HIPAAT®
Consent Management Specialists

CONSENT MANAGEMENT

Implementing Consumer Privacy Preferences in Health Information Exchange (HIE) using Service-oriented Architecture (SOA)

March 2009

Introduction

The digitization of health records brings many benefits to consumers, healthcare providers and Health Information Organizations (HIOs) – more reliable patient information, fewer medical errors, reduced adverse drug events, improved care and billions of dollars in cost savings to the healthcare industry.

However, the sharing of personal/protected health information (PHI) significantly increases the risks associated with patient privacy. No information is more personal than PHI; with PHI available to any number of individuals at the click of a mouse, the question arises: how is consumer privacy respected and protected? Also, if robust privacy protections are in place, can healthcare providers be assured they will have access to the medical records they need at the point of care to treat their patients?

The American Recovery and Reinvestment Act of 2009 (ARRA) signed into law by President Barack Obama on February 17, 2009 clearly calls for the accelerated creation and exchange of electronic health records (EHRs) for all Americans.[i] Mandates by Canada Health Infoway to build an EHR infostructure, the National Health Service Care Records Service to link patient information across England, and initiatives by other nations also call for countrywide EHRs.[ii] The challenge for the healthcare industry is not only to achieve this impressive objective, but to do so in a way that respects patient privacy and addresses consumer consent preferences without hindering care.

The goal is to stimulate electronic health information exchange to improve quality of care and reduce costs, leveraging EHR systems that enforce consumer privacy.

The goal is therefore to stimulate electronic health information exchange to improve quality of care and reduce costs by leveraging interoperable EHR systems that enforce consumer privacy.

This white paper presents a practical model for Web-based, interoperable privacy and consent management at all levels of health information exchange (HIE) using Service-oriented Architecture (SOA).

Market drivers

The need to accommodate – and automate – consumer privacy preferences in HIE has been recognized by the healthcare IT industry for some time, as evidenced by the standards activities underway to address just that.[iii] But additional factors are pushing consumer privacy and consent onto center stage:

1. Legislative Mandates

   The impetus of many countries to develop EHRs – most recently highlighted by the U.S. ARRA – reinforces the importance of consumers' involvement in the privacy and exchange of their PHI, and the requirement for care delivery organizations (CDOs) and HIOs to put new protections in place. For example, the ARRA:

   - requires the HIT Policy Committee to recommend technologies that protect health information privacy and security in EHRs, including segmenting and protecting specific, sensitive PHI from disclosure so that patients are not reluctant to seek care or disclose medical condition information because of privacy concerns[iv]
   - requires covered entities' business associates that obtain or create PHI, such as Personal Health Record vendors, to follow the same privacy requirements as covered entities[v]
   - requires covered entities to notify individuals of security breaches, where their unsecured PHI has been subject to unauthorized use or disclosure[vi]
   - enables individuals to restrict certain disclosures of PHI when the individual has paid for the related medical service or treatment out of pocket[vii]
   - enables patients to receive an accounting of disclosures made through an EHR – even for those related to treatment, payment or healthcare operations.[viii]

2. Expensive data breaches

   Privacy and security breaches are an ongoing threat to health information exchange. During 2006-2007, more than 1.5 million names were exposed in data breaches in U.S. hospitals alone, not taking into account other care settings such as clinics.[ix]

   The costs are enormous. A 2008 U.S. study found the average total cost per organization to be over $6.6 million per breach, ranging between $613,000 and almost $32 million.[x] Data breaches cause healthcare organizations to lose the greatest number of customers (6.5% on average) in relation to organizations in other industries, even financial services, due to the particularly sensitive nature of health information.[xi] According to the study, more than 88% of breaches involved insider negligence.[xii]

"Many see the 'insider' threat – employees who have legitimate access to a network and the personal information it contains, but who choose to abuse this privilege – as the most dangerous security and privacy threat and the one that is the most difficult to defend against."

~ Jennifer Stoddart, Privacy Commissioner of Canada, Infosecurity Canada Conference & Exhibition. Toronto, June 2006.

Cost breakout associated with a breach of non-compliance, from a Director of IT in the U.S.:

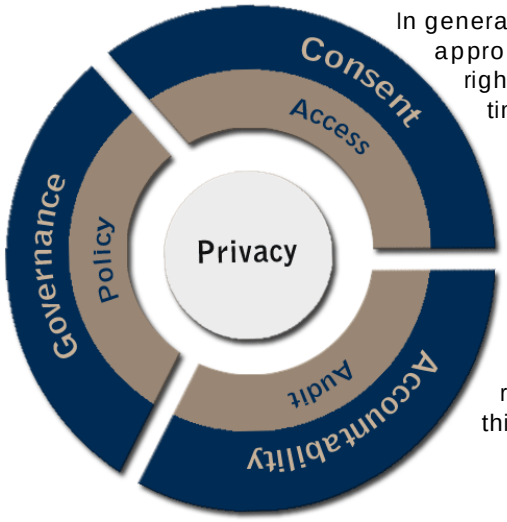
Description	Cost
HHS "Resolution Amount"	$ 100,000
Annual Report	$30,000
Develop policies subject to HHS approval	$50,000
Mandatory workforce training within 90 days	$50,000
Conduct Risk Assessment	$50,000
Mandatory quarterly monitoring of training	$1,000,000
External initial + 3 annual compliance audits	$800,000
States Breach Notification (365,000 individuals)	$500,000
Credit monitoring for one year @ $10/person	$3,650,000
Total	**$6,230,000**

Source: NCHICA Conference, Hewitt & LaBanc presentation [slide 9], September 08, 2008

The threat of internal breaches is not sufficiently mitigated by privacy policies and procedures; automation is the necessary complement. Through automation of consumer consent preferences, organizations can prevent most health information privacy breaches, and be immediately alerted to unauthorized disclosures of PHI when they do occur.

Health Information Privacy and Consent Management

Health Information Privacy Management



In general terms, health information privacy management refers to the appropriate provision of PHI to authorized healthcare providers, such that the right provider has access to the right PHI, for the right purpose, at the right time, for the right patient. There are three main components:

Governance – the policies, laws and regulations of a given healthcare jurisdiction govern how health information is to be collected, accessed, used and disclosed.

Consent – In many jurisdictions, consumers have the right to restrict access to their PHI, and in some cases must provide consent to permit access.

Accountability – there must be accountability to the consumer regarding the safeguarding and management of their PHI. To enable this, all PHI-related transactions must be audited.

Consent Management

Consent Management is a process that:

1) enables consumers to affirm their participation in eHealth initiatives in cases where participation cannot or should not be implied or assumed
2) enables consumers to establish privacy preferences / policies to direct who shall have access to their electronic PHI, for what purpose and under what circumstances
3) supports the dynamic creation, management and subsequent enforcement of consumer, organizational and jurisdictional privacy policies through access control mechanisms.

Why is consent management important?

- **It impacts patient safety and quality of care.** Individuals concerned about the confidentiality of their PHI are less likely to participate in HIE or be forthcoming when seeking treatment.[xiii] This results in less reliable health information available to providers and therefore reduced quality of care. Individuals with PHI privacy concerns may avoid treatment altogether,[xiv] putting their health at risk.

- **It is key to building consumer and provider trust in HIE[xv] and necessary to the overall success and adoption of EHRs**. Many consumers expect such privacy protections before they will entrust their PHI to be shared electronically.[xvi] If privacy protections are not properly implemented – and balanced with provider access to PHI – HIE will fail.[xvii]

- **It is law.** In various jurisdictions of a number of countries – including the United States and Canada – consumers have the legal right to limit disclosure of their PHI.[xviii]

Health information privacy to date

Many countries have laws specifically protecting the privacy and confidentiality of individually identifiable health information. However, even CDOs that have been strong on governance have often proven weak on controls. [xix] Computerized healthcare systems to date have done a poor job of preventing users from accessing PHI that is beyond their required need-to-know.[xx] Role-based access control (RBAC) typically permits users to access PHI available to their role even when such access is inappropriate. For example, does a urologist need to access the diagnostic images of a broken arm?

Relying primarily on healthcare providers themselves to enforce the policies and procedures that govern health information privacy is both unfair and ineffective. Widespread data breaches persist.[xxi] And consumers, often not fully aware of their privacy rights, question the confidentiality of their PHI when it is shared electronically, undermining the success of HIE.[xxii]

To enforce consumer privacy policy, privacy-based access control is needed.

Implementation challenges

Implementing consumer privacy in HIE brings key challenges. CDOs and HIOs must:

- Add privacy management to disparate clinical applications and systems (e.g. diagnostic imaging or drug information systems) from multiple vendors so that privacy policies can be applied consistently.
- Make legacy systems 'privacy aware.'
- Deal with the complexities and variations in consent-related data sets, formats, definitions and regional differences, so that local systems can apply privacy rules appropriately.
- Log all access to PHI for auditing and accountability.
- Capture consumer preferences (consent directives) using consent management suitable for automation – and apply those preferences system-wide.
- Consistently enforce consumer consent preferences as well as organization-specific policy (e.g. treatment of VIPs' or employees' PHI) and jurisdictional privacy policy (e.g. specific treatment of mental health records) with respect to the use and disclosure of PHI within and outside the organization.
- Ensure patient safety is paramount, allowing authorized providers to access restricted PHI – e.g. through override – when needed to treat their patients (as permitted by legislation).

"So when you think about this from an implementation standpoint, what this means... is that you're going to need to plan and implement consent management so that you can keep a record of the consents you have on file, make sure all the requests for information are filtered properly by those consents, and allow your client base access to the consents and the ability to change them when they want."

~ Dr. William A. Yasnoff, Founder, National Health Information Infrastructure Advisors, in a Podcast: eHealth and Compliance in Healthcare IT Infrastructure, posted on IT Knowledge Exchange, January 19, 2009

The Solution: Automating Consent Management using SOA

As internet technologies have become faster and increasingly secure and reliable, network services in general have proliferated. Service-oriented Architecture (SOA) offers an attractive solution to the challenges of implementing privacy and consent management network-wide, allowing the use of existing infrastructure to achieve new functionality.

SOA

Service-oriented Architecture is a "paradigm for organizing and utilizing distributed **capabilities** that may be under the control of different ownership domains."

~ Reference Model for Service Oriented Architecture 1.0, OASIS Standard, October 12, 2006

Why SOA?

SOA brings consistent, interoperable privacy management capabilities to all PHI-related applications and nodes within and across CDOs and HIOs, with minimal overhead and integration. It moves the burden of validating consumer-centric PHI permissions from diverse applications to specialized network-based privacy services.

Underlying Issues:

All data processing nodes in a health information network (see Fig. 1.0 for examples) need to be privacy-aware. However, the application nodes (e.g. clinical workstations) at the edges of the network – which provide PHI to users of various roles – need to enforce access control of the PHI, as this is where all the factors affecting the privacy decisions are known. These factors include **when** the PHI is requested, **what** PHI is being accessed, **who** is requesting the PHI and **why** the PHI is required.

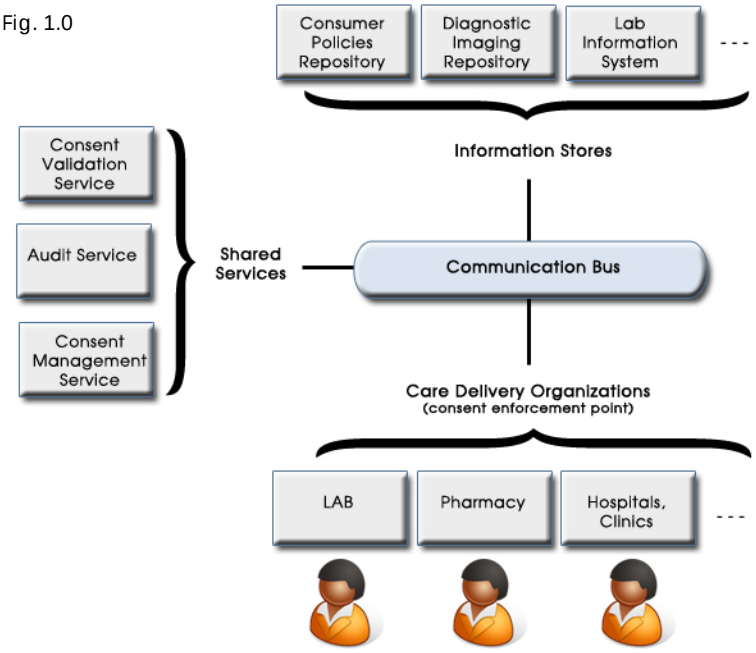
It is certainly possible for an application node at a point of service – or a network application server – to obtain the privacy and consent policies of the consumer in question and then adjudicate whether to allow access to the PHI in question. However, this is not necessarily achievable in the case of every application or clinical device, as they come in a range of capabilities from a diversity of vendors.

Using SOA:

What SOA does is allow these weighty decisions to be offloaded to a specialized processor that is optimized for this purpose. Instead of dealing with consent locally, the following occurs: when a user requests access to PHI, the clinical application sends the known attributes of the PHI, the requester and the intended use for the PHI to a trusted Consent Validation Service (an SOA-based Web service). It then receives a simple answer in response: Permit access, Deny access, or Permit through override.

Fig. 1.0 shows an HIE network supporting consent services that are used by both CDO applications and information stores.

Fig. 1.0



Required elements

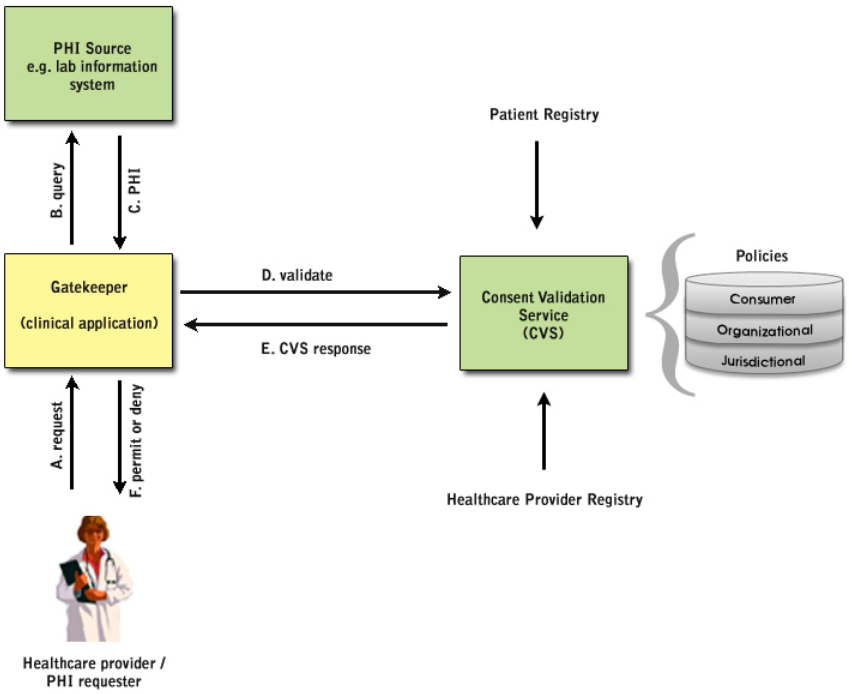
A number of elements are integral to this model, including:

* Consumer Policies Repository – also called the Policy Information Point (PIP), this repository stores consumer preferences / consent directives.
* Consent Management Service (CMS) – Also known as the Policy Administration Point (PAP), the CMS is a Web service that enables the creation and administration of organizational and jurisdictional privacy policies, in the form of access rules.
* Consent Validation Service (CVS) – Also called the Policy Decision Point (PDP), the CVS is a Web service that adjudicates a user's authorization to access a consumer's PHI, based on the rules of the existing privacy policies.
* Consent Enforcement Point – Also called the Policy Enforcement Point (PEP), it is a point of service application – often an existing clinical application – that enforces consumer consent preferences by allowing or denying access to PHI, in accordance with the decision received from the CVS.
* Audit Service – a centralized, standards-based repository of audit events that logs all access and attempted access to PHI.

How consent validation works

Figure 2.0 illustrates a basic model for consent validation using SOA-based Web services. Validation occurs after privacy policies have been created (e.g. via a personal health record or other user interface) and stored as consent validation rules.

Fig. 2.0



A. Healthcare provider requests patient PHI.

B. Clinical application queries the information from the clinical source(s), e.g. laboratory information system.

C. PHI source provides details (metadata) about the information and in some cases may also supply the requested PHI.

D. Clinical application acts as the gatekeeper and requests the network CVS to validate the PHI access, passing in the attributes that are known at the time, including: patient ID, provider ID, intended purpose of use, PHI attributes, etc.

E. The CVS uses the given attributes together with a number of other inputs to adjudicate a response of 'Permit,' 'Deny' or 'Permit through override.'

F. In the case of a 'Permit' response, the clinical application retrieves the PHI not already present and provides access to the healthcare provider. Otherwise the clinical application will inform the provider of the unavailability of the data, or the option to override the restriction.

In this model, a Web-based CVS is able to compute many attributes when validating privacy-based user access permissions. Some of these factors are related to the PHI in question, such as the clinical domain of the data and the date range associated with the PHI (representing one or more care encounters). Some factors are related to the provider requesting the data, such as his/her current role and location. Some are related to real-time factors, such as purpose of use, and others to long-standing factors such as regional policies.

Interoperability, Standards and Consent

There are a number of industry / standards development organizations addressing the interoperability issues of security, privacy and consent. These include HL7, IHE, HITSP/ANSI, NIST and OASIS.[xxiii] The OASIS eXtensible Access Control Markup Language (XACML) specification is seeing increasing adoption as the standard way to express access control policies in a number of application areas, including healthcare. For specifying consent rules and policies, there are two areas where this is useful:

- **As a language for expressing access rules in structured consent documents.**
- **As a format for querying access to PHI and receiving a response.**

XACML, however, must be supplemented by data sets defined by other standards, such as those of HL7. Such data sets are necessary to represent the attributes used in XACML. It is also necessary to establish mappings to attributes used to describe health information, user roles and permissions, and purpose of use.

When looking to standards for implementing consumer preferences, it is wise to take a flexible approach that can evolve as the standards evolve.

10 things to look for in a privacy and consent management solution

1. *SOA-based*
2. *Interoperable/vendor agnostic*
3. *Non-disruptive to clinical workflow*
4. *Centralized to consistently enforce policies network-wide*
5. *Enables all clinical applications to support consumer consent*
6. *Accommodates granular directives*
7. *Audits all access to PHI in real time*
8. *Supports break-the-glass/override access*
9. *Provides alert mechanism for privacy breaches*
10. *Flexible*

Benefits of an SOA approach

- **Reduced costs:** using SOA, one CVS system can support a large network of existing clinical applications, systems and technologies, therefore reducing costs.
- **Straightforward implementation:** The standards-based network interface, using XACML with HL7 vocabulary, is simple to implement.
- **Non-disruptive:** there is virtually no impact to clinical workflow.
- **Interoperable/vendor agnostic:** all types of clinical applications that attach to the network are able to support consent validation, from large web clusters down to embedded devices.
- **Consistent:** the CVS provides a central place where policies are consistently enforced; policy changes are made network-wide in real time.
- **Accommodates granular directives:** consumer, organizational and jurisdictional directives are accommodated; consumers may restrict access to specific, sensitive portions of their record.
- **Provides real-time auditing:** the CVS generates an audit trail for all access and attempted access to PHI.

Conclusion

Consumer preferences can be implemented and enforced consistently at all levels of health information exchange by offloading the privacy decision processes to a specialized, third-party source.

A standards-based SOA approach to health information privacy and consent management can be leveraged **now**. It provides distinct benefits over alternatives in that:

- consent preferences and jurisdictional policies are rigorously managed in one or more central servers, with policy changes available network-wide in real time
- complex policies are implemented consistently across diverse applications and environments
- existing clinical applications are easily integrated and have greater value as they become 'privacy aware.'

The result? Greater patient and provider confidence in EHRs, increased privacy compliance and improved quality of care.

HIPAAT's Consent Management and Auditing Solution: Components

myConsentMinder

A consumer-centric consent policies repository that enables individuals to easily create, edit and store privacy policies using Web-based templates. myConsentMinder interfaces with standards-based Consent Validation Services.

Privacy eSuite v2.0

An SOA-based consent engine powered by two Web services: a Consent Management Service that enables consumer, organizational and jurisdictional privacy rules to be created and administered; and a Consent Validation Service that adjudicates PHI access requests received from policy enforcement points. Privacy eSuite supports override ('break the glass') access to PHI when legislation permits.

Privacy Manager v2.0

A point of service software application that integrates with clinical applications to enforce privacy policies. Privacy Manager allows or denies access to PHI based on the adjudication of a standards-based Consent Validation Service.

Universal Audit Repository v2.0

A standards-based repository that logs all access – and attempted access – to PHI. It automatically alerts the Privacy Officer or other recipients of override (unauthorized) access.

About HIPAAT

HIPAAT provides consent management and security auditing solutions to healthcare. Our SOA-based software balances consumer information privacy with the clinical need to access personal health information. Our interoperable, standards-based approach enables stakeholders at all levels of health data exchange to implement, audit and enforce patient, organizational and jurisdictional privacy policies.

UNITED STATES
568 9TH STREET SOUTH, SUITE 108, NAPLES, FL USA, 34102

CANADA
5925 AIRPORT RD. SUITE 200, MISSISSAUGA, ON CANADA L4V 1W1

[i] Superintendent of Documents, United States Government Printing Office, "American Recovery and Reinvestment Act of 2009."

[ii] Canada Health Infoway, "Vision 2015 – Advancing Canada's Next Generation of Healthcare." HIMSS Enterprise Systems Steering Committee and the Global Enterprise Task Force, "Electronic Health Records: A Global Perspective," August 2008.

[iii] Health Information Technology Standards Panel (HITSP), "TP 30 - HITSP Manage Consent Directives Transaction Package." Health Level 7, "Community-based Collaborative Care Project." Integrating the Healthcare Enterprise (IHE), "Basic Patient Privacy Consents (BPPC)." Organization for the Advancement of Structured Information Standards (OASIS), "Cross-Enterprise Security and Privacy Authorization (XSPA) Profile of XACML v2.0 for Healthcare Version 1.0."

[iv] Superintendent of Documents, United States Government Printing Office, "American Recovery and Reinvestment Act of 2009," Sec. 3002 – HIT Policy Committee.

[v] Superintendent of Documents, United States Government Printing Office, "American Recovery and Reinvestment Act of 2009," Sec. 13404 – Application of Privacy Provisions to Business Associates of Covered Entities.

[vi] Superintendent of Documents, United States Government Printing Office, "American Recovery and Reinvestment Act of 2009," Sec. 13402 – Notification in the Case of Breach.

[vii] Superintendent of Documents, United States Government Printing Office, "American Recovery and Reinvestment Act of 2009," Sec. 13405 – Restrictions on Certain Disclosures and Sales of Health Information; Accounting of Certain Protected Health Information Disclosures; Access to Certain Information in Electronic Format.

[viii] Superintendent of Documents, United States Government Printing Office, "American Recovery and Reinvestment Act of 2009," Sec. 13405 – Restrictions on Certain Disclosures and Sales of Health Information; Accounting of Certain Protected Health Information Disclosures; Access to Certain Information in Electronic Format.

[ix] Kroll Fraud Solutions, "2008 HIMSS Analytics Report: Security of Patient Data," April 2008. Page 3.

[x] Ponemon Institute LLC, "2008 Annual Study: Cost of a Data Breach," February 2009. Page 4.

[xi] Ponemon Institute LLC, "2008 Annual Study: Cost of a Data Breach," February 2009. Page 4.

[xii] Ponemon Institute LLC, "2008 Annual Study: Cost of a Data Breach," February 2009. Page 5.

[xiii] Harris Interactive, "The Harris Poll #27: Many U.S. Adults are Satisfied with Use of Their Personal Health Information," March 26, 2007. "One in six adults (17%) – representing about 38 million persons – says they withhold information from their health providers due to worries about how the medical data might be disclosed." The figure increases to 21% among those in fair or poor health.

[xiv] Superintendent of Documents, United States Government Printing Office, "American Recovery and Reinvestment Act of 2009," Sec. 3002 – HIT Policy Committee.

[xv] Office of the National Coordinator for Health Information Technology, U.S. Department of Health and Human Services, "Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information," December 15, 2008. Page 8 – Individual Choice.

[xvi] EKOS Research Associates, "Electronic Health Information and Privacy Survey: What Canadians Think – 2007," August 2007. A study co-sponsored by Canada Health Infoway, Health Canada and the Office of the Privacy Commissioner of Canada. Pages 47, 64.

[xvii] Leavitt, M., U.S. HHS Secretary, "Secretary Leavitt Announces New Principles, Tools to Protect Privacy, Encourage More Effective Use of Patient Information to Improve Care," December 15, 2008.

[xviii] Superintendent of Documents, United States Government Printing Office, "American Recovery and Reinvestment Act of 2009," Sec. 13405 – Restrictions on Certain Disclosures and Sales of Health Information; Accounting of Certain Protected Health Information Disclosures; Access to Certain Information in Electronic Format. Pritts J., Connor K., "The

Implementation of e-Consent Mechanisms in Three Countries: Canada, England and the Netherlands (The ability to mask or limit access to health data)," A report prepared for the Substance Abuse and Mental Health Services Administration (SAMHSA) of the U.S. Department of Health and Human Services (HHS). February 16, 2007, page 4 – Consent Mechanisms.

[xix] Rubenstein, J., "Are Your Medical Records at Risk? Amid Spate of Security Lapses, Health-Care Industry Weighs Privacy Against Quality of Care," The Wall Street Journal, April 29, 2008.

[xx] Rubenstein, J., "Are Your Medical Records at Risk? Amid Spate of Security Lapses, Health-Care Industry Weighs Privacy Against Quality of Care," The Wall Street Journal, April 29, 2008.

[xxi] Johnson, M. Eric, "Data Hemorrhages in the Health-Care Sector," Center for Digital Strategies, Tuck School of Business, Dartmouth College, February 2009.

[xxii] Harris Interactive, "The Harris Poll #27: Many U.S. Adults are Satisfied with Use of Their Personal Health Information," March 26, 2007. "One in six adults (17%) – representing about 38 million persons – says they withhold information from their health providers due to worries about how the medical data might be disclosed." The figure increases to 21% among those in fair or poor health. EKOS Research Associates, "Electronic Health Information and Privacy Survey: What Canadians Think – 2007," August 2007. A study co-sponsored by Canada Health Infoway, Health Canada and the Office of the Privacy Commissioner of Canada. Pages 47, 64.

[xxiii] Health Level 7 (HL7), Integrating the Healthcare Enterprise (IHE), Health Information Technology Standards Panel (HITSP)/American National Standards Institute (ANSI), National Institute of Standards and Technology (NIST), Organization for the Advancement of Structured Information Standards (OASIS)