patient consent to collect, use, and disclose PHI
 - Opt-out
 - Total
 - Conditional
 - Opt-in
 - Total
 - Conditional
- Within Nodes (Regional Hubs, Sub-networks)
 - Share generally agreed upon privacy policies
- Among Nodes on NHIN
- Role Based Access
- Standards for electronic consents, shared secrets, privacy policies

Opt-out

- Actively refusing to authorize an entity to collect, use, or disclose PHI
- Actively refusing to authorize a requesting entity to access, use or *re-disclose* PHI
- May opt-out at the record or data element level
- Opt-out may be
 - Total
 - Conditional

Opt-out

■ ***Total Opt-out***

- Off Node
- Locked/Masked on Node

■ ***Conditional Opt-out***

- PHI is Masked / Locked
- Some collection, use, disclosure permitted
 - Pre-determined: By User, Role, Context Based Access
 - Ad-Hoc: By Shared Secret

■ ***Implied Consent = not Opting out***

■ ***Deemed Consent***

- Public health or legal requirements may override Opt-out

Opt-out

Non-action = implied consent

Encounter
Provider
DX
PX
HX
RX

Encounter
Provider
DX
PX
x Sensitive Lab

May not have a choice where there is a public health issue

Requires active dissent by record / data element

x	Sensitive Encounter
	Sensitive Provider
	Sensitive DX
	Sensitive PX
	Sensitive RX

Conditional Dissent by Data Element

Problem List
DX
x Sensitive DX
x Sensitive DX
x Sensitive PX
DX
PX
DX

Opt-in

- Actively authorizing an entity to collect, use, or disclose PHI
- Actively authorizing a requesting entity to access, use, or *re-disclose* PHI
- May Opt-in at the record or data element level
- Opt-in may be
 - Total
 - Conditional

Opt-in

Conditional Opt-in

- PHI is Masked / Locked
 - Some collection, use, disclosure permitted
 - Pre-determined: By User, Role, Context Based Access
 - Ad-Hoc: By Shared Secret
- ***Implied Dissent = not Opting in***
- ***Deemed Consent***
 - Public health or legal requirements may override Dissent

Opt-in

Non-action =
dissent

x	Sensitive Encounter
	Sensitive Provider
	Sensitive-DX
	Sensitive-PX
	Sensitive-RX

Requires active assent
by record / data
element

Encounter
Provider
DX
PX
HX
RX

Conditional
Assent by
Data
Element

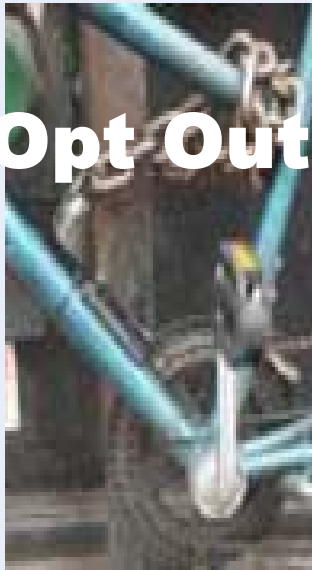
	History
x	Sensitive Provider
x	Sensitive-DX
x	Sensitive-PX
x	Sensitive-RX
	DX
	RX

May not have a
choice where
there is a public
health issue

	Encounter
	Provider
	DX
	PX
x	Sensitive Lab

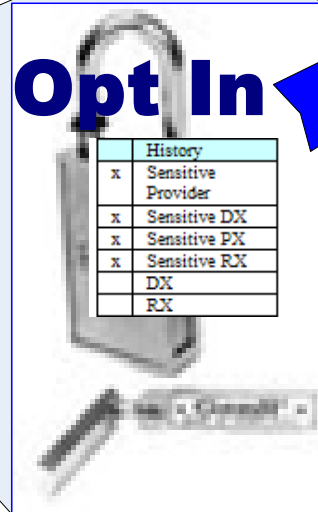
Opt-in / Opt-out Infrastructure

Opt Out

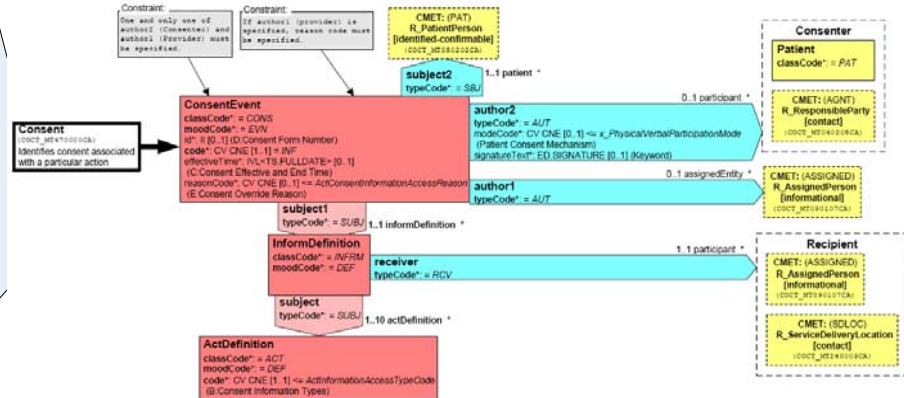
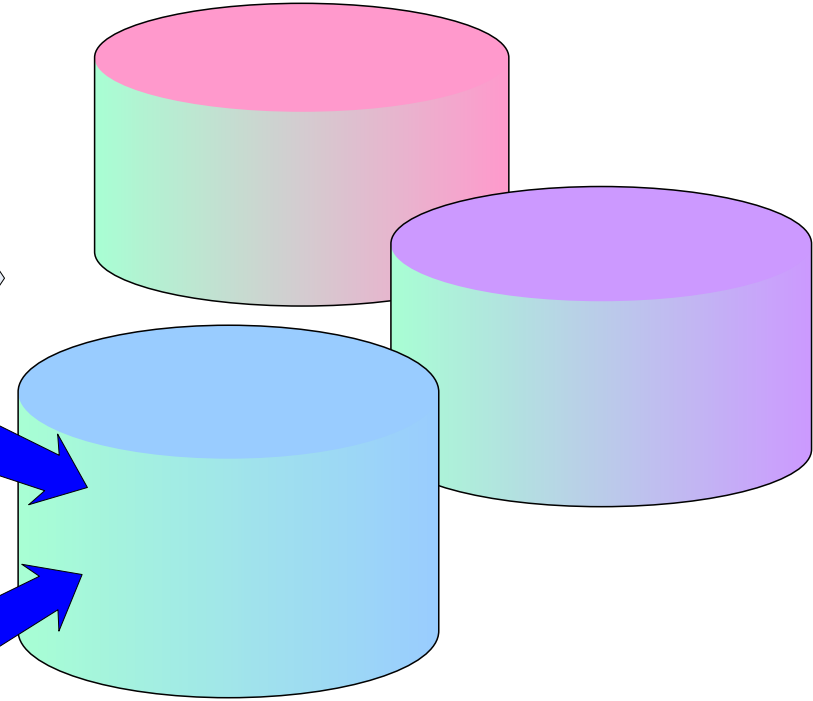


	History
x	Sensitive Provider
x	Sensitive DX
x	Sensitive PX
x	Sensitive RX
	DX
	RX

Opt In



	History
x	Sensitive Provider
x	Sensitive DX
x	Sensitive PX
x	Sensitive RX
	DX
	RX



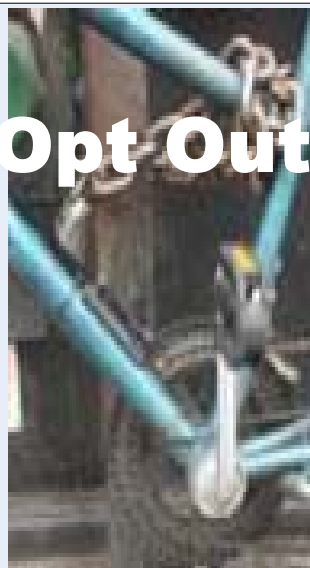
Role Based Access Control

IHE Basic Patient Privacy Consent Profile

Functional Role	Sensitivity						
	Billing Information	Administrative Information	Dietary Restrictions	General Clinical Information	Sensitive Clinical Information	Research Information	Mediated by Direct Care Provider
Administrative Staff	✓	✓					
Dietary Staff		✓	✓				
General Care Provider		✓	✓	✓			
Direct Care Provider		✓	✓	✓	✓		✓
Emergency Care Provider		✓	✓	✓	✓		✓
Researcher						✓	
Patient or Legal Representative	✓	✓	✓	✓	✓		

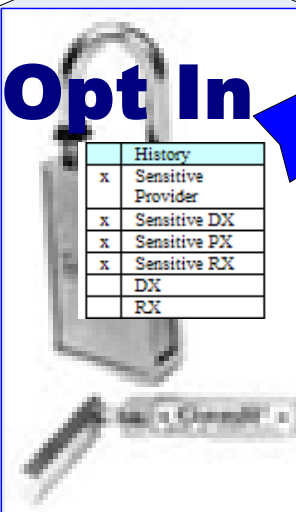
RBAC Support 4 Opt-in / Opt-out

Opt Out



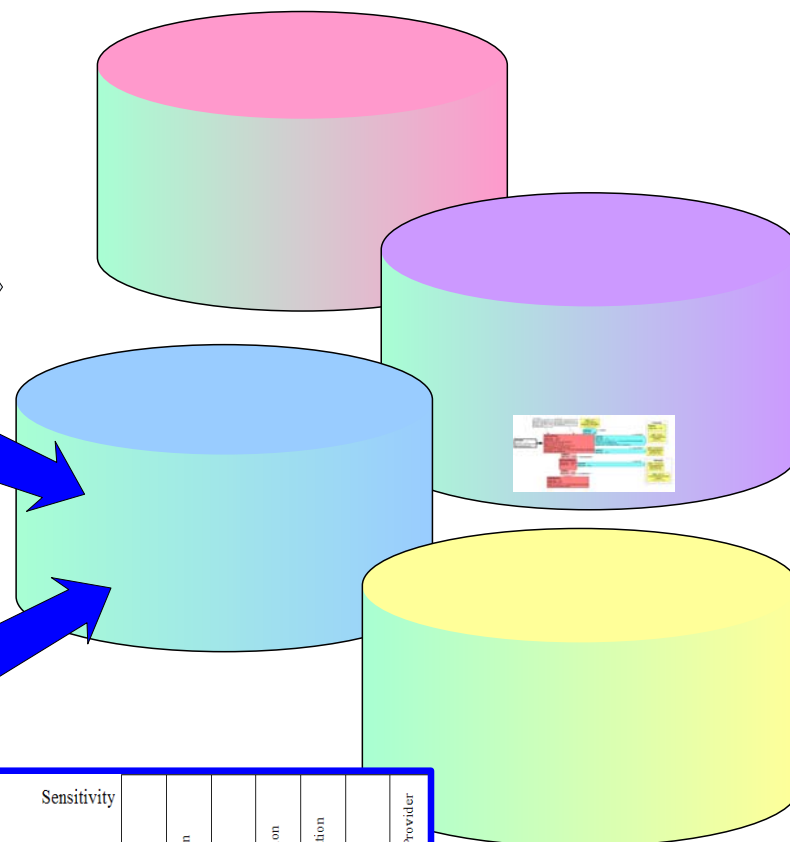
	History
x	Sensitive Provider
x	Sensitive DX
x	Sensitive PX
x	Sensitive RX
	DX
	RX

Opt In



	History
x	Sensitive Provider
x	Sensitive DX
x	Sensitive PX
x	Sensitive RX
	DX
	RX

Functional Role	Sensitivity						
	Billing Information	Administrative Information	Dietary Restrictions	General Clinical Information	Sensitive Clinical Information	Research Information	Mediated by Direct Care Provider
Administrative Staff	√	√					
Dietary Staff		√	√				
General Care Provider		√	√	√			
Direct Care Provider		√	√	√	√		√
Emergency Care Provider		√	√	√	√		√
Researcher						√	
Patient or Legal Representative	√	√	√	√	√		



Shared Secret supports **Conditional Access** that is **time limited** and may be **revoked by the Patient**

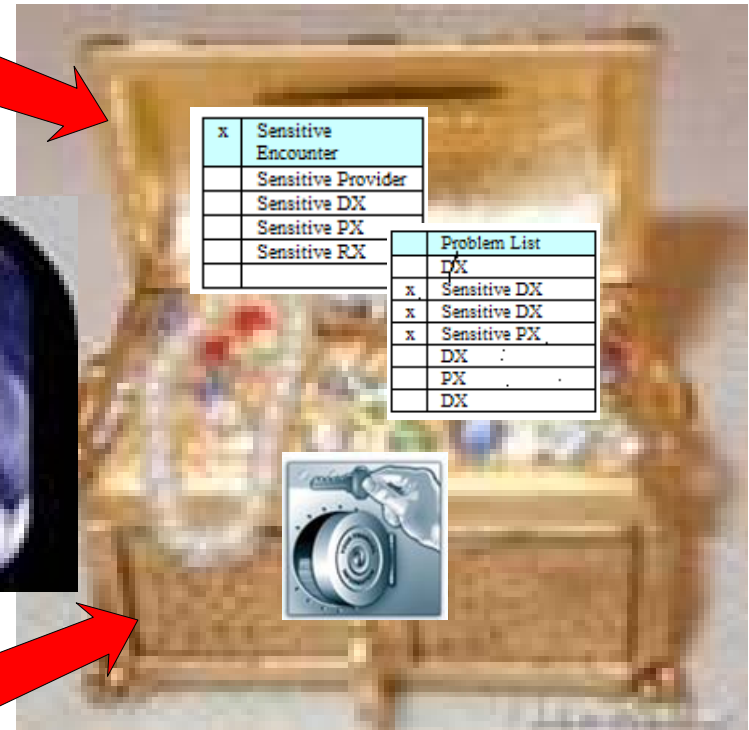
Opt Out

x	Sensitive Encounter
	Sensitive Provider
	Sensitive DX
	Sensitive PX
	Sensitive RX



Opt In

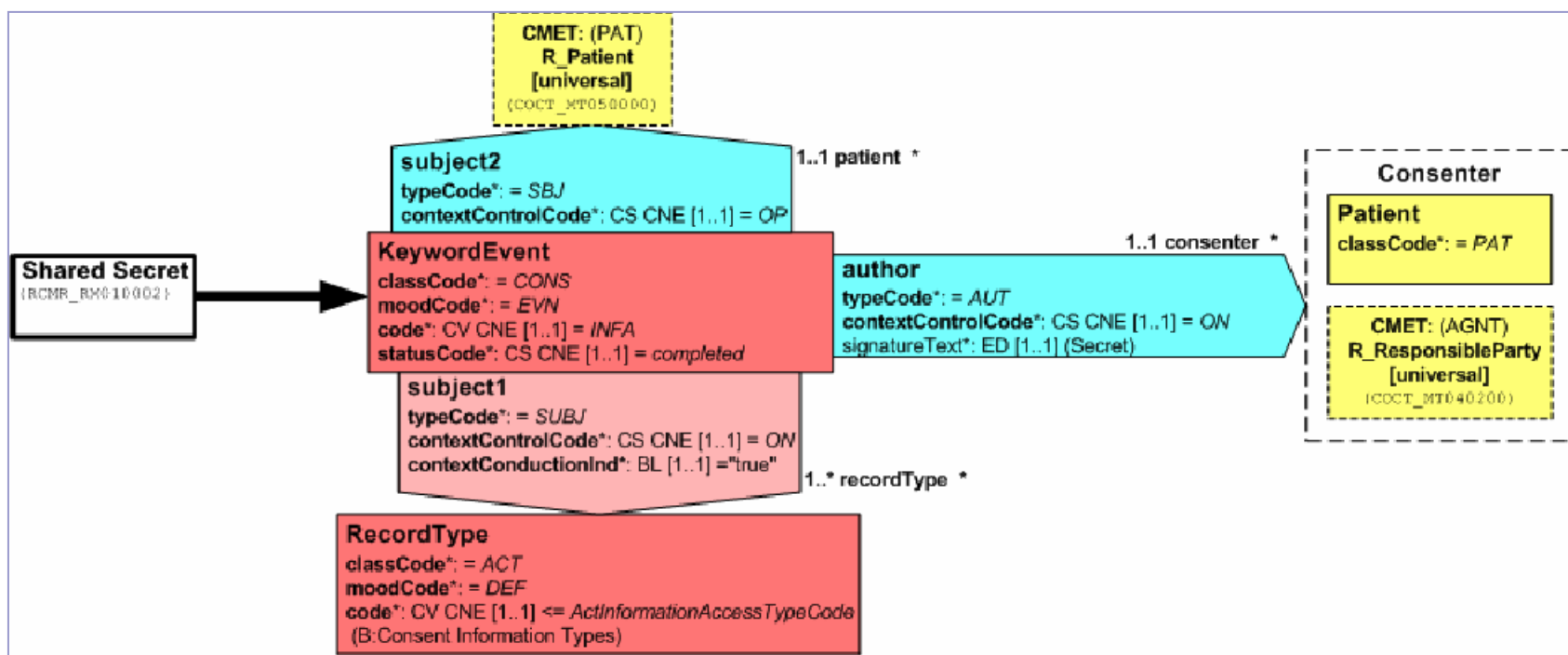
	Problem List
	DX
x	Sensitive DX
x	Sensitive DX
x	Sensitive PX
	DX
	PX
	DX



x	Sensitive Encounter
	Sensitive Provider
	Sensitive DX
	Sensitive PX
	Sensitive RX

	Problem List
	DX
x	Sensitive DX
x	Sensitive DX
x	Sensitive PX
	DX
	PX
	DX

Masking Supports Conditional OPT-IN / OPT-OUT



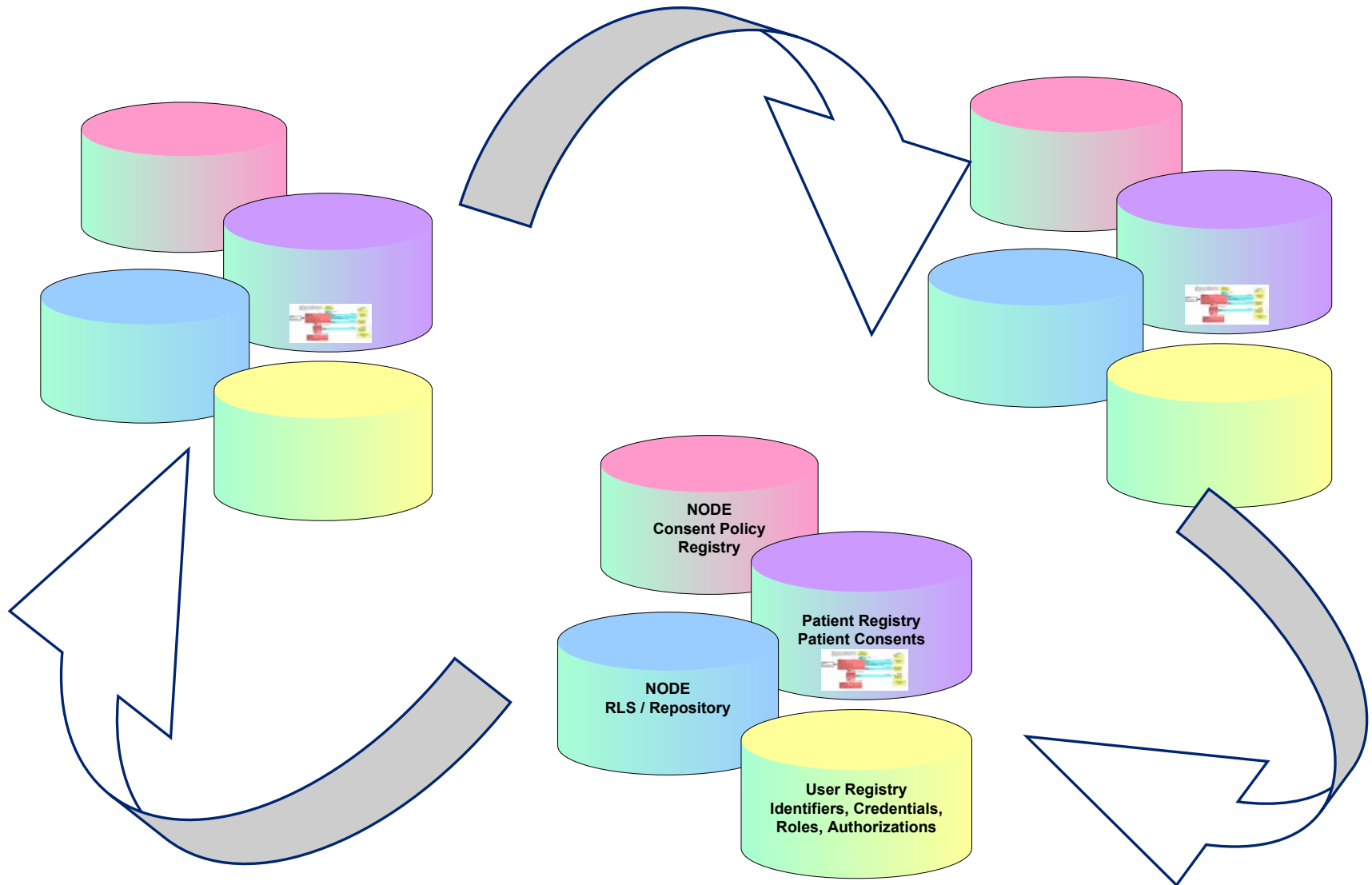
RBAC and Masking Issues

- Mapping User Types to Roles
- Defining Teams
- Mapping Roles to Authorizations
- Downstream application of consent parameters
- Ontology of roles, authorizations, and consent parameters needed for computable interchange
- Security mechanisms to support time limited, renewable, and revocable shared secret, e.g., scheduled change of key hash with patient ability to revoke key access

RBAC with support for Masking

	Billing Information	Administrative Information	Dietary Restriction	General Clinical Information	Sensitive Clinical Information	Substance Use Information e.g. 42 CFR protected	Masked Diagnosis, Procedure, Demographic or Provider Information
Admin Staff	X	X					
Dietary Staff		X	X				
General Care Provider		X	X	X			
Direct Care Provider		X	X	X	X	Must request disclosure	Must request disclosure
Emergency Care Provider		X	X	X	X	Must request disclosure Break Glass	Must request disclosure Break Glass
Direct Provider of sensitive services requiring consent for any disclosure under jurisdictional law		X			X	X	X
Provider with Authorization to access masked	N/A				X	X	X
Provider where context prompts to request disclosure	N/A				Must request disclosure Break Glass	Must request disclosure	Must request disclosure Break Glass only if not 42 CFR

NODE2NODE via NIN



NHIN Support for Consent

- Standards for electronic representation of Node consent policies and patient consents
- Computable access to Node consent policies
- Computable patient consent transmitted with associated PHI
- Standards for computable negotiation of multiple node policies associated with a patient's PHI