# The Implementation of E-consent Mechanisms in Three Countries: Canada, England, and the Netherlands

## (The ability to mask or limit access to health data)

by

Joy Pritts, JD
Kathleen Connor, MPA

February 16, 2007

## Acknowledgements

This report was prepared by Joy Pritts and Kathleen Connor for the Substance Abuse and Mental Health Services Administration (SAMHSA) of the U.S. Department of Health and Human Services (DHHS) under Contract No.270-02-7120, Task Code 108-01144 with support by FOX Systems, Inc., under Contact No. 270-02-7120, Task Order No. 108-01129 and Contract No. 283-03-9030, Task Order No. 13. Additional non-financial contributions were made by Fox Systems.

## Disclaimer

The content of this white paper does not necessarily reflect the views or policies of SAMHSA or DHHS. The authors are solely responsible for the content.

## Public Domain Notice

## Originating Office

Organization and Financing Branch, Division of Services Improvement, Center for Substance Abuse Treatment, Substance Abuse and Mental Health Services Administration, One Choke Cherry Road, Rockville, MD 20857, Sarah Wattenberg, MSW, Government Project Officer.

## Table of Contents

## LIST OF TABLES AND FIGURES

# Executive Summary

## BACKGROUND

The United States is in the midst of a ten year plan to develop and implement a nationwide electronic health information infrastructure (NHII) that will allow authorized health care professionals to securely access relevant patient data from any location in the country at any time. As envisioned, the NHII in the United States will be a series of cross-jurisdictional interconnected regional health information exchanges or organizations. Various initiatives are underway to foster the development of the NHII along these lines. One core issue that has repeatedly surfaced in these initiatives is how to appropriately protect the privacy and security of health information in an interconnected electronic health information system. Of particular concern is whether and how, as a practical matter, such a system will be able to accommodate the various legal restrictions on disclosing what is generally considered to be potentially sensitive health information (such as information related to HIV/AIDS status, genetic makeup, domestic abuse, mental health conditions or treatment, and substance use). A variety of laws require specific patient consent to disclose this type of information even for treatment purposes.

This paper uses the term “consent” policies and practices when referring to policies and practices that govern whether and how individuals have the right to control when and how their health information can be shared with others. The term "consent mechanism" is used to refer to the methods by which an individual can exercise such control.

## STUDY PURPOSE

The Substance Abuse and Mental Health Services Administration (SAMHSA), HHS commissioned this study to examine other countries' implementation of their respective consent policies and practices, especially with respect to "sensitive" health information, in the context of their developing NHIIs. This study is intended to examine the consent mechanisms currently used or proposed in other countries that could potentially be utilized to implement the existing consent requirements for sensitive health information in the United States.

## METHODOLOGY

We selected for review three countries, Canada, England, and the Netherlands, each of which is further along in the development of their respective NHII than the United States. We selected these countries because they have substantial written materials concerning the country's consent policies and practices available in English and because their consent laws and policies grant their citizens some degree of control over the flow of their electronic health information. We examined each country's NHII model and its current status, the country's consent policies, and their current or proposed implementation of such policies. We limited our review to consent policies related to the disclosure of health information for treatment purposes for two reasons: First, to study policies with respect to consent for disclosing health information for all potential purposes (*e.g.*, public health and research) would require time and monetary resources well beyond those available for this project. Second, the consent policies with respect to disclosing health information for treatment appear to be more settled than policies with respect to electronically sharing health information for other purposes. Because Canada’s privacy policies are largely set at the provincial level, our review of that country focused on e-health projects designed to form components of the Canadian NHII in three different provinces. To put the discussion in the appropriate context we also briefly looked at each country's general funding and structure for providing health care. We reviewed the published literature and websites for each of the pertinent countries and spoke to international health information experts.

## FINDINGS

### Health Care Delivery Systems

Canada, England, and the Netherlands all have some form of universal health insurance. In general, England has a very centralized health care system in which health care services are publicly funded by the federal government. Canada's health care system is more decentralized with the federal government setting policies and standards and the provinces and territories providing health care services. In both countries, basic health care services are free of charge. The National Health Service accounts for 88% of healthcare expenditures in the United Kingdom. Public funding accounts for 70% of healthcare expenditures in Canada. The Netherlands has recently moved to a private health care system. Every resident is required to purchase private health insurance. Private health insurers are required to accept every resident in their coverage area. Insurers must provide a standard basic benefits package at a standard price. People receive a government allowance if the standard premium is excessive in light of their income. Low-income citizens can qualify for a government “healthcare allowance” to go towards the cost of their premiums. The United States has a mixture of public and private insurance. Together, the publicly funded Medicare and Medicaid insurance programs cover 25% of the population and account for approximately 32% of health care expenditures. Private health insurance, through employers or individually purchased, covers 58% of the population (including those with publicly funded insurance). Sixteen percent of the population was uninsured in 2005.[1]

Health care in all countries is somewhat fragmented, particularly with respect to services for "sensitive" medical conditions. While primary care or general practice providers (GPs) often serve as the entry point for most health care, services for mental health, sexually transmitted disease, and alcohol and substance abuse diagnosis and treatment can take place in a number of different forums including specialized clinics, community rehabilitation facilities, and hospitals.

### NHII General Architecture

The countries have adopted different architectural models for their developing national health information infrastructures (NHIIs). They range from data being held primarily at the national level in a central database in England, to data being maintained locally with access through a national document locator service in the Netherlands. Canada's proposed NHII fits somewhere in between. Canada’s NHII will be formed by linking provincial or territorial electronic health information exchange systems, each of which includes domain specific data repositories.

#### *Canada*

Canada Health Infoway, a not-for-profit organization made up of federal, provincial and territorial representatives, is responsible for developing the overall framework and standards for the Canadian NHII. The NHII will be based on province-wide electronic health information exchange networks consisting of patient and provider registries as well as domain registries for prescription drug data, diagnostic imaging, and laboratory results. The provincial/territorial networks will be linked to each other nationwide. Because the privacy laws and policies in

Canada are primarily set at the provincial level, we reviewed operational e-health projects in 3 different provinces.

1. Alberta Netcare POSP
   This program is intended to help physicians move to electronic medical record systems that can be integrated with Alberta's province-wide electronic health information exchange network. The program provides partial funding for physician office system technology that conforms to provincial-wide system requirements, including privacy and security specifications.

2. British Columbia PharmaNet
   PharmaNet is a well-established province-wide electronic network that links all BC pharmacies, as well as many emergency department physicians and medical practitioners in private practice to a central set of data systems, including a prescription database.

3. Ontario Drug Profile Viewer (DPV) System
   The DPV enables the Ministry of Health and Long Term Care to share the prescription drug claim histories of patients who receive government prescription drug benefits. It was scheduled to be fully implemented in 183 hospitals by the end of 2006.

### *England*

England's NHII is designed to serve the National Health System, the publicly funded health care provider for over 50 million people. England's NHII is highly centralized with a central database for individual demographic data and summary health information (Summary Care Records). The Summary Care Record will contain links to patients' Detailed Care Records, which will be maintained locally. Data in the Summary Care Record is to be available nationwide to NHS offices through a private broadband service. Pilots of the Summary Care Record are scheduled for spring 2007 with data supplied from GP records. Due to privacy concerns, the initial summary will only include information about current medications, and suspected adverse and allergic reactions.

### *The Netherlands*

The development of the Netherlands NHII is being coordinated by NICTIZ (National IT Institute for Healthcare), a foundation composed of governmental and private organizations. The Netherlands does not have a central database of health information. Rather, the Netherlands is using a central Web based record locator service, the National Healthcare Information Hub (LSP), which went live in 2006. Under this system, clinical data will be maintained locally in the system of the health care practitioner or existing regional database and will be accessed through a central registry which will tell the requester what data is held in which local database and allow them to access it through links. The LSP has been called a health care "Google." The system will produce a virtual electronic patient record. The first components of the nation-wide electronic patient record will be the Electronic General Practitioner's Record (which will allow after-hours GPs access to a summary health care record from the patient's regular GP) and the Electronic Medication Record (which will contain information about prescriptions and allergies). These records are scheduled for implementation trials in early 2007.

## Privacy Laws and Policies

Canada, England and the Netherlands all have national data protection statutes that implement the EU Privacy Directive. Under all three federal data protection statutes, identifiable health information is included in the "special" category of data entitled to heightened protection. The statutes use an implied consent model for disclosure of health information for treatment purposes coupled with the individual's right to object to disclosure (opt out).[2]

Although Canada has a federal data protection statute, health information privacy is primarily regulated at the provincial level. The provinces reviewed here, Alberta, British Columbia, and Ontario, have privacy statutes with differing requirements. However, all three provinces have endorsed the Pan-Canadian Health Information Privacy and Confidentiality Framework developed by the Advisory Committee on Information and Emerging Technologies (ACIET) of the Federal/Provincial/Territorial Conference of Deputy Ministers. This framework, like that of the EU directive, provides for implied knowledgeable consent for the disclosure of health information for treatment coupled with the individual’s right to withhold or withdraw their consent (opt out).

In addition to adhering to statutes and regulations, providers in all jurisdictions must comply with professional ethical standards that impose on them the duty of maintaining the confidentiality of information received during the course of treating patients.

## Consent Mechanisms

All three countries plan on incorporating in their NHII-related projects electronic mechanisms that support individuals’ rights to control the disclosure of their health information for treatment. In general, these mechanisms involve coding data in such a way that access to or transfer of the data is restricted. This process is often known as “masking.”[i] Masking may be applied at the data source. In addition or as an alternative, masking can occur at a central record repository or on the record index of a record locator service repository depending on the type of health information exchange architecture in which the record may be shared. Organizations may elect to apply masking functionality at differing levels of data granularity or by specific user or category of users.[3] Masking may include access permissions such as “read only” and “may not redisclose” and may stipulate the period during which the permission is granted. Generally, masked data remains accessible to the person or organization that is the source of the information. Masking is currently available to various degrees in electronic health information systems in all three countries. In some systems, masked data may be overridden. In some cases, individuals may give a provider a keyword that allows them to override the masking. This is often called a “shared secret.” The following table describes some of these consent mechanisms as well as other system access.

[i] In this paper we use the term “masking” in general discussions of these mechanisms. Because England uses the terms “sealing” and “sealing and locking” to refer to these mechanisms, we use the English terms when discussing the implementation of these consent mechanisms in that country.

## Table 1: System Access Controls and Consent Mechanisms

| SYSTEM ACCESS CONTROLS AND CONSENT MECHANISMS | | |
|---|---|---|
| **Components** | **Capabilities** | **Description** |
| **Access Control Type**<br>**Definition:**<br>A means of ensuring that the resources of a data processing system can be accessed only by authorized entities in authorized ways. NOTE: May have combinations of Access Control Types, e.g., Doctor X only when she is the attending emergency provider on weekends. | Role-Based Access (RBA) | Granting access based on role of requester, e.g., a provider type; provider with a "legitimate relationship" to the patient or on the patient's care team, or in a work area in which a patient is treated. NOTE that the role criteria may blend with context |
| | User-Based Access | Granting access based on the identity of the requester |
| | Context-Based Access | Granting access to a requester based on context of the request; e.g., Emergency room or only on weekends. Context may be identified based on information supplied by requester and/or information linking the requester's information system to a context; |
| | Shared Secret Access | Granting access to a requester who supplies the patient's keyword or "shared secret". |
| **Access Restriction Mechanism**<br>NOTE: Possible to phase implementation to scale in complexity, e.g., Masking the Record Index based on RBA with READ permission for Information Categories if the Record Index if both RBA and Record Index are linked to these categories. A 2nd phase could add electronic capture of the Consent Directives, implement user- and context-based access, Identifiable Records, and add permissions. Later phases could add remaining capabilities. There will be dependencies among capabilities, as in examples above, i.e., cannot have Masking at the record level & Shared Secret only at the record index level. A federated HIE architecture will require different capabilities than a centralized one. | Masking or Sealing a Record | Concealing the data of record at the source when it is created or retrospectively. May include having flags to alert a provider that a record is masked or sealed. Should include the ability to unmask or unseal the record until a keyword expires or is reset, or until the record is again masked or sealed. |
| | Masking or Sealing a Record Index | Concealing the record index that provides the address of the source data, e.g., in a Record Locator Service. May include having flags to alert a provider that a record is masked or sealed. Should include the ability to unmask or unseal the record index until a keyword expires or is reset, or until the record index is again masked or sealed. |
| | Locking a Record or Record Index | Further restrictions on access to a masked or sealed record or record index, e.g., not having flags to alert a provider that a record is masked or sealed; and more stringent thresholds to warrant an override of the concealment. |
| | Consent Directive | A record of a patient's permissions concerning access to health information. May include consents and dissents with respect to<br>Types of access control, e.g., all out-of-jurisdiction emergency providers, not Doctor X except in an emergency<br>Access permissions, e.g., Doctor X may READ but not AUGMENT a record<br>Access to categories of information; e.g., all HIV related information; all behavioral health providers, diagnoses, and treatments<br>Access to specific items of information, e.g., a prescription for an antidepressant |
| | Shared Secret | A keyword assigned to a record, a record index, or a category of information (e.g., all HIV-related information) that a patient may share on an ad hoc basis with a provider who would not otherwise have access to the information. A patient may have several keywords to segregate access. Keywords attached to the concealed information may need to be reset to reinstate concealment. In the alternative keywords may be randomly-generated with set effective time spans. |

| SYSTEM ACCESS CONTROLS AND CONSENT MECHANISMS | | |
|---|---|---|
| **Components** | **Capabilities** | **Description** |
| **Access Permissions**<br>NOTE: It is unlikely that patients will be consenting to access permissions at this level of detail except in the case of "Read only". Consent policies will likely inform patients that if they consent to e.g., access by care teams that they may either permit all typical appropriate uses, or they may restrict usage to "Read only". | Read only | Permitted to read the information only. All other uses is prohibited |
| | Store | Permitted to store the information. May be combined with other permitted uses. |
| | Print | Permitted to print the information. May be combined with other permitted uses. |
| | Disclose | Permission to disclose the information per applicable policy or law. |
| | Create | Permitted to create new information in the record. May be combined with other permitted uses. |
| | Amend | Permitted to update or modify information in the record per applicable policy or law, e.g., updates of demographic information by clerical staff is permitted; updates to attested records by anyone is prohibited. May be combined with other permitted uses. |
| | Augment | To provide additional information regarding the healthcare data, which is not part of the data itself, e.g. linking patient consents or authorizations to the healthcare data of the patient. |
| | Delete | Permitted to delete information in the record per applicable policy or law. e.g., delete only if the provider has not yet attested to the record. May be combined with other permitted uses. |
| **Access Information Type** | Access Information Category Type | Demographic |
| | | Condition |
| | | Diagnosis |
| | | Treatment |
| | | Medication |
| | | Provider Type |
| | Identifiable Record | Record that can be uniquely identified. If the record is unstructured, i.e., is electronic image of uuencoded data, e.g., a scanned letter; then identification is only possible at the record level. |
| | Identifiable Data Element | Data Element identified syntactically - e.g., all data in X12 271 in the EB01 segment related to behavioral health programs; or semantically - a behavioral health provider taxonomy code |
| | Record Index | Uniform Resource Identifier (URI) for the record – e.g., in a Record Locator Service Repository |
| **Access Restriction Override Mechanisms** | Flag | An alerting mechanism that indicates that relevant information has been masked/sealed. The provider may request patient consent to access, and may be given a keyword to do so. The provider may override the concealment based on policy criteria, e.g., the patient is unable to give consent and is at risk; or for public welfare. |
| | Override | The ability of a provider to access concealed health information without the patient's consent. |

### *Canada*

Canada has designed the privacy and security architecture of its NHII to support various models of consent. This flexibility means that provinces and territories can use the architecture to implement the privacy protective features that are consistent with their local policy and legislative requirements.

Because health information privacy is primarily regulated at the provincial level in Canada, we reviewed e-health projects in three provinces with differing health privacy statutes. Although all three of the provinces have endorsed the Pan-Canadian Privacy Framework, the method in which they have implemented the framework varies. All three of the projects currently have the technological capacity to mask health data.

The systems of physicians participating in the Alberta Physician Office System Program, are capable of masking data at the discrete data element level (partial opt out). The systems also are capable of overriding the masking of the data, and logging the override, including the user's id, date and time, and the reason for the override. As of 2008, the systems also must be capable of allowing individuals to allow or restrict access to their data to specific health care providers, purposes or circumstances (e.g., emergency). The systems will also be required to be able to alert the user when a new prescription order or dispense interacts with a masked record.

In the British Columbia PharmaNet project, individuals can mask their entire prescription record by having their pharmacist attach a keyword to the record. They then have the ability to allow the providers of their choice to access their record by sharing the keyword with them (shared secret). Emergency departments can override the masking in emergencies by having the keyword reset.

Systems participating in Ontario's Emergency Department to Drug History Initiative have the ability to totally mask an individual's prescription record (total opt out). In addition, the systems can mask specific drugs identified by the individual at their request (partial opt out). Temporary access to otherwise masked data can be obtained using the patient's health number.

### *England*

The NHS has committed in the future to enabling individuals to limit access to sensitive information within their records. The individual will be able to request that specific information within their clinical record is accessible only with their consent. In England, this function is called "sealing" and the information to which access has been limited is said to be in a "sealed envelope."

Although some provider software in England already provides a degree of sealing functionality, wide-spread sealing functionality along the lines described below is expected to become available in 2008-9. Under current plans, individuals will be able to restrict access to sensitive information in their Summary Care Record or Detailed Care Record by having it "sealed" (opt out). Sealed information remains available to the provider who created the information and the health care team to which the provider belongs. The sealed information generally will not be available to providers not on the team. A provider generally cannot override the seal without the patient's permission.

### *The Netherlands*

In the Netherlands, individuals will be able to mask or restrict access to their data by data element; by user or category of users; and by context.

An individual can totally opt out of participating in the electronic exchange of their health information (in which case it is not recorded in the national registry and cannot be accessed in an emergency). They also can request their provider to conceal or mask discrete data items in their medical record. When the provider's system receives an inquiry for the masked data, the system will not return the data. When information is masked at this level, it is generally concealed from *all* health care providers other than the generating source.

Individuals also will be able to restrict access to their data by user or category of users through specifying choices in their authorization profiles. Authorization profiles, which will be maintained in a national registry, will allow individuals more detailed choices including establishing: which providers or class of providers may access their health information; the context in which they may access (e.g., “only in emergency”); and the category of information (e.g., demographic or medical) which is accessible.

This paper presents a "snapshot" of these countries' proposed frameworks for patient consent as of January 2007. Table B summarizes some of the main consent functions that are present or planned for these nationwide (and in the case of Canada, provincial) health information infrastructures.

## Conclusion

There are a number of mechanisms currently in use that may be useful in managing "sensitive" medical information in the proposed US NHII. Consent mechanisms can be used to mask data when the individual has not consented to its disclosure. Certain providers may implement systems that automatically mask health information which, by law, requires specific consent to disclose. Masking in combination with a "shared secret" could potentially be used to permit individuals the ability on an ad hoc basis to specifically consent to the disclosure of their sensitive health information only to those to whom they provide the shared secret. Providers’ ability to override masking could potentially fulfill legal provisions which allow physicians to access even sensitive information to provide care in emergency situations. The proposed "seal" and "lock" could enable the compliance with the strictest level of confidentiality requirements. For example, substance use information could potentially be sealed and locked against access by law enforcement authorities, where applicable. Detailed authorization profiles also hold much promise, potentially allowing individuals to specify with varying degrees of granularity the providers to whom they consent (or do not consent) to disclose their health information.

These mechanisms, however, are not perfect. The mechanisms described work best with coded data. With respect to unencoded data, the consent mechanisms can be used at a high level (e.g., masking or sealing an entire record in a particular database). They cannot be used to shield or restrict the transfer of unencoded data at the discrete data element level (*e.g.,* a portion of a scanned letter). Given the potential wide-spread distribution of health data, it may also prove difficult to ensure that copies of data are masked along with the original. It is also difficult as a practical matter to maintain patient control over masked data that is incorporated into new records, *e.g*., a provider’s narrative about an encounter with the patient in which the patient has permitted that provider access to sensitive masked data. Furthermore, identifying and marking all the health data elements that would reveal a patient’s condition is difficult particularly on a prospective basis and will require development of algorithms.

Experience in other countries, which are further along in the development of their respective nationwide health information infrastructures, may shed some light on whether and how the United States may be able to implement information policies based on individual control or consent in its NHII.

## Table 2: Consent Mechanisms

| Consent Mechanisms Can/Will Be Able to Support | Canada Provincial HIIs | | | England (Summary Care Record) NHII | The Netherlands[1] (Electronic GP Record) NHII |
|---|---|---|---|---|---|
| | Alberta POSP | British Columbia PharmaNet | Ontario DPV | | |
| **Total opt out** of having any clinical information uploaded or *registered* in system[2] | N | N | N | Y | Y |
| Registering or uploading clinical information, **but total opt out** of electronically *sharing* any health information through system | Y | Y | Y | Y | Y |
| **Partial opt out** with respect to sharing *selected health information* beyond originating provider | Y | N | Y | Y | Y |
| **Partial opt out/in** with respect to sharing health information with *selected health care providers* or categories of providers | Y[3] | Y | N | N | Y[4] |
| **Partial opt out** with respect to potentially sensitive data in demographic profile | Y | Y | Y | Y[5] | Y |

Y—Yes - proposed or in place
N—No

[1] In the Netherlands, only basic information will be registered in a national registry index which serves as a document locator service.
[2] When an individual chooses not to have their information uploaded or registered at all, the information is not available through the health information infrastructure for emergency care. When an individual chooses to have their information uploaded but sealed or masked, the information is potentially available for emergency care.
[3] Scheduled to be implemented in 2008.
[4] Proposed as part of authorization profile.
[5] Decision whether to "stop note" sensitive patient demographic data (*i.e.*, make it inaccessible to general users of the system) is not made solely by patient.

# 1 Introduction

## 1.1 Background

The United States has committed to promoting the development and implementation of a nationwide health information infrastructure (NHII) that will provide access to the right health information at the right time and the right place.[4] As envisioned, the NHII will be a series of cross-jurisdictional interconnected healthcare data-sharing organizations, often called regional health information organizations.[ii] The administration has established the Office of National Coordinator of Health Information Technology (ONC), United States Department of Health and Human Services (HHS) to, among other things, provide leadership for the development and nationwide implementation of an interoperable health information technology infrastructure to improve the quality and efficiency of health care and the ability of consumers to manage their care and safety.[5]

The NHII is intended to improve the quality, safety and efficiency of health care while ensuring that the privacy and security of patients' identifiable health information is protected. In pursuing this goal, HHS has voiced the belief that success of moving from a paper-based to electronic health information system hinges in part on maintaining and improving consumer confidence in the privacy and security of their health information.[6] HHS also believes that electronic health information systems have the potential to provide a less burdensome means of meeting existing privacy and security standards that govern the provision and limitation of access to health information.[7]

A number of federally sanctioned initiatives to advance the development of the NHII have been undertaken under the auspices of ONC including, but not limited to:

- *American Health Information Community (AHIC)* which is charged with advising the Secretary of HHS and recommending specific actions to achieve a common interoperable framework for health IT.
- *Healthcare Information Technology Standards Panel (HITSP)* which serves as a cooperative partnership between the public and private sectors for the purpose of achieving a widely accepted and useful set of standards specifically to enable and support widespread interoperability among healthcare software applications, as they will interact in a local, regional and national health information network for the United States.[8]
- *Health Information Security & Privacy Collaboration (HISPC)* which, through a contract awarded by the Agency for Healthcare Research and Quality (AHRQ), will conduct assessments in 33 states and one territory to identify organization-level business policies and state laws affecting the electronic clinical health information exchanges; developing best practices and proposed solutions to address identified challenges; and increasing expertise about health information privacy and security protection in communities.[9]

[ii] There are a number of terms applied to such organizations including regional health information organizations (RHIOs), health information exchanges (a generic term used by eHealth Initiative), subnetwork organizations (the term used by Connecting for Health and the collaborative response to the Office of the National Coordinator for Health Information Technology) and health information network.

The issue of how to appropriately protect the privacy and security of health information in an electronic interoperable health information system cuts across all of these initiatives.[iii] Of particular concern is whether and how, as a practical matter, such a system will be able to accommodate  the various legal restrictions on disclosing what is generally considered to be potentially sensitive health information (such as information related to HIV/AIDS status, genetic makeup, domestic abuse, mental health conditions or treatment, and substance use).

The Privacy Rule issued under the Health Insurance Portability and Accountability Act (HIPAA) (45 C.F.R. part 164, subpart E) generally treats all health information (with the exception of narrowly defined psychotherapy notes) the same and allows health care providers to disclose protected health information without the individual's express permission for treatment, payment and health care operations.[iv] Thus, under the HIPAA Privacy Rule, even "sensitive" health information may be disclosed to others for treatment, payment and health care operations without the individual's express permission.

However, the HIPAA Privacy Rule is not the sole standard that governs the exchange of this health information. Most states have statutes or regulations that afford a higher degree of protection to information related to certain health conditions and treatment.[10] These laws often require the individual's written permission in order to disclose this "sensitive" health information, sometimes even for treatment purposes.[11] In addition, a separate federal law (section 543 of the Public Health Service Act, 42 U.S.C. 290dd-2) and its implementing regulations (42 CFR part 2) establish federal standards that specifically impose additional confidentiality requirements on patient records that are maintained in connection with any federally-assisted specialized substance abuse treatment program. Because most alcohol and chemical dependency providers receive some sort of federal assistance or payment, the regulation is broadly applied. In addition, most providers in this field require a patient’s consent before disclosing clinical data due to ethical obligations. These heightened confidentiality requirements were imposed to address concerns that the potential stigma associated with certain health conditions (and, with respect to substance abuse, fear of prosecution) deterred people from entering treatment.[12]

## 1.2 STUDY PURPOSE

While the goal of these state and federal confidentiality standards is to ensure that those with health conditions that may subject them to discrimination and stigma get treatment, there is some concern that electronically implementing these standards will interfere with the exchange of health information in the context of a NHII. The requirements that individuals with certain "sensitive" health conditions have control over whether and with whom their health information is shared originated in a paper-based system. There is limited experience in the United States

[iii] Among its many duties, AHIC is specifically directed to advance and develop recommendations for the protection of health information through appropriate privacy and security practices HITSP is charged with assisting in the development of the NHIN by identifying and recommending privacy and security standards needed to accomplish specified use cases

[iv] The HIPAA Privacy Rule allows, but does not require, a provider to obtain an individual’s written permission to disclose health information for treatment, payment or health care operations. The Rule uses the term "consent" to describe written permission to disclose for these purposes. For many other purposes, the Privacy Rule requires a health care provider to obtain an individual's written "authorization." See 45 C.F.R. §§ 164.506 and 164.508.

with implementing individual control over health information in the context of an electronic health information system.
The Substance Abuse and Mental Health Services Administration (SAMHSA), HHS[v] commissioned this study to examine the current and proposed consent mechanisms being implemented in other countries (especially with respect to "sensitive" health information) in the context of their developing NHIIs.

This paper uses the term "consent" policies and practices when referring to policies and practices that govern whether and how individuals have the right to control when and how their health information can be shared with others. As used in this paper, the term "consent mechanism" refers to the method by which an individual can exercise such control.

## 1.3 STUDY METHODOLOGY

We selected for review three countries, Canada, England, and the Netherlands[vi] each of which:

- Is further along in the development of national health information infrastructure than the United States;
- Has substantial written materials concerning the country's consent policies and practices available in English;
- By law or policy grants its citizens some degree of control over the flow of their electronic health information for treatment purposes.

We examined each country's national health information infrastructure model and its current status; the country's consent policies; and their implementation (or planned implementation) of such policies. To put the discussion in the appropriate context we also briefly looked at the country's general health system structure.

We reviewed the published literature and websites for each of the pertinent countries on

- General framework for delivery of general health care and care related to sensitive health conditions such as HIV/AIDs, mental health and substance use
- Confidentiality laws and policies with respect to information related to these sensitive health conditions and treatment
- Confidentiality laws and policies with respect to general health information;
- General data exchange laws and policies, if necessary

[v] SAMHSA is devoted to building resilience and facilitating recovery for people with or at risk for substance abuse and mental illness.
[vi] We note that although Australia is widely recognized for its advancements in health information technology, it is currently in the process of re-evaluating its privacy framework. The National E-Health Transition Authority, a not-for-profit company responsible for establishing a new national health information management and information and communication technology, recently released a Privacy Blueprint for Unique Health Care Identifiers for comment. A separate blueprint setting out the consent model for the proposed Shared Electronic Health Record is currently being drafted. See *NEHTA's Approach to Privacy* vers. 1 (July 4, 2006) and *Privacy Blueprint-Unique Healthcare Identifiers*. Retrieved January 13, 2007, from http://www.nehta.gov.au/component/option,com_docman/task,cat_view/gid,141/Itemid,139/.

- General framework (or proposed framework) for countries' national health information infrastructure
- Technical implementation of laws and policies related to individual control (if any) over access to their health information for treatment purposes particularly with respect to identifiable information related to sensitive health conditions

In addition, we spoke with international health information technology experts.

We reviewed each country's consent mechanisms in terms of four generally recognized types of consent:

- General consent or "opt in." This is a blanket consent given by an individual for any health care professional working within a specified health context to access any and all of their health information for any purpose related to their care.
- General consent with specific exclusions or "partial opt out." The individual provides a general consent (or there is implied or deemed consent) but the individual withholds or denies consent in a limited fashion. For example, the individual can partially opt out of:
  - The disclosure of particular information or categories of information;
  - Disclosing information to a particular party or category of parties; or
  - Disclosing information for a particular purpose (e.g. employment)
- General denial with specific consent (partial opt in). This consent is similar to the prior category, but here the individual denies all access to their health data with the exception of:
  - Certain categories of their information (e.g., demographic details)
  - Identified parties (e.g., their general practitioner)
  - Disclosure for a specific purpose (e.g., in a medical emergency).[13]

We identified which form(s) of consent a country afforded its citizens with respect to sharing their health information for treatment purposes. Although there are countless other purposes for which health information can be shared, each of these purposes would require a separate analysis, which is beyond the scope of this paper.

We reviewed the choices individuals have with respect to the collection and disclosure of their clinical health information for treatment purposes. When the country permitted an individual to opt out (either wholly or partially) of sharing their health data, we also analyzed whether and in what circumstances the individual's choice could be overridden by a health care provider. Where information was readily available, we also reviewed whether an individual could withhold their personal information from the patient registries that record demographic information.

# 2 Canada Findings

## 2.1 FUNDING AND GENERAL STRUCTURE HEALTH CARE DELIVERY SYSTEM

Canada has publicly funded universal coverage for medically necessary physician and hospital services. This public funding accounts for 70% of healthcare expenditures in Canada. Basic services are provided free of charge. Management and delivery of health care services are the responsibility of the provincial and territorial governments. The provincial and territorial health plans receive funding from the federal government conditioned on their meeting federal policies and standards.[14]

Primary care providers such as general practitioners are generally the first point of contact for health care. The treatment of mental health as well as substance abuse addiction is provided in a variety of settings.[15] Testing and treatment for sexually transmitted diseases also takes place in a variety of clinical settings including GP offices, community family planning clinics, and community clinics devoted to STDs.

## 2.2 NHII

### 2.2.1 Overview

Canada's goal is to have an interoperable electronic health record (EHR) in place across 50 per cent of Canada (by population) by the end of 2009.[16] The EHR is envisioned as providing each of the 32 million people in Canada with a secure lifetime record of their key health history and care within the health system. The record will be available electronically to authorized health providers and the individual anywhere, anytime in support of high quality care.[17]

Canada Health Infoway, Inc., a not-for-profit corporation, whose members are Canada's 14 federal, provincial and territorial Deputy Ministers of Health, is coordinating the drive for a pan-Canadian EHR.[18] Infoway, which is funded by the federal government, works in collaboration with the provinces and territories, to establish the framework and standards for a pan-Canadian EHR based on interconnected regional systems. [19] Key elements of this framework are set out in the Electronic Health Record Solution Blueprint, revised in 2006.

Infoway has $1.2 billion in investment capital and expects to have spent 85% of this amount in electronic health information projects by March 2007.[20] Infoway strategically invests in nine key areas that contribute towards the development of a network of interoperable electronic health record systems across the country including: Registries (client, provider and service delivery location), Diagnostic Imaging Systems, Drug Information Systems, Laboratory Information Systems, Telehealth, Public Health Surveillance, Interoperable Electronic Health Record, Innovation and Adoption and Infostructure. As a strategic investor, Infoway participates in all project phases including planning, design, implementation and evaluation.[21] It does not, however, build health information systems or hold any health information.

On average, Infoway invests 75% of the planning and implementation costs for approved projects, with provinces and territories funding the balance.[22] Adherence with the Blueprint is one of the key criteria for a project's being eligible for Infoway investment.

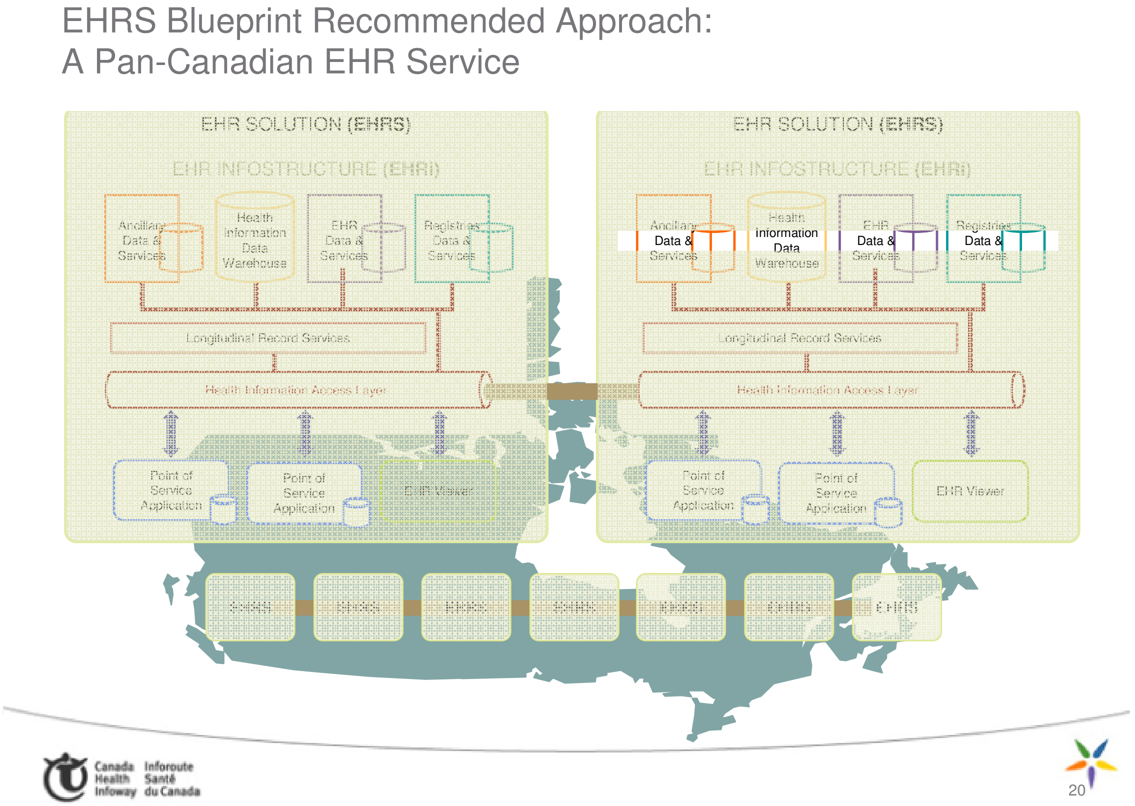
Architecturally, there will not be a central, national data base. Health information will generally be maintained and managed at the jurisdictional level (often the provincial or territorial level) in regional health information networks called Electonic Health Record Solution Infostructures (EHRi). These EHRi's will be interoperable; using a message based architecture, and will be interconnected across Canada.[23] The resulting EHR will be a "virtual" record consisting of information which, although maintained at various sources, is perceived by the user of the system as a single integrated record.

Point of service (POS) applications (e.g., applications used by doctors, hospitals or clinics) will push appropriate subsets of a patient's health data to the EHRi serving their jurisdiction.[24] The EHRi will maintain patient/client data in regional registries and data repositories. Each jurisdictional EHRi will be composed of:

- **Registry systems**, including **client registries** that contain current patient health identification numbers and demographic information (e.g., name, address, health insurance card number).[25] The client registry will also contain pointers to other jurisdictions' client registry entries if the client has presented for care and has been registered in the other jurisdiction.[26]
- **Domain repositories** each of which will store, maintain and manage specific clinical subsets of data including laboratory results and reports, prescription drug information (e.g., medications dispensed and allergic reactions), and diagnostic imaging (e.g., X-rays, and MRIs) [27]
- **Shared Health Record repository which will** maintain select clinically relevant data not otherwise maintained in specific domain repositories (e.g., encounter basic information, referral orders, and encounter summaries).[28]
- **Longitudinal Record Service,** of which a key component will be the **EHR Index**. The EHR Index will record summary information about patient clinical events recorded in the EHRi. It will maintain a sequential list of all events that affect the patient. It also will provide the location where the data relevant to each event is kept in the EHRi. It can also be used to trace the information about a specific event.[29]
- **Consent directive repository,** maintaining information concerning a patient’s consent directives (i.e., the granting, withholding or withdrawal of consent) for the collection, use or disclosure of identifiable health information in accordance with applicable privacy legislation and policies**.**[30]

POS applications interact with the EHRi (e.g., access EHRs) through a common access layer, which also serves as the connecting point between different EHRi's.[31] A diagram of the proposed infrastructure is provided below.

**Figure 1: Proposed Infrastructure**



EHRS Blueprint Recommended Approach:
A Pan-Canadian EHR Service

EHR SOLUTION (EHRS)
EHR INFOSTRUCTURE (EHRi)
Ancillary Data & Services
Health Information Data Warehouse
EHR Data & Services
Registries Data & Services
Longitudinal Record Services
Health Information Access Layer
Point of Service Application
Point of Service Application
EHR Viewer
EHR SOLUTION (EHRS)
EHR INFOSTRUCTURE (EHRi)
Ancillary Data & Services
Health Information Data Warehouse
EHR Data & Services
Registries Data & Services
Longitudinal Record Services
Health Information Access Layer
Point of Service Application
Point of Service Application
EHR Viewer
EHRS
EHRS
EHRS
EHRS
EHRS
EHRS
EHRS
Canada Health Infoway
Inforoute Santé du Canada
20

### 2.2.2 Privacy Laws and Policy in the NHII

In Canada, the privacy of personal health information is protected at the federal and provincial/ territorial level. At the federal level, the Privacy Act applies to information held by federal departments and agencies while the Personal Information Protection and Electronic Documents Act (PIPEDA) applies to private sector organizations (including most private sector health organizations[32]) that collect, use or disclose personal information during the course of commercial activity.[33] PIPEDA generally requires knowledgeable consent for the collection, use or disclosure of personal information.[34] The type of consent (e.g., express or implied) may vary depending on the circumstances and must take into account the sensitivity of the information.[35] Although health information is considered to almost always be "sensitive"[36] the federal Privacy Commissioner has recognized the principle of *implied consent* for health information to flow freely within the circle of care.[37] PIPEDA also confers the right to withdraw consent at any time, subject to the legal obligations of another party. Where a province enacts legislation that the federal government deems to be substantially substantive to PIPEDA, only the provincial legislation will apply to the collection, use or disclosure of information *within* the province. PIPEDA will still govern with respect to information that flows across provincial or national borders.[38]

Provinces and territories also have privacy laws (both general and specific to health information) that may impact the creation, use and disclosure of EHRs.[39] Four provinces, Alberta, Manitoba, Ontario, and Saskatchewan have health information statutes that apply to most organizations and persons that collect, use or disclose identifiable health information.[40] In addition British Columbia and Quebec have more generally applicable data protection laws that impact the collection, use and disclosure of health information.[41]

*Implied consent to disclose health information for treatment*

While these provinces base their privacy statutes on slightly different legal theories, they all permit the disclosure of health information for treatment without express consent, with the exception of Quebec which requires a patient's express permission to disclose health information for treatment purposes.[vii] [42]

*Individual right to withhold or withdraw consent (opt out)*

While express consent is not required to use or disclose health information for treatment in most provinces, individuals have the statutory right to partially opt out of (or limit) the disclosure of their health information for treatment. These statutory provisions are generally called ***"lockbox"*** provisions. The ability for an individual to restrict the use or disclosure of their electronic health information (whether pursuant to a statutory lockbox provision or an internal policy) may be implemented through ***"masking"***.[43] The right of individuals to mask their data varies from province to province.

One province, Saskatchewan, affords individuals only the right to opt out of access to and disclosure of their "comprehensive health record," essentially a "total opt out" right.[44] Other provinces such as Ontario and Manitoba provide the statutory right for an individual to wholly or partially restrict disclosure of their health information (total or partial opt out) but do not specify the type of health information or at what level of granularity individuals may restrict access. In contrast, Alberta only requires that a provider consider the express wishes of the patient in determining how much health information to disclose for treatment.[45]

In an attempt to harmonize these and other differing provincial and territorial privacy requirements, the Advisory Committee on Information and Emerging Technologies (ACIET) of the Federal/Provincial/Territorial Conference of Deputy Ministers developed the *Pan-Canadian Health Information Privacy and Confidentiality Framework*. An underlying principle of the Framework is that the collection, use and disclosure of PHI is to be carried out in the most limited manner, on a need-to-know basis, and with the highest degree of anonymity possible in the circumstances.

With respect to consent for disclosing health information for health care, the ACIET Framework generally provides as follows:

- There is implied knowledgeable consent to share health information within the circle of care (*i.e.* consent hinges on notice of practices).

[vii] British Columbia, Alberta, Manitoba and the Atlantic province use the “no consent” model, in which no consent is required to collect, use or disclose personal health information for treatment or care. Saskatchewan uses the “deemed consent model” in which the individual is deemed to consent to disclosure and may only opt out of access to and disclosure of his or her comprehensive health record. Ontario utilizes the “implied consent” model, which assumes that the patient gives consent unless the patient directs otherwise. Quebec is the only jurisdiction to require express consent to share health information for treatment and care.

- The individual has the right to withhold or withdraw their consent to share health information (opt out).
- The health care provider with custody of the health information must inform the individual of the consequences of any such restrictions
- The health care provider disclosing information which is incomplete must furnish notice to the receiving health care provider that information has been withheld if, in the opinion of the disclosing provider, the information is important for care and treatment.
- There must be the potential for a provider to override a withdrawal of consent in an emergency situation. [46]

This consent model was endorsed by all territories and provinces with the exception of Saskatchewan and Quebec. [47]

### 2.2.3 Consent Architecture and Mechanisms

Although Infoway has no mandate to develop privacy and security policy,[48] it is required to incorporate the protection of personal health information in all its activities in accordance with applicable laws and privacy principles, including provincial and territorial laws and policies.[49] Infoway achieves this by, among other things, ensuring that privacy and security are addressed in the projects it funds. Every project is required to conduct a Privacy Impact Assessment (PIA) that describes how the system will function and how it will address privacy rules in place in the jurisdiction.

In one of its key projects, Infoway worked with clinicians, business, and technology and privacy experts across the country to develop a conceptual privacy and security architecture (P&S Architecture) that can be used to build secure and privacy enhancing interoperable EHRs across Canada. The P&S Architecture presents a vision of a desired future state of how the EHRi should operate in years to come.[50] While the P&S architecture is designed to support the implied knowledgeable consent model of the ACIET Framework, it also supports alternative models of consent.[51] This flexibility means that jurisdictions can use the architecture to implement the privacy protective features that are consistent with their local legislative requirements.

Some of the key consent-related components of the conceptual P&S Architecture include:

- The potential to mask health data at the data element level
- The potential to mask health data from specific providers or electronic health record users
- The ability to override masking
- Consent directive repositories which will store individuals’ consent choices [52]

While some elements of the P&S Architecture are to be implemented in the future, masking functions are currently being utilized in several Canadian e-health projects.

#### *Three Provincial e-Health Projects*

Numerous projects that will form components of the pan-Canadian EHR are currently underway in every province and territory across Canada. These projects include picture archiving and communications systems to electronically capture x-rays, MRI's and CAT scans; pharmacy networks with comprehensive patient medication profiles and drug-to-drug interaction decision support; primary health care information management systems including interoperable health records and telehealth. The implementation of consent in these initiatives will vary depending on the jurisdiction's privacy law requirements and policies. Projects in three provinces that have implemented consent in varying ways are described below.

## 2.3 ALBERTA NETCARE PHYSICIAN OFFICE SYSTEM PROGRAM

### 2.3.1 Overview

The Alberta Physician Office System Program (POSP) is one component of Alberta Netcare, a set of projects overseen by the Ministry of Health and Wellness. Alberta Netcare is designed to create an integrated province-wide EHRi that will link physician offices, clinics, hospitals, pharmacies and other points of care to patient information. The EHRi currently includes Pharmaceutical Information System (prescription depository and related services) the Client Registry, and Laboratory Repository. [53]

The POSP is intended to help physicians move to electronic medical records so that their office systems can be integrated with the EHRi. The POSP provides physicians with partial funding for the implementation of information technology in their offices over a period of 48 months. POSP assists a full range of physicians from those who have little information technology to those who are ready to move to a comprehensive electronic medical record as a replacement for traditional paper-based charts. As of July 2006, 61% of Alberta physicians were receiving support through POSP to computerize their practices, with over 80% of these physicians being funded to transition to a comprehensive electronic medical record.[54]

To qualify for funding, physicians must use an office system that meets POSP vendor conformance and usability requirements (VCUR). Among its many functions, the system must be able to:

- Maintain demographic data;
- Generate daily reports;
- Provide prescription creation and printing and/or transmission at the point of care
- Provide access to a sufficiently powerful alert capacity to be able to identify major drug-drug interactions and potentially dangerous drug doses on prescriptions.
- With respect to the electronic medical record, the system must maintain the following information using discrete data elements:
  Allergy data
  Medication data
  Problem lists
  Diagnosis data
  Procedure data[55]

#### *System Access Controls*

The POSP requires users of the system to have a unique user ID and a password. The system uses role-based access that limits information accessible based on the individual's role in the office and the information they need to accomplish their job. The system creates an access log by user. The log includes failed access attempts as a means of identifying those who may be abusing the system. It requires two-factor authentication when communicating with an external system. It limits the ability to print a record by user and location. The system also provides end-to-end encryption when a physician accesses the system remotely.[56]

### 2.3.2 Privacy Laws and Policies

The primary law governing the use and disclosure of health information in Alberta is the Health Information Act (HIA), which applies to health service providers who are paid under the Alberta Health Care Insurance Plan to provide health services. HIA allows personal health information to be collected, used and disclosed for treatment and care without an individual's express consent.[57] HIA also permits a provider to disclose health information without consent if they believe on reasonable grounds that the disclosure will avert or minimize an imminent danger to the health or safety of any person. Under the HIA, in deciding how much health information to disclose, a provider must consider as an important factor any expressed wishes of the individual who is the subject of the information regarding disclosure, together with any other factors the provider considers relevant.[58]

Alberta has endorsed the ACIET Pan-Canadian Health Information Privacy and Confidentiality Framework which is based on implied knowledgeable consent to share health information within the circle of care coupled with the individual’s right to opt out.[59]

### 2.3.3 Consent Architecture and Mechanisms

Physician systems that have met the POSP VCUR are capable of implementing the consent model described below.[60]

#### *Clinical information*

**Recording clinical information**
No opt out. Patients of providers who use electronic medical records do not have the right to opt out of having their information recorded in an electronic medical record.

**Masking clinical information**
Opt out. Physician's systems must be able to mask a patient's record or a portion of their record that contains highly sensitive medical data. Masking can take place at the discrete data element level.[61]

As of April 2008, the systems must be capable of allowing individuals to allow or restrict access to their data for a specific health care provider, purpose or circumstance (*e.g.* emergency).[62]

**Override of masking**
The system must be able to override the restriction placed on access. The physician's system must have the capability to allow the override for a specified period of time and then to reapply the restriction automatically. The system must be able to log the override, including user id, date and time and the reason for the override. [63]

**Masking and drug interaction alerts**
As of April 2008, if a new prescription order or dispense interacts with a masked record (a masked drug, a masked condition or a masked allergy or intolerance) the system will promptly alert the person originating the information that there is a contraindication with a masked record.[64]

### *Demographic information*

**Recording demographic information**
Individuals *cannot* totally opt out of having their demographic information entered.

**Masking demographic information**
Through their physician, individuals may mask fields in their demographic record that contain highly sensitive information.[65]

### *Technical information*

A list of physician office system applications that have met the VCUR, along with the vendors who provide them is available on the POSP's website at http://www.posp.ab.ca/accepted/vcur-product-list.asp.

## 2.4 BRITISH COLUMBIA PHARMANET

### 2.4.1 Overview

PharmaNet is one of the British Columbia's key e-health projects. PharmaNet is a province-wide electronic network that links all BC pharmacies, as well as many emergency department physicians and medical practitioners in private practice to a central set of data systems, including a Client Registry. The data is maintained by the College of Pharmacists, BC on behalf of the Ministry of Health. PharmaNet supports drug dispensing, drug monitoring and claims processing. The system maintains:

- Patient drug profiles including all drugs dispensed during the last 14 months, drug allergies and clinical conditions, and patient demographics which include the personal health number, name, address, gender and date of birth.
- Drug information for pharmacists, patients, and drug interaction evaluation.
- Claim information including eligibility, coverage and deductibles. [66]

Pharmacies access Pharmanet through a private government high speed network, while medical practitioners can access the system through a commercial internet provider.[67]

Community pharmacies are the source of most of the data entered into the system including prescriptions filled, over the counter drugs used (at the pharmacists' option), and adverse events reported. Hospital out-patient pharmacies also send prescription information to the system. In-patient pharmacies do not normally add prescription information to the system but can send more limited information, such as patient adverse reaction information.[68] In addition, medical practitioners may also enter data including adverse events, dispensing of drugs (e.g., samples), and explanations of unusual dosages.[69]

### *System Access Controls*

All users must register with the Ministry for purposes of authentication. They must also sign a confidentiality agreement before being granted access to PharmaNet. Users must provide a unique ID and password when logging on to PharmaNet. Access is role based. For example, in a hospital, generally only emergency department physicians would be able to access PharmaNet. Access is also context based. For example, pharmacists can access medication information only in the performance of their professional duties. If a medication history is accessed when a prescription is not dispensed, the pharmacist must keep a record of the reason for the access. The system is designed to detect improper browsing.[70]

## 2.4.2 Privacy Laws and Policies

There is no specific health privacy legislation in British Columbia. The main statutes governing the privacy of information are the Freedom of Information and Protection of Privacy Act (FOIPPA), which applies to the collection use and disclosure of personal information (including health information) by public bodies and the Personal Information Protection Act (PIPA), which governs the private sector. The FOIPPA requires that individuals be given notice of the purposes for which their information is collected. It allows information to be used and disclosed in accordance with the purposes for which it was collected and for consistent purposes. [71] The Ministry of Health, as a public body, is subject to the FOIPPA.[72]

The PIPA permits the collection, use and disclosure of information with the individual's express consent. Providers can also rely on implied consent to disclose the individual's information for treatment provided the individual is given adequate notice and the opportunity to object. [73] Most medical practitioners and pharmacists would be subject to PIPA.

To address concerns with respect to potential access to PharmaNet data, the Pharmacists, Pharmacy Operations and Drug Scheduling Act specifically limits the classes of individuals who have access to PharmaNet data to pharmacists, as well as medical practitioners and certain other persons designated in regulation.[74]

British Columbia has endorsed the ACIET Pan-Canadian Health Information Privacy and Confidentiality Framework which is generally based on implied knowledgeable consent to share health information within the circle of care coupled with the individual's right to opt out.[75]

## 2.4.3 Consent Architecture and Mechanisms

Community pharmacists generally act as the "gatekeeper" for individual's interaction with PharmaNet. Individuals can request a printed copy of their personal data stored on PharmaNet through their local pharmacy, which will submit the request to the College of Pharmacists for action. They can also request that their medication record be assigned a keyword through their pharmacist. The keyword masks the record. Once the keyword has been set, the record is generally inaccessible unless the patient provides the keyword. Keywords can be changed and removed by the community pharmacist.[76] The details of the operation of these consent mechanisms are further detailed below.

## *Clinical information*

### Recording clinical information

No opt out. All prescription medications dispensed by community and in-house hospital pharmacies in BC must be recorded on the PharmaNet central database. Individuals cannot opt out of having their information included. [77]

### Accessing clinical information

The consent model by which a provider can access a patient's prescription medication record varies by the category of provider.

**Pharmacists.** Implied consent. Pharmacists have implied consent to access a patient's prescription drug information maintained on PharmaNet.[78]

**Emergency department physicians.** Implied consent. Emergency department physicians may access a patient's prescription drug data under implied consent. However, the emergency department must post a notice telling patients that authorized staff may access their PharmaNet medication profile.

Emergency department physicians can view and can retain an electronic or printed copy of the medication profile. The print out must either become part of the patient's chart (and must be treated with the same confidentiality considerations as with other highly sensitive, confidential information), or be destroyed. [79]

**Medical practitioners.** Express consent required. Medical practitioners must have the patient's written consent to access their prescription drug information maintained on PharmaNet.[80]

Practitioners can retain an electronic or printed copy of the medication profile, which must either become part of the patient's chart (and treated with the same degree of confidentiality as other confidential health information) or be destroyed.[81]

### Masking clinical information

Individuals can restrict access to (mask) their prescription data by asking their pharmacist to attach a keyword to the individual's records. The pharmacist transmits the request to the central PharmaNet database where the actual masking takes place. Individuals can also request that their keyword be changed or removed through their pharmacist.[82]

**Override masking with permission (shared secret).** With the keyword in place, only those pharmacists and physicians with whom the individual shares the keyword can access their records. This is generally called a "shared secret." [83]

**Pharmacists.** The patient can give a pharmacist their keyword to access their masked data. The pharmacist is allowed to store a patient keyword on the local system if the patient gives consent. This affords the pharmacist chosen by the patient easy access to the patient's records. The pharmacist cannot share the keyword with others (e.g., other pharmacists) even if they are sharing patient information. This restricts access to the patient's record and medication profile to the pharmacist(s) chosen by the patient.[84]

**Emergency department physicians.** The patient can give an emergency department physician access to their masked record by giving the emergency department physician the keyword (the shared secret).

- **Duration of access.** ED physicians are permitted to store the patient's keyword on the local system for use within the same treatment period if the patient gives their consent. Keywords cannot be shared among providers sharing patient information. This restricts access to the patient's record and medication profile to provider(s) chosen by the patient and therefore protects their right to privacy. [85]

- **Retention of unmasked information.** Retaining and printing an unmasked record appear to be governed by the same rules that apply to records that are accessed through regular means: *i.e.*, The ED can retain an electronic or printed copy of the medication profile. The print out must either become part of the patient's chart (and must be treated with the same confidentiality considerations as with other highly sensitive, confidential information), or be destroyed.[86]

▫ **Medical Practitioners.** A patient can give a medical practitioner their keyword in order for the medical practitioner to access their masked PharmaNet record.[87]

- **Retention of unmasked information.** Retaining and printing an unmasked record appear to be governed by the same rules that apply to records that are accessed through regular means: *i.e.*, Practitioners can retain an electronic or printed copy of the medication profile, which must either become part of the patient's chart (and treated with the same degree of confidentiality as other confidential health information) or be destroyed.[88]

**Override of masked information in emergency (without patient permission)**

- **Emergency department physicians.** Emergency department physicians may override the keyword if the patient requires urgent medical care and is unable to remember or communicate their keyword. The physician must contact the PharmaNet Help Desk to have the keyword reset. They then must notify the patient within a reasonable period of time that this action has been taken to ensure that the patient is aware that their keyword has been reset and that they will need to re-establish a new one if they so desire.[89]

  - **Logging of override.** When a keyword is reset in this way the PharmaNet Help Desk records the name and College of Physicians and Surgeons ID number of the physician requesting the reset as well as the name of the person calling on behalf of the physician.

The College will notify the patient, in writing, that their keyword was reset as a result of their emergency room department visit.[90]

- **Medical practitioners.**
  General medical practices do not have the authority to override keywords.[91]

#### *Demographic information*

PharmaNet maintains its own patient demographics, which are synchronized with the British Columbia Ministry of Health centralized Client Registry System. The centralized Client Registry System maintains the following information on every person who receives health services in the province: name, address, gender, date of birth and personal health number (PHN). Entry of telephone number is optional. It is not clear from publicly available documents whether demographic data can be masked.[92]

#### *Technical information*

PharmaNet Professional and Software compliance standards are available at http://healthnet.hnet.bc.ca/catalogu/tech/pnetcompdocs.html

## 2.5 ONTARIO DRUG PROFILE VIEWER (DPV) SYSTEM

### 2.5.1 Overview

One of Ontario's key e-health projects is the Emergency Department Access to Drug History Initiative. The initiative provides a province-wide electronic information system, known as the Drug Profile Viewer (DPV) System. The DPV enables the Ministry of Health and Long Term Care to share with providers the prescription drug claim histories of patients who receive benefits through the Ontario Drug Benefit Program, which covers seniors, and through the Trillium Drug Program, which assists people who have high prescription drug costs in relation to their income (collectively referred to as ODB). [93] It was scheduled to be fully implemented in 183 hospitals by the end of 2006.

Emergency department staff will be able to view the names, dosage forms, strengths, and quantity of the drugs which have been prescribed to a patient through the ODB program. In addition, the prescriber and pharmacy information for these drugs will be displayed. Because the DPV system only provides access to ODB prescription claims history, providers are advised that the data available:

- Does not include medications obtained from other sources, such as over the counter drugs
- Includes only that portion of data claims information that the patient has consented to release
- May include information related to claims for prescriptions that were submitted but never picked up. [94]

The claims information is stored on a central database and is accessed by emergency departments in Ontario hospitals which are connected to the Smart System for Health Agency (SSHA) secure network, an IP-based managed private network with secure Public Key Infrastructure and authentication. Each hospital must enter into a data access agreement with the Ministry to participate. The DPV System will be maintained and operated on an ongoing basis under the direction of the Ministry. [95]

#### *System Access Controls*

All users of the DPV System must be identified, registered, and have proper authorization to gain access to ODB and TDP drug claims history. In addition, the Ministry will maintain a record of each authorization that is granted to view an ODB recipient's drug claims history at an emergency department and furnish a copy of the list to the recipient upon their request.[96]

### 2.5.2 Privacy Laws and Policies

The use and disclosure of health information by private and public entities in Ontario is governed by the Personal Health Information Protection Act (PHIPA), which has been deemed to be substantially similar to PIPEDA.[97] PHIPA uses a knowledgeable implied consent model, which permits a provider to assume that he or she has the individual's consent to collect, use or disclose the information for the purpose of providing health care.[98] Implied consent is conditioned on the individual's knowledge of the intended use and disclosure of the information collected and their right to withdraw consent. Knowledgeable consent is generally achieved by the provider's posting or furnishing appropriate notice of the intended use and disclosure of the information and the individual's right to withdraw their consent.[99] The individual has the right to totally or partially withhold or withdraw their consent.[100] If the individual limits disclosure of their health information and the creating provider believes that disclosure of the masked information is reasonably necessary for the receiving provider to provide care, the creating provider must notify the recipient that they are not receiving all of the individual's health information.[101] Providers have the right to override the individual's restriction in very limited circumstances to eliminate or reduce a significant risk of serious bodily harm to a person or group of persons.[102]

Ontario has endorsed the ACIET Pan-Canadian Health Information Privacy and Confidentiality Framework which is based on implied knowledgeable consent to share health information within the circle of care coupled with the individual's right to opt out.[103]

### 2.5.3 Consent Architecture and Mechanisms

#### *Clinical information*

**Recording clinical information**
No opt out. ODB recipients' prescriptions are automatically recorded by the Ministry of Health, the agency overseeing the program. Recipients of ODB benefits may not opt out of having this information recorded and stored in the central database.

**Accessing clinical information**
The Ministry of Health relies on implied consent to disclose drug claims history to authorized emergency department personnel for the purpose of providing health care.[104]

**Masking clinical information**
Individuals are encouraged to consult with a healthcare provider about the benefits of disclosing their drug claims history to emergency departments at which they seek treatment and the potential health risks of fully or partially withdrawing consent. However, if the individual determines that they want to withdraw their consent, they may do so. A decision to withdraw consent will not affect an ODB recipient's eligibility to receive ODB or TDP benefits or any other health care service funded by the Province of Ontario.[105]

Individuals can withdraw their consent (opt out) either fully or partially of having their prescription drug information disclosed.[106] Forms for withdrawing consent and reinstating consent are available on the Ministry's website or by calling the Ministry. The individual receives notice when their request has been acted upon. [107] The details for masking information are described in detail below.

**Full masking of prescription drug claims history**
An individual who does not want a*ny* of their drug claims history disclosed to an emergency department can opt out by withdrawing their consent. The recipient must file a *Full Withdrawal of Consent Form* with the Ministry.[108] The individual's entire record is masked at the central database maintaining ODB/Trillium prescription information.

**Flag that data is not available**

When an emergency department provider electronically requests masked data, they receive a flag (notice) that drug information is not available either because the patient is not an ODB recipient or because the patient may have withdrawn their consent.[109]

**Partial masking of prescription drug claims history**
An individual can partially opt out by identifying specific drugs they do not want to be disclosed. The individual must submit a *Partial Withdrawal of Consent Form* with the Ministry. Only the identified drugs are masked. Individuals may change the list of drugs they want withheld at any time by submitting a new list and a new Partial Withdrawal of Consent Form. [110]
Providers using the system have been given general notice that the drug information that is accessible thought the DPV is only that portion of the drug claim information that the patient has consented to release.[111]

**Unmasking information (reinstating consent through normal channels)**
An individual can reinstate their consent and unmask their data through normal channels by submitting a *Consent Reinstatement Form* with the Ministry.[112]

**Override masking with permission (shared secret)**
An individual may be able to temporarily reinstate consent during their visit to the emergency room. To do this, the patient or their substitute decision maker must communicate their wishes to reinstate consent to the emergency department staff and the staff must have access to the patient's health number. Generally, the provider can obtain the individual's health number from their health card or, with the patient or substitute decision maker's written permission, from the Ministry. The patient's health number acts as a "shared secret" to provide temporary access to the otherwise masked data. [113]

**Duration of override**
The override lasts the duration of the ED visit.[114]
**No selective override**
If the patient reinstates their consent in the emergency department, the staff will have access to all of that patient's ODB drug claims history. The patient cannot selectively choose which information to unmask in this situation. [115]

**Retention of unmasked information**
It is recommended that the emergency department copy the patient's drug history and include it in their record when they are admitted to the emergency department.

**Number of recipients who masked data**
Out of over 1.5 million ODB and Trillium recipients, only 508 fully withheld consent and 11 partially withheld consent from June 2005 through February 2006.[116]

# 3 England Findings

## 3.1 FUNDING AND GENERAL STRUCTURE OF HEALTH CARE DELIVERY SYSTEM

England has a universal, publicly funded health care system. A wide range of services, largely free at delivery, is provided by the National Health Service (NHS), the largest health care organization in Europe. The National Health Service accounts for 88% of healthcare expenditures in the United Kingdom.[117]

Ten Strategic Health Authorities (SHAs) manage the NHS locally and are responsible for, among other things, developing plans for improving health services in their local area, and ensuring the quality of local health services. The SHAs oversee a variety of trusts (e.g., Primary Care, Acute Care, and Mental Health Services Trusts) each of which pays for and monitors a different class of health care in their region.[118]

While GPs generally serve as the gatekeepers for care, individuals can be treated by a number of different health care providers. Mental health services, for example, are provided in a wide range of settings from GPs or other primary care services, community services to hospital wards.[119] Furthermore, individuals can self-refer to sexual health clinics, which are required to maintain confidentiality and do not, as a matter of course, share information with the patient's GP.[120]

## 3.2 NHII

### 3.2.1 Overview

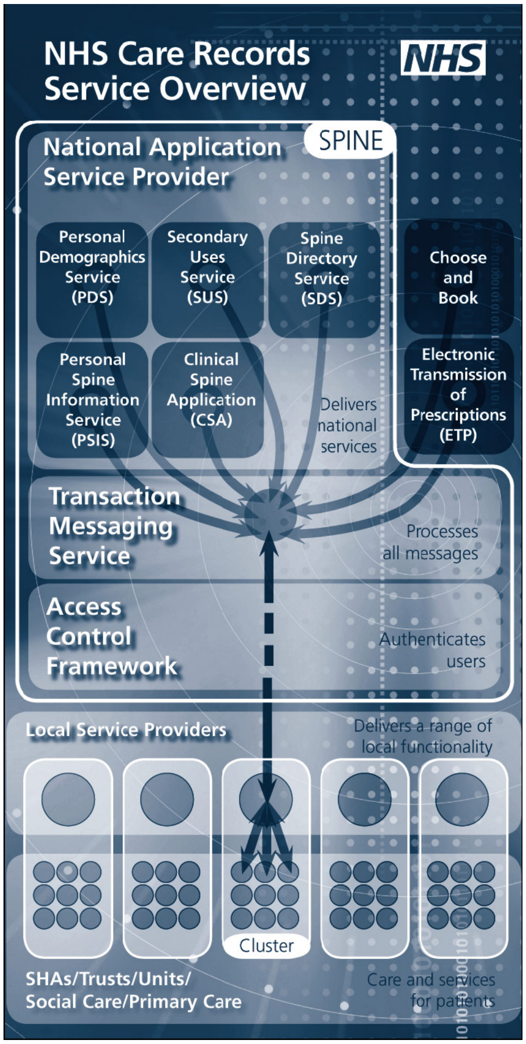
England is developing a centralized nationwide health information exchange infrastructure to support the NHS. The project, the National Programme for Information Technology (NPfIT), was launched in 2002.[121] Once fully operational, the new IT infrastructure will connect more than 100,000 doctors, 380,000 nurses and 50,000 other healthcare professionals, as well as give 50 million patients access to their health information.[122] Its size and complexity make it the largest health information technology program in the world.[123] According to the National Audit Office, Connecting for Health now projects that NHS's 10-year expenditures on the program will be £12.4 billion (2004-5 prices).[124]

Connecting for Health, an agency of the Department of Health is responsible for the central management and administration of the NPfIT. Local IT procurement and management is handled through 5 geographic clusters, each of which comprises 1-2 SHAs working in concert. Each cluster has chosen a Local Service Provider (an information technology vendor) to deliver IT services in its respective part of the country.[125]

#### *Electronic Patient Records*

Over 90% of GP offices in England are computerized. Estimates vary widely on the proportion of GPs that use electronic patient records, perhaps due to different definitions of the term. However, there appears to be agreement that only a small percentage of these systems have the capacity to share information with clinicians outside their practice.[126]

**Figure 2: NHS Care Records Service Architecture**


NHS Care Records Service Overview
NHS
National Application Service Provider
SPINE
Personal Demographics Service (PDS)
Secondary Uses Service (SUS)
Spine Directory Service (SDS)
Choose and Book
Personal Spine Information Service (PSIS)
Clinical Spine Application (CSA)
Delivers national services
Electronic Transmission of Prescriptions (ETP)
Transaction Messaging Service
Processes all messages
Access Control Framework
Authenticates users
Local Service Providers
Delivers a range of local functionality
Cluster
SHAs/Trusts/Units/ Social Care/Primary Care
Care and services for patients

Source: Connecting for Health, NHS

To remedy this situation, the core of the NPfIT will be the NHS Care Records Service, which is intended to create an electronic patient record for every NHS patient and to make electronic summaries of those records available nationally by 2010.[127]

Care Records will be made of a number of components, including:

- The Detailed Care Record. The Detailed Care Record contains the detailed records of patient encounters and care and is to be accessible locally.
- The Summary Care Record. The Summary Care Record will be a summary of essential clinical health information that is available nationwide. It is intended to be used for out-of-hours care, accident and emergency care, treatment of patients who are traveling out of their region and for less complex care across organizations. [128] Eventually, the Summary Care Record will contain a patient's essential clinical health information such as major

diagnoses, procedures, current and regular prescriptions, adverse reactions, and drug interactions.[129]

- Personal demographic data (*e.g.*, name, address, gender, NHS number, date of birth, consent preferences).[130]

Detailed Care Records will be maintained locally. Each geographic cluster will have one or more regional data center(s) run by the cluster's Local Service Provider. Each cluster data center will maintain the Detailed Care Records of the providers in its region. Subject to patient approval, Detailed Care Records are potentially available to other providers within the cluster. For example, when a GP refers a patient to a hospital, the hospital may be able to access the relevant parts of the GP's detailed records.[131] Cluster data centers are not directly linked to each other.

Essential information in the Detailed Care Record is automatically uploaded to form the Summary Care Record. The Summary Care Record and personal demographic data will be maintained in a central national database and messaging center called the Spine. The data are maintained in separate applications, the Personal Demographics Service and the Personal Spine Information Service, but are linked by a unique patient identifier, the NHS Number. In addition to summarizing essential health information, the Summary Care Record will also provide links to data in the Detailed Care Record. Summary Care Record and PDS information will be available nationwide using a high speed broadband intranet called N3. [132]

Patients will have access to their own Summary Care Record through NHS HealthSpace. An initial version of HealthSpace already exists as a personal health organizer which allows people to note personal information about their health, use Choose and Book services to book appointments, and keep a calendar for appointments. Over time the services it provides will expand to provide patients with a link to their NHS Summary Care Record. [133]

### *Status of NHII*

There has been steady progress in the development of the Care Records Service. The Personal Demographics Service, which was initially populated from a database used to trace NHS numbers for patients, went live in June 2004. As of August 2006, PDS was being accessed by over 250,000 users in conjunction with selected NPfIT services including Choose and Book and Electronic Prescription Services.[134]

As of December 2006, over 98% of England's GP offices have been connected to the N3 national broadband network.[135] However, most GP office systems have not yet met the specific requirements for being eligible to participate in the Care Records Service, including being able to generate Summary Care Records. Connecting for Health has initiated a program to encourage GPs to move to compliant systems or up grade their existing systems to bring them into compliance. Under this scheme, which is subject to Department of Health and HM Treasury approval, GPs will receive IT funding based on their achieving progressive compliance levels, including moving (or upgrading) their practice systems to systems that are Spine-compliant, and migrating their records to the cluster data center serving their region. [viii] The target date for the commencement of this program is April 2007. [136]

### Access and Audit Controls

Access to the electronic health records will be controlled in three ways:

- **User authentication.** A Smartcard with photographic ID and pin number must be used every time an NHS employee logs onto the system.
- **Role based access control.** Anyone accessing a patient's record will have access to only as much information as they need to know for the purpose of the job role they are performing. Job roles will be defined centrally and assigned locally.
- **Legitimate relationships.** Anyone accessing a patient's record is required to have a "legitimate relationship" with that patient, so a clinician will not normally be allowed to access the record of a patient not under their care. Systems will automatically construct a legitimate relationship when a patient is referred to another health care professional. In exceptional circumstances, care professionals will be able to create a legitimate relationship with a patient without referral or consent: for example, an emergency clinician treating an unconscious accident victim. [137]

The system will also ensure confidentiality through the use of alerts and audit trails. The organization’s privacy officer will be alerted where there is a question about the appropriateness of user access. In addition, an audit trail will be established on each and every occasion that a patient's medical records are accessed. Patients will have the right to request a copy of the audit trail.[138]

The NHS is scheduled to pilot the Summary Care Record in spring 2007, with tentative plans to implement it nationally in 2008. At that time, it will also pilot patient access to the Summary Care Record through HealthSpace with a small group of patients.[139]

## 3.2.2 Privacy Laws & Policies

Health information in England is primarily protected under the Data Protection Act, Human Rights Act, common law duty of confidence, and professional ethical standards. The Data Protection Act uses an implied consent model for the use and disclosure of health information for treatment, and includes the right of the individual to object to disclosure.[140] The British Medical Association has consistently taken the position that pursuant to medical ethics, express consent should be obtained for the sharing of health information in an electronic national system.

As the NPfIT has progressed, major concerns regarding the confidentiality and potential accessibility of patient information have been raised and remain a matter of controversy.[141] To resolve some of these concerns, the Care Record Development Board released the Care Record Guarantee, which sets out the general rules that will govern information held in the NHS Care Records Service when it goes live. This guarantee will be updated every 12 months to reflect changing circumstances.

[viii] According to the National Audit Office, 500,000 patient records are being converted and cleansed every month. National Audit Office, United Kingdom, *The National Programme for IT in the NHS* (June 16, 2006).

Some of the key principles of the 2006 Care Record Guarantee include:

- Those involved in a patient's care will have access to the patient's health records. The information will be limited to what the person needs to perform their health care role.
- The patient can choose to limit how NHS shares the information in their electronic care record.
- NHS generally will not otherwise share identifiable health information unless:
  The patient requests that they do so
  The patient gives their specific permission
  It is required to share by law
  It has special permission for health or research purposes
  Has special permission because the interests of the public are thought to be of greater importance than the patient's confidentiality (e.g., reporting an infectious disease)
- Patients will be able to check their own care records and ask for factual inaccuracies to be corrected.[142]

The Care Record Guarantee also provides that in the future, people who are concerned about particular entries in their record can ask that they be kept from general view (partial opt out). In England, the mechanism for limiting access to data is called "sealing" data or using a "sealed envelope."[143]

### 3.2.3 Consent Architecture and Mechanisms

Electronic care records will consist of Detailed Care Records, to be maintained locally, and Summary Care Records which will be maintained in the Spine, the national database, and be available to NHS providers throughout the country.[ix] The creation and content for each of these two types of records is described first, followed by a discussion of "sealing," the consent mechanism to be used for both types of records. The development of the policies surrounding these records is an ongoing process and subject to change.

#### 3.2.3.1 Detailed Care Records

Since GP records will be the first components of the electronically shared Care Record, the following discussion is limited to those records.

##### *Clinical Information*

**Recording clinical information**
No opt out of recording clinical information. Patients will *not* have the right to prevent their GP from making a detailed record of their treatment. This is because the clinician is required, under professional rules, to keep a record of the consultation and the treatment the patient receives.[144]

[ix] The discussion on the developing consent architecture and mechanisms with respect to the Care Records Service appears to have primarily focused on the Summary Care Record.

**Electronically sharing clinical information**
Potential opt out. Currently, it is expected that patients will have the right to request that all Detailed Care Records held by clinicians be held nondigitally in paper format or in an electronic system that is not connected to the wider NHS system (*i.e.*, opt out of having their information potentially available through the NHS electronic Care Record Service).[145]

**Limiting access by provider category**
It has been proposed that patients have three levels of choice with respect to *sharing* their locally maintained Detailed Care Records with providers. The patient will be able to grant access to their care records to:

Only the treating physician
Only organizations involved in their care
To the entire system.[146]

These access controls will be augmented by the "sealed envelope" which will allow a patient to identify a particular part of their record and seal it off from access. [147] Sealed envelopes are described in more detail below.

#### 3.2.3.2 Initial Summary Care Records

This section describes content and patient controls of access that will be utilized in the initial phase of introducing Summary Care Records.

**Content of Summary Care Record**
Because the technology for sealed envelopes will not be available during the early adopter pilot projects in spring 2007, it has been determined that the initial Summary Care Record should only contain "non-sensitive" information. Accordingly, only information about current medications and suspected adverse and allergic reactions to medications will be included in the initial Summary Care Records. Furthermore, the initial upload of information will come solely from records originating in GP clinical computer systems.[148]

**Creating a Summary Care Record**
Express and implied consent. The issue of patient consent with respect to the Summary Care Record has been a matter of debate. In very general terms, the British Medical Association and the Ethics Committee of the Royal College of General Practitioners have taken the position that the creation of a Summary Care Record for a particular patient should require that patient's explicit consent. In contrast, the Department of Health has taken the position that an opt-out approach is appropriate.[149] After considerable consultation, the stakeholders agreed to the following scheme for patient consent for the early adopter pilots. A Summary Care Group Advisory Group will oversee the issues that may arise in the pilot project (including consent) and address potential resolutions.[150]

**Notice of creation of Summary Care Record**
There will be a public information campaign to alert people to the plan to undertake the generation of Summary Care Records. The public information campaign will alert patients that they have a specific timeframe in which to view their proposed summary and to set limits on sharing, should they wish to do so. As each practice goes live, a

text-only Summary Care Record will be extracted from the GP database for each patient on the database. Patients will be able to review their summary via HealthSpace or by requesting a print-out of their summary from their GP.[151] Patients will be invited to correct or amend their record at this point.

**Choice re creation of Summary Care Record**
Express and implied consent. Patients will have the choice whether to have their clinical information uploaded to the national database to create a Summary Care Record. After the public information campaign, they will be invited to give their permission for the creation of a Summary Care Record.[152]

Individuals who, after a realistic period of time following the public information campaign notice, have not reviewed their record will be presumed to have given their *implied consent* for their Summary Care Record to be created and shared in appropriate circumstances.[153]

The Summary Care Advisory Group is to consider the issue as to how to implement these rights.[154] The possibility of opting out of the creation of a Summary Care Record (available nationally) but not the shared Detailed Care Record (available regionally) remains an open issue.[155]

**Sharing of the Summary Care Record**
Total opt out. Individuals will be able to allow the creation of a Summary Care Record but *opt out of sharing* the record. The patient's PDS would show "no data sharing" and only clinicians inside the GP workgroup would be able to view the data.[156]

#### 3.2.3.3 Subsequent Summary Care Records

Subsequent to the initial text-based Summary Care Record, a coded Summary Care Record will be generated and uploaded to replace the text version.[x] With the introduction of coded summaries, patients will have the following *additional* opportunity to limit access to their clinical health information.

**Content of coded Summary Care Records**
Opt out of including data in Summary Care Record. With the introduction of coded summaries, a compliant GP system will indicate to a clinician what information would normally be included in a summary. The GP then has the ability to easily mark/unmark entries for inclusion or exclusion in the summary. This will allow the Summary Care Record to be refined pursuant to patient request. Information that is not included in the summary will not be available to providers outside the GPs workgroup.[157]

[x] When data are "coded" the data are transmitted and stored as codes, but the person viewing the record will see the rubrics derived from those codes.

### 3.2.3.4 Sealing and Sealing and Locking Information

The NHS is committed in the future to enabling patients to limit access to sensitive information within their records. The patient will be able to request that specific sensitive information within their clinical record is accessible only with their consent. Because this masking feature is often referred to as "sealing," (or using a "sealed envelope") in England, we use those terms in describing them in this paper.

#### *Overview*

Under current plans, patients will be able to opt to have sensitive information "sealed". Patients will also be able to impose an addition layer of control on their records by requesting that they be "sealed and locked." When a record is sealed and locked, no one beyond the provider who generated the information and members of that provider's health care team (workgroup) will be able to access the information. The following section describes some of the elements that are common to "sealed" and "sealed and locked" records. Because consent mechanisms are implemented in slightly different fashions with "sealed" and "sealed and locked" information the specifics for these two means of masking are described in separate sections below.

**Status of sealing mechanism**

NHS Connecting for Health contracts with contractors involved in developing the NHII originally specified high-level "sealed envelope" requirements. Detailed sealing requirements were developed and revised in response to patient representative and clinician feedback. The detailed sealing requirements explained below are summarized from the NHS "Sealed Envelopes" Briefing Paper: "Selective Alerting Approach," drafted in late 2006.[158] These requirements are still being developed and may change.

Although some provider software already provides some patient sealing functionality, wide-spread sealing functionality along the lines described below is expected to become available in 2008-9.[159]

**Notice to patient of consequences of sealing or sealing and locking**

Patients must be advised of the potential implications that may result from specific decisions to restrict access. Sealing, and even more so sealing and locking, introduces the risk that:

inappropriate treatment options are offered to the patient; or
appropriate treatment options are not offered to the patient.

**Right to seal or seal and lock information and exception**

If a patient with mental capacity understands that their request to seal or seal and lock their information may be harmful to their health, and despite this still wishes to go ahead, then under common law, the patient's decision should be respected and the provider must seal the information. Clinicians will be able to, and will be advised to, record their concerns about such decisions. However, a request may be refused where it could impact adversely on the health and welfare of others.

**Duration of sealing/locking information**

When a patient seals, or seals and locks, data the restrictions will apply until the patient changes their mind or dies.

**Decision support and sealed/sealed and locked information**
The mechanisms for how the sealed envelope systems will operate with decision support software are still being developed.

**No policy limits on type of clinical information that can be sealed/sealed and locked**
Generally, patients will be able to seal or seal and lock any part of their Summary Care Record or Detailed Care Record except demographic information. The right to seal is not limited to specific types of information such as those typically associated with potential stigma and discrimination.

**Technological limits on type of clinical information that can be sealed/sealed and locked**
All entries in the Summary Care Record will be "sealable." However, it will not be possible to seal certain types of data in the Detailed Care Record. For example, parts of images such as a letter that has been scanned into the system will not be "sealable." It is also expected that there will be standard units of clinical data that can be sealed (such as standard clinical messages) and it would not be possible to seal components of those standard units.

### *Sealed Information*

**Flag that record contains sealed information**
When someone attempts to access sealed information a flag (an icon with a message) appears warning them that the information they are attempting to access has been sealed. The flag only appears when that part of the record that is sealed is being accessed. The content of the message varies with the entity attempting to access the record.

> **Author and workgroup.** When the provider who created the information (the author) or his workgroup attempt to access sealed data, a flag (an icon) appears advising them that are attempting to access sealed data and instructing them how to view it.
> **Others outside the workgroup.** When anyone outside the workgroup attempts to access the "sealed" information there will be a flag telling them that the information is only available for view with the patient's permission. The message also instructs them how to override the seal and cautions them that if they do so an alert will be sent to the organization's privacy officer.

**Access to sealed information**

> **Author and workgroup.** The author and members of his workgroup with role-based access permission will be able to access the sealed information. They will not need to override the seal.
> **Others outside the workgroup.** Those outside the workgroup generally may not access the information without the patient's permission.

**Override of sealed information with patient's permission**
A provider outside the author's workgroup can override the seal with the patient's express permission.

**Override of sealing without patient's permission**

A provider outside the author's workgroup generally cannot override the seal without the patient's permission. If the patient has sealed data and it is not practical to ask permission to view that data then access must be justified through one of the following reasons:

Public interest;
Access is required by statute; or
A court order demands access

Best interest of the patient is not sufficient on its own to justify access, even if the patient is unconscious.

A public interest defense will be applicable very rarely. It relies on the clinician being able to justify the breach of patient confidence in the interests of the public, such as a genuine risk that specific individuals, or the public in general, will be harmed if the clinician is unable to see the withheld information within the patient's record.

The above list is subject to further legal analysis and may change.

### *"Sealed and Locked" Information*

Information which is "sealed and locked" has an additional layer of protection.

**Flag that record contains information that has been sealed and locked**

**Author and workgroup.** When the provider who created the information (author) and members of his workgroup attempt to access sealed and locked information a flag (an icon with a message) appears warning them that the information they are attempting to access has been sealed and locked. The flag also advises them of the steps to take to access the sealed and locked information.

**Others outside the workgroup.** No flag appears to those outside the provider and his workgroup.

**Access to sealed and locked information**

**Author and workgroup.** The author and those in his workgroup with role based access would be able to access the sealed and locked information.

**Others outside workgroup.** No one outside the workgroup will be able to access the sealed and locked information. They will not know that it exists.

### *Consent Mechanisms for Personal Demographics Service*

**Inclusion in PDS**

No opt out. NHS patients do not have the right to opt out of having their information included in the national Personal Demographics Service.[160]

### Concealing vulnerable data

Patients' whose demographic data may be particularly vulnerable (*e.g.*, victims of domestic violence, adoption cases, or those in a witness protection program) may have their details "stop noted". In these cases the patient's address, telephone numbers and GP registration will not be generally available through the PDS.[161] The PDS will include a sensitive record indicator which indicates that "the record is not accessible to PDS users or the content of the record is being reviewed to ensure the data is correct."[162]

# 4 The Netherlands

## 4.1 General Structure of Health Care Delivery System[xi]

The Netherlands has recently moved to a private health care system for its 16.5 million citizens. As of 2006, basic primary and secondary care ("care with intent to cure") health insurance is compulsory for all residents. Private insurers are obligated to accept every resident in their coverage area and to offer a standard premium with a standard benefits package. The government pays a premium subsidy based on income for those who cannot afford the standard premium. Long term care and uninsurable medical risks are funded by government under the Exceptional Medical Expenses Act.[163]

Patients must register with a primary care physician, who acts as a gatekeeper to the health system. Family physicians must give their approval before patients can access hospital and specialist care. There are local clinics for treating sexually transmitted disease which do not require GP referral. Mental health and substance abuse treatment can take place in a variety of settings including GPs, private practices, outpatient clinics, health centers for drug and alcohol abuse, regional institutions for ambulatory mental health and general psychiatric hospitals. [164]

## 4.2 NHII

### 4.2.1 Overview

The development of the NHII in the Netherlands primarily is being conducted under the guidance of the National IT Institute for Healthcare (Dutch acronym: NICTIZ),[xii] a foundation made up of government and private organizations involved in IT and healthcare. NICTIZ is funded by the Ministry of Health, Welfare and Sport.

The Dutch NHII, called AORTA, will have many components, including national Electronic Patient Records (EPR).[165] The EPR is intended to allow authorized health care professionals to securely access patient data from any location in the country at any time. It will be a "virtual" record, with information pulled from many sources presented to the authorized healthcare provider in a cogent manner.[166]

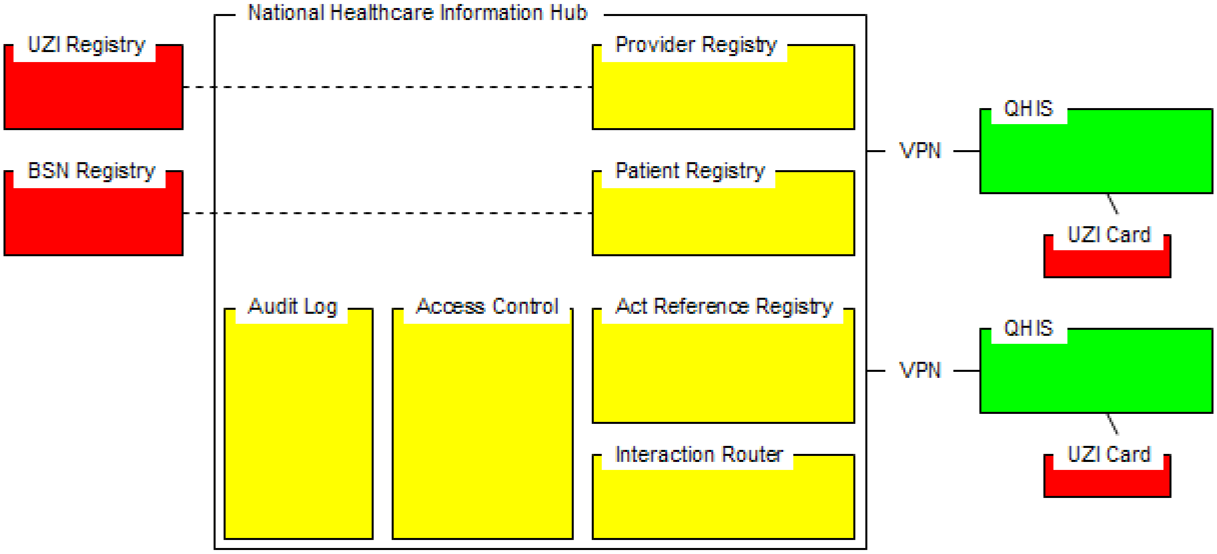
The Netherlands will not have a central database of health information. Rather, the Netherlands is using a central Web based record locator service, the National Healthcare Information Hub (LSP or ZIM), which went live in 2006. The LSP has been called a health care "Google." Under this system, clinical data will be maintained locally in the system of the health care practitioner or existing regional database. The practitioner registers clinical data for patients with the National Reference Index. There will be a standard set of data that will be registered for a patient encounter (e.g., patient name, name and type of health care provider, type of encounter). When a provider subsequently sends a query through the LSP, the National Reference Index, through the use of metadata keys, allows the requesting provider to identify which other providers have relevant patient information in their local data systems and to pull up the accessible data.[167]

[xi] Funding information was not included because it was not available for the newly re-designed health insurance structure.
[xii] We use the accepted Dutch abbreviations for terms (e.g., National ICT Institut in de Zorg, *NICTIZ*).

To facilitate matching data with the correct patient, a unique identifier, the Citizen Service Number (Dutch acronym BSN),[xiii] will be issued to every individual in the Netherlands.[168] Healthcare providers will also register for unique provider numbers (Dutch acronym UZI). Patient and provider registries of these unique identifiers form components of the LSP.

Health care practitioners can connect to the LSP and share information with others via the network connections of commercial providers of communication, application and content services. In order to link to the LSP, practitioners' must be Qualified Health Information Systems, i.e., systems that meet specified criteria that are both organizational as well as technical. Their systems must, for example, have 24/7 data accessibility and meet security specifications.[169]

Figure 3: AORTA[170]



Once a health care provider's system has been connected to the LSP, the provider may, among other things:

- Register an individual's health information at the reference index (subject to the individual's objection or opt out)
- Call up an overview that states the nature and location of patient data stored within the national system that can be retrieved (which allows the provider to narrow their selection of returned records);
- Retrieve specific patient data from individual patient records from the various healthcare providers; and
- Send service orders (e.g., medication instructions, lab requests) to other healthcare providers[171]

[xiii] The Netherlands is in the process of debating legislation that would permit the use of the Citizen Service Number (BSN), similar to the Social Security Number, to be used as the unique patient ID. The BSN is being used, with special permission, in the pilot regions.

### *Status of NHII*

Currently, 97% of Dutch GPs use a computer-based GP information system. Almost all use their system to record clinical notes during their consultation with a patient. A few regions use a regional GP system where all GPs work on a regionally hosted server. There are 22 regional healthcare networks that permit electronic communication between GPs and other local healthcare providers. [172] The Netherlands NHII will build on these regional networks.

The first two components of the Electronic Patient Record to be implemented are the Electronic General Practitioner's Record and the Electronic Medication Record. The Electronic GP Record allows an after-hours GP (a "locum") to access a summary health care record from the patient's regular GP. It also supports the transmission of information about services performed by the locum back to the patient's regular GP. There, the GP can review the information and update the patient's record. The Electronic Medication Record will give a healthcare provider insight into the medication history of his own patients via his own information system. The medication information will be maintained at the source (e.g., GP, pharmacy) but will be available to other providers and prescribers through the LSP.[173]

Proof of concept trials (in "laboratory" conditions) testing all the components necessary for the Electronic GP Record and the Medication Record were completed in 2006. The Electronic GP Record and Medication Record will be implemented in 11 pilot areas in early 2007.

### *Technical Information*

The LSP infrastructure and applications were designed, developed and deployed by an international IT company. The system is based on a commercially available application integration platform. There are around 10 vendors of GP healthcare information systems approved to connect to the LSP.[174]

### *System Access Controls*

Providers will register for a unique provider ID with the Unique Healthcare Provider Identification Register (UZI-register). They will be provided with an UZI chip card to use for authentication when using the LSP. The card also has an electronic signature. Providers may only connect to the LSP via a secure link once their office system has met the specified national standards. The LSP will provide role based access control based on the identity, role of the requester of data, and the level of data that they are authorized to receive. The LSP logs who has seen what data and when so that it can be verified whether access was justified.

### 4.2.2 Privacy Laws and Policies

Health information in the Netherlands is primarily protected by the Medical Treatments Contracts Act (Dutch acronym WGBO), the Individual Healthcare Professions Act and the Personal Data Protection Act. Under these laws, a health care provider generally cannot disclose health data to other parties. However, a patient's consent is assumed (implied) for sharing health information with persons who are directly involved in the patient's treatment. The information that can be shared is limited to that which is essential to the particular treatment. The individual has the right to object to the sharing of their medical data, even for treatment. If the individual objects, no medical data may be disclosed. In an emergency (e.g. a patient/client in critical situation) a healthcare provider may bypass all restrictions and obtain access to the required patient data.[175]

### 4.2.3 Consent Architecture and Mechanisms

In the Netherlands, individuals will be able to exercise control over their health information through a combination of national authorization profiles and the masking or concealing of specific information at the local level.

#### *Clinical Information*

**Notification of registering clinical data with Reference Index**
It is recommended that when a region is ready to begin registering data in the Act Reference Index, providers in the region should send out a letter notifying individuals that their information may be registered. They should also notify individuals of other health care providers who may exchange electronic health information, the information that will be available to them, based on their role, options that are available to the patient, and technical features that exist to protect their privacy.

**Registering clinical information in Reference index**
After notice, information will be registered in the Act Reference Index and will be available to other providers through the LSP under implied consent.

**Totally opting out of registering clinical information in the Act Reference Index.** An individual may withhold his consent to participate *at all* in the nationwide electronic exchange of his patient data (total opt out). When an individual chooses this option, health care providers may not register the patient's clinical information at the Act Reference Index. A disadvantage of this option is that if the patient later decides to consent, providers will not be able to retrieve past data since its existence was never recorded with the registry. Even when an individual exercises this option, his BSN will be registered with the national patient index.[176]

**Flag that information is not available.** When a provider (other than the source of the information) requests the patient's data, a flag will appear on the computer screen advising the requesting provider that the patient has declined to share data.[177]

**Partially opting out of registering information in the Act Reference Index.** A healthcare provider, in consultation with the patient, can decide not to register information with the Act Reference Index. If the information is not registered, it will not be accessible through the LSP.[178]

**Masking by data element**
Individuals can also opt out of sharing discrete data items (partial opt out). This is essentially a masking function that occurs at the point of service. When the local system receives an inquiry for masked data, it will not return the data. When information is masked at this level, it is generally concealed from *all* health care providers in the NHII other than the generating source.[179]

### Limiting access by provider

#### Current ability to limit by provider

In some regional applications, individuals currently can limit access to their records to specific health care providers. Providers who are given such permission can access the entire summary record. The individual cannot selectively arrange so that only sensitive patient data (e.g. psychiatric, HIV infection, abortion) is blocked for a particular healthcare practitioner.[180]

### Proposed ability to limit access

In the future, the Netherlands proposes to record individual consent choices in authorization profiles maintained in a single centrally administered registry to enable the national exchange of patient data via the LSP. The system will support individuals' detailed wishes to block specific healthcare parties from access as an additional restriction to the generic role-based authorization protocol.[181] The following summarizes the proposed levels at which the individual will be able to limit access to their information.

**By category of party requesting information.** The individual will be able to limit access to healthcare information by the category or professional capacity of the requesting party. (e.g., "All healthcare practitioners can view my data." or "No healthcare insurer may view my data.")

**By the individual provider using unique id number.** The individual will be able to limit access based on the unique provider number (UZI). (e.g., "No healthcare practitioner except Dr. Smith, unique id no. XYZ, can access my health data.")[182]

**By differing levels of authority.** The system will allow an individual to choose the level of authority granted to a variety of health care parties. The level of authority to access can include:

- Always
- Only in emergency
- Only after explicit consent
- Never[183]

(*e.g.,* "GPs can always view my information." "Hospitals may access my record only in an emergency.")
Utilization of authorization profiles can serve as an alternative to an individual's total opt out of participation in the nationwide electronic exchange of his health information. Instead of totally opting out of participating, an individual can choose to consent to participate but set their authorization profile to "never share." This way, patient data is registered at the referral index but is not visible to anyone.[184] Should the individual change their mind in the future, their information would be accessible, since it had already been registered.

**By class of data.** The individual will be able to choose the general data class of information that the retrieving party can view (e.g., "My health care provider can view all my information; my health insurer can view all personal, logistical and financial data, but not my detailed medical data.)[185]

**Ability to change profile.** The individual will be able to change their authorization profile in order to permit previously blocked access. It has not yet been determined who will be responsible for administering authorization profiles. If authorization profiles are administered through a third party, the individual will have to go back to administrator in order to change authorization profile. They could not grant access on the spot. If national electronic ID cards are utilized (as proposed) the individual may be able to grant access on the spot by changing own authorization profile via the Internet.[186]

### *Demographic information*

The Netherlands will have an identity repository or Patient Registry. The patient registry will be based on the BSN Registry which is a registry of all persons living in the Netherlands, managed by the Ministry for the Interior. It is proposed that the use of the BSN for healthcare be mandatory and that all patients must have this information registered with the Patient Registry. Patients will not be able to mask their name or BSN.[187]

# 5 Conclusion

There are a number of mechanisms currently in use that may be useful in managing "sensitive" medical information in the proposed US NHII. Consent mechanisms can be used to mask data when the individual has not consented to its disclosure. Certain providers may implement systems that automatically mask health information which, by law, requires specific consent to disclose. Masking in combination with a "shared secret" could potentially be used to permit individuals the ability on an ad hoc basis to specifically consent to the disclosure of their sensitive health information only to those to whom they provide the shared secret. Providers' ability to override masking could potentially fulfill legal provisions which allow providers to access even sensitive information to provide care in emergency situations. The proposed "seal" and "lock" could enable the compliance with the strictest level of confidentiality requirements. For example, substance use information could potentially be sealed and locked against access by law enforcement authorities, where applicable. Detailed authorization profiles also hold much promise, potentially allowing individuals to specify with varying degrees of granularity the providers to whom they consent (or do not consent) to disclose their health information.

These mechanisms, however, are not perfect. The mechanisms described work best with coded data. With respect to unencoded data, the consent mechanisms can be used at a high level (e.g., masking or sealing an entire record in a particular database). They cannot be used to shield or restrict the transfer of unencoded data at the discrete data element level (*e.g.,* a portion of a scanned letter). Given the potential wide-spread distribution of health data, it may also prove difficult to ensure that copies of data are masked along with the original. It is also difficult as a practical matter to maintain patient control over masked data that is incorporated into new records, *e.g.*, a provider's narrative about an encounter with the patient in which the patient has permitted that provider access to sensitive masked data. Furthermore, identifying and marking all the health data elements that would reveal a patient's condition is difficult particularly on a prospective basis and will require development of algorithms.

Experience in other countries, which are further along in the development of their respective nationwide health information infrastructures, may shed some light on whether and how the United States may be able to implement information policies based on individual control or consent in its NHII.

[1] Commonwealth Fund, *Descriptions of Health Care Systems: Australia, Canada, Germany, the Netherlands, New Zealand, the United Kingdom, and the United States*. Paper distributed at 2006 International Symposium on Health Care Policy (November, 2006). Retrieved January 16, 2007 from http://www.cmwf.org/newsroom/newsroom_show.htm?doc_id=420192]. Note that public expenditure figures are not available for the Netherlands, probably due to the recent changes in its health insurance structure.

[2] Dutch Data Protection Act. Retrieved January 15, 2007 from http://www.dutchdpa.nl/indexen/en_ind_wetten_wbp_wbp.shtml; University of Alberta, Health Law Institute and University of Victoria, School of Health Information Science. *Electronic Health Records and the Personal Information Protection and Electronic Documents Act* (April 2005) [hereinafter University of Alberta, *EHRs and PIPEDA*]. Retrieved January 16, 2007 from http://www.law.ualberta.ca/centres/hli/pdfs/ElectronicHealth.pdf

[3] Canada Health Infoway, *Electronic Health Record Infostructure (EHRi) Privacy and Security Conceptual Architecture: Version .1.1* at 7, 63 (June 2005) [hereinafter Canada Health Infoway *P&S Architecture*]. Retrieved December 27, 2006 from http://www.infoway-inforoute.ca/en/home/home.aspx; Path: Infoway Passport; Knowledgeway; Blueprint (free registration required).

[4] See Executive Order 13335, 69 Fed. Reg. 24059 (April 30, 2004); U.S. Department of Health and Human Services, *The Decade of Health Information Technology: Delivering Consumer-centric and Information-rich Health Care* (July 21, 2004). Retrieved February 12, 2007 from http://www.hhs.gov/healthit/documents/hitframework.pdf

[5] See U.S. Dept. of Health and Human Services, *Notice: Office of the National Coordinator for Health Information Technology; Statement of Organization, Functions, and Delegations of Authority*, 70 Fed. Reg. 48718-48720 (August 19, 2005).

[6] U.S. Dept. of Health and Human Services, *The Decade of Health Information Technology,* supra note 4, at 5.

[7] *Id.*

[8] See http://www.ansi.org/standards_activities/standards_boards_panels/hisb/hitsp.aspx?menuid=3

[9] See U.S. Department of Health and Human Services, *State Privacy and Security Subcontract Opportunities Announced Under Expanded HHS Contract with RTI.* Press Release. (May 23, 2006). Retrieved January 16, 2007 from: http://www.hhs.gov/news/press/2006pres/20060523.html

[10] Joy Pritts, et. al, *The State of Health Privacy: An Uneven Terrain* (2d ed. 2002). Retrieved December 27, 2006 from http://hpi.georgetown.edu/privacy/publications.html.

[11] *Id.*

[12] *See* U.S. Department of Health and Human Services, Substance Abuse and Mental Health Services Administration, *The Confidentiality of Alcohol and Drug Abuse Patient Records Regulation and the HIPAA Privacy Rule: Implications for Alcohol and Substance Abuse Programs* at 2 (June 2004). Retrieved December 27, 2006 from http://www.hipaa.samhsa.gov/Part2ComparisonClearedTOC.htm.

[13]Enrico Coiera and Roger Clarke, "e-Consent: the Design and Implementation of Consumer Consent Mechanisms in an Electronic Environment, 11 *Journal of the American Medical Informatics Association* 129-140 (2004).

[14] Commonwealth Fund, *Descriptions of Health Care Systems*, supra note 1. Health Canada, *Canada's Health Care System* (2005). Retrieved January 15, 2007 from http://www.hc-sc.gc.ca/hcs-sss/index_e.html

[15] Standing Senate Committee on Social Affairs, Science and Technology, *Out of the Shadows at Last: Transforming Mental Health, Mental Illness and Addiction Services in Canada* (May 2006). Retrieved January 14, 2007 from http://www.parl.gc.ca/39/1/parlbus/commbus/senate/com-e/soci-e/rep-e/rep02may06-e.htm.

[16] Canada Health Infoway. *Annual Report 2005-2006*. (n.d.) Retrieved October 1, 2006, from http://www.infoway-inforoute.ca/Admin/Upload/Dev/Document/Annual%20Report%2005-06%20EN.pdf

[17] Canada Health Infoway. *EHRS Blueprint*. Powerpoint Presentation. (March 2006). Retrieved January 15, 2007, from Retrieved December 27, 2006 from http://www.infoway-inforoute.ca/en/home/home.aspx; Path: Infoway Passport; Knowledgeway; Blueprint (free registration required).

[18] Canada Health Infoway. *Who We Are: Overview*. (2005). Retrieved September 25, 2006, from http://www.infoway-inforoute.ca/en/WhoWeAre/Overview.aspx

[19] Canada Health Infoway. *How We Work: Overview.* 2005. Retrieved September 25, 2006, from http://www.infoway-inforoute.ca/en/HowWeWork/Overview.aspx

[20] Canada Health Infoway. *Corporate Business Plan 2006-2007*. (n.d.) Retrieved January 13, 2007 from http://www.infoway-inforoute.ca/Admin/Upload/Dev/Document/Business%20Plan%2006-07%20EN.pdf

[21] Canada Health Infoway. *Annual Report 2005-2006*. (n.d.) Retrieved October 1, 2006, from http://www.infoway-inforoute.ca/Admin/Upload/Dev/Document/Annual%20Report%2005-06%20EN.pdf

[22] *Id.*

[23] Canada Health Infoway. *EHRS Blueprint: An Interoperable EHR Framework: Version 2* at 81(March 2006). Retrieved December 27, 2006 from http://www.infoway-inforoute.ca/en/home/home.aspx; Path: Infoway Passport; Knowledgeway; Blueprint (free registration required).

[24] *Id*. at 104.

[25] *Id.* at 111.

[26] *Id.* at 175.

[27] *Id. at 11, 115-116.*

[28] *Id.* at 116.

[29] *Id.* at 129.

[30] Canada Health Infoway, *P&S Architecture*, supra note 3 at 120.

[31] Canada Health Infoway. *EHRS Blueprint.* Powerpoint Presentation, supra note 17.

[32] PIPEDA does not govern the core functions of hospitals (patient care and treatment). University of Alberta, *EHRs & PIPEDA,* supra note 2 at 25.

[33] *Id.* at 4.

[34] Personal Information Protection and Electronic Documents Act, S.C. 2000, c.5, Schedule 1. s. 4.3 (hereinafter

PIPEDA); Canada Health Infoway. *Electronic Health Record (EHR) Privacy and Security Requirements: Version 1.1*.at App. B. (February 7, 2005) [hereinafter Canada Health Infoway *P&S Requirements*]. Retrieved December 27, 2006 from http://www.infoway-inforoute.ca/en/home/home.aspx; Path: Infoway Passport; Knowledgeway; Blueprint (free registration required).

[35] Canada Health Infoway *P&S Requirements*, supra note 34.

[36] PIPEDA, c.5, Schedule 1. s. 4.3

[37] University of Alberta, *EHRs& PIPEDA,* supra note 2, at 27.

[38] *Id*. at 28, 35-36.

[39] Canada Health Infoway, *P&S Requirements*, supra note 34.

[40] See University of Alberta, *EHRs& PIPEDA,* supra note 2, at 36, 73-74.

[41] Canada Health Infoway. *P& S Architecture*, supra note 3, at 61-62.

[42] *Id*.

[43] *Id.* at 7, 63.

[44] *Id.* at 64.

[45] *Id.* at 63.

[46] Advisory Committee on Information and Emerging Technologies, Federal/Provincial/Territorial Conference of Deputy Ministers of Health. *Pan-Canadian Health Information Privacy and Confidentiality Framework* (January 2005) [hereinafter ACHIET, *Pan-Canadian Framework*]. Retrieved September 27, 2006, from http://www.hc-sc.gc.ca/hcs-sss/pubs/ehealth-esante/2005-pancanad-priv/index_e.html

[47] *Id.*

[48] Canada Health Infoway. *P&S Requirements*, supra note 34, at 11.

[49] Canada Health Infoway. *Who We Are: Overview*, supra note 18.

[50] Canada Health Infoway. *P&S Architecture,* supra note 3, at 18.

[51] *Id*. at 4.

[52] *Id.* at 120.

[53]Alberta Netcare. *What is Alberta Netcare?* Retrieved January 7, 2007, from http://www.albertanetcare.ca/2.htm; Alberta Netcare. *What Is an Electronic Medical Record?*

[54] Alberta NetCare, *POSP—Three Levels of Support* (2006). Retrieved September 29, 2006 from http://www.posp.ab.ca/interested/three-levels-of-support.asp; Alberta NetCare, POSP News, *61% of Alberta's Physicians in POSP* (July 25 , 2006). Retrieved September 29, 2006 from http://www.posp.ab.ca/news/03-22-2006.asp.

[55] Alberta NetCare. Electronic Health Record. Physician Office System Program. *Vendor Conformance & Usability Requirements 2006*. Appendix 1 (March 2005) [hereinafter *Netcare VCUR*]. Retrieved September 29, 2006 from http://www.posp.ab.ca/vendors/.

[56] *Id*. at 30, 46.

[57] See Alberta Health Information Act, section 35(1). Retrieved November 16, 2006 from http://www.assembly.ab.ca/HIAReview/Health_Information_Act.pdf .

[58] See *id*., sections 35 and 58.

[59] ACHIET, *Pan-Canadian Framework,* supra note 46.

[60] Netcare *VCUR*, supra note 55.

[61] *Id.*

[62] *Id.* at 30.

[63] *Id.* at 29-30.

[64] *Id.* at 24.

[65] Netcare VCUR supra note 55 at 29.

[66] British Columbia Ministry of Health. *Pharmanet: What Information Is Maintained?* (June 21, 2006). Retrieved December 27, 2006 from http://www.healthservices.gov.bc.ca/pharme/pharmanet/answer21.html; British Columbia Ministry of Health, British Columbia College of Physicians and Surgeons, and College of Pharmacists of British Columbia, *PharmaNet Professional and Software Compliance Standards, Volume 2 Business Rules, Pharmacies (version 3.1)* at 23, 32-34 (November 2004) [hereinafter BC Ministry of Health, *Pharmanet Business Rules for Pharmacists*]. Retrieved December 27, 2006 from http://healthnet.hnet.bc.ca/catalogu/tech/ppscs2ph.pdf.

[67] British Columbia Ministry of Health, British Columbia College of Physicians and Surgeons, and College of Pharmacists of British Columbia, *PharmaNet Professional and Software Compliance Standards Volume 1, Introduction, ( version 3.1)* at 20-21( November 2004 ). Retrieved December 27, 2006 from http://healthnet.hnet.bc.ca/catalogu/tech/ppscs1.pdf.

[68] BC Ministry of Health, *Pharmanet Business Rules for Pharmacists* supra note 66, at 41, 43.

[69] British Columbia Ministry of Health, British Columbia College of Physicians and Surgeons, and College of Pharmacists of British Columbia, *PharmaNet Professional and Software Compliance Standards, Volume 2, Business Rules, Medical Practice Access version 4.1* (July 2005) [hereinafter B.C. Ministry of Health, *Pharmanet Business Rules for Medical Practice Access*]. Retrieved December 27, 2006 from http://healthnet.hnet.bc.ca/catalogu/tech/ppscs2mp.pdf.

[70] British Columbia, Ministry of Health, *Who Can Access PharmaNet?* (June 21, 2006). Retrieved December 27, 2006 from http://www.moh.hnet.bc.ca/pharme/pharmanet/answer46.html.

[71] University of Alberta, *EHRs & PIPEDA,* supra note 2, at 78-79.

[72] *See* British Columbia, Ministry of Health.*: What Safeguards Are in Place to Protect My Privacy*? (June 21, 2006) Retrieved December 27, 2006, from http://www.moh.hnet.bc.ca/pharme/pharmanet/answer22.html.

[73] University of Alberta, *EHRs & PIPEDA* supra note 2, at 79.

[74] See Pharmacists, Pharmacy Operations and Drug Scheduling Act, R.S.B.C, 1996 Section 38.1 and Access to PharmaNet Patient Record Information Regulation B.C. Reg. 537/2004. Retrieved January 15, 2007 from http://www.quickscribe.bc.ca/secure/bills/OIC/537-2004-1189.pdf.

[75] ACHIET, *Pan-Canadian Framework,* supra note 46.

[76] See BC Ministry of Health, *PharmaNet Business Rules for Pharmacists,* supra note 66.

[77] British Columbia, Ministry of Health. *Can I Choose Not to Use Pharmanet?*" (June 21, 2006). Retrieved December 27, 2006, from http://www.moh.hnet.bc.ca/pharme/pharmanet/answer40.html; BC Ministry of Health, *PharmaNet Business Rules for Pharmacists* supra note 66.

[78] BC Ministry of Health, *PharmaNet Business Rules for Pharmacists* supra note 66.

[79] British Columbia Ministry of Health, British Columbia College of Physicians and Surgeons, and College of Pharmacists of British Columbia, *PharmaNet Professional and Software Compliance Standards, Volume 2, Business Rules, Emergency Departments version 3.1* at 22-23 (November 2004) [hereinafter BC *PharmaNet Business Rules for Emergency Departments*]. Retrieved December 27, 2006 from http://healthnet.hnet.bc.ca/catalogu/tech/ppscs2ed.pdf.

[80] B.C. Ministry of Health, *Pharmanet Business Rules for Medical Practice Access*, supra note 69 at 7.

[81] *Id*. at 21.

[82] BC Ministry of Health, *PharmaNet Business Rules for Pharmacists* supra note 66, at 37.

[83] BC Ministry of Health, *PharmaNet Business Rules for Pharmacists* supra note 66, at 37.

[84] *Id*. College of Pharmacists of British Columbia, *Patient Keyword* (n.d.) Retrieved December 27, 2006 from http://www.bcpharmacists.org/youandyourpharmacist/pharmanet/keyword/.

[85] BC *PharmaNet Business Rules for Emergency Departments* note 79 supra, at 23, 29-30.

[86] *Id*.

[87] BC *Pharmanet Business Rules for Medical Practice Access*, supra note 69 at at 27-28.

[88] *Id*. at 21.

[89] *Id*. at 30.

[90] *Id.*

[91] *Id*. at 27-28.

[92] British Columbia Ministry of Health, British Columbia College of Physicians and Surgeons, and College of Pharmacists of British Columbia, *PharmaNet Professional and Software Compliance Standards Volume 3A, Client Registry Standards (version 2.1)* (Nov.21, 2003).

[93] Ontario Ministry of Health and Long-Term Care. *Emergency Department Access to Drug History Project/Drug Profile Viewer (DPV) System*. Fact sheet (April 2006) [hereinafter *DPV Fact sheet*]. Retrieved September 27, 2006, from http://www.health.gov.on.ca/english/providers/project/eda_drug/eda_factsheet.pdf

[94] Ontario Ministry of Health and Long Term Care. *Emergency Department Access to Prescription Drug History: Frequently Asked Questions* (July 2006) [hereinafter *EDA FAQs*]. Retrieved December 28, 2006 from http://www.health.gov.on.ca/english/providers/project/eda_drug/eda_faq.html.

[95] Cisco*, Smart Systems for Health Agency Lays the Foundation To Improve Healthcare Across Ontari.* Press Release (April 27, 2005). Retrieved January 14, 2007, from http://newsroom.cisco.com/dlls/global/canada/news/2005/cp_04-27b.html; Ontario Ministry of Health and Long-Term Care. *DPV Fact Sheet*, supra note 93.

[96]Ontario Ministry of Health and Long-Term Care. *DPV Fact Sheet*, supra note 93.

[97] See Governor in Council, Order in Council, P.C. 2005-2224, November 28, 2005; 139 Canada Gazette No. 25 (December 14, 2005). Retrieved September 29, 2006, from

http://canadagazette.gc.ca/partII/2005/20051214/html/sor399-e.html.

[98] See Ontario Personal Health Information Protection Act. 2004 S.O. 2004, c. 3. Section 20. Retrieved December 28, 2006 from the Canadian Legal Information Institute at http://www.canlii.org/on/laws/sta/2004c.3sch.a/index.html.

[99] See *Id*. Section 18.

[100] *Id*. Sections 19, 20, 37(1)(a).

[101] *Id.* Section 20(3).

[102] *Id.* Sections 40(1).

[103] ACHIET, *Pan-Canadian Framework,* supra note 46.

[104] Ontario Ministry of Health, *DPV Fact Sheet*, supra note 93.

[105] Ontario Ministry of Health, *EDA FAQs*, supra note 94.

[106] *Id*.

[107] Ontario Ministry of Health and Long Term Care, *Consent Forms for Recipients of the Ontario Drug Benefit Program and Trillium Drug Program* (June 2005) [hereinafter Ontario Ministry of Health, *Consent Forms for ODB*]. Retrieved January 12, 2007 from http://www.health.gov.on.ca/english/providers/project/eda_drug/eda_forms.html.

[108] *Id*.

[109] Ontario Ministry of Health and Long Term Care and Smart Systems for Health Agency, *Drug Profile Viewer System: Providing Better Care for Ontario Seniors*. Powerpoint presentation, slide 15 (May 1, 2006) [hereinafter Ontario Ministry of Health, *DPV Powerpoint*]. Retrieved September 28, 2006, from http://www.e-healthconference.com/default.asp?ID=1368#.

[110] Ontario Ministry of Health, *EDA FAQs* supra note 94.

[111] *Id*.

[112] Ontario Ministry of Health, *Consent Forms for ODB*, supra note 107.

[113] Ontario Ministry of Health, *EDA FAQs*, supra note 94.

[114] *Id*.

[115] *Id*.

[116] Ontario Ministry of Health, *DPV Powerpoint*, supra note 109 at slides 7, 16.

[117] Commonwealth Fund, *Descriptions of Health Care Systems*, supra note 1; Sheila Leatherman and Kim Sutherland, "Quality of Care in the NHS of England," 4 *BMJ USA* 144 (April 17, 2004). Retrieved December 29, 2006 from http://www.bmj.com/cgi/reprint/328/7445/E288.

[118] National Health Service, England, *About the NHS—How the NHS Works*. Retrieved January 12, 2007 from http://www.nhs.uk/england/AboutTheNhs/Default.cmsx#gps.

[119] United Kingdom, House of Commons*,* Select Committee on Health*, Fourth Report 1999-2000* (July 13, 2000). Retrieved January 13, 2006 from http://www.publications.parliament.uk/pa/cm199900/cmselect/cmhealth/373/37302.htm.

[120] NHS Direct, *Sexual Health Clinics.* Retrieved January 12, 2007 from http://www.nhsdirect.nhs.uk/articles/article.aspx?articleId=473&sectionId=26027.

[121] National Audit Office, United Kingdom, *The National Programme for IT in the NHS* at 1, 4 (June 16, 2006). Retrieved December 27, 2006 from http://www.nao.org.uk/publications/nao_reports/chronindex.asp?type=vfm.

[122] Connecting for Health, National Health Service, *A Guide to the National Programme for Information Technology*" at 3 (April 2005) [hereinafter *Guide to NPfIT Brochure*]. Retrieved September 23, 2006, from http://www.connectingforhealth.nhs.uk/publications/brochures/npfit_brochure_apr_05_final.pdf

[123] National Audit Office, supra note 121, at 9.

[124] *Id*. at 6.

[125] *Id.* at 10. Connecting for Health, *Guide to NPfIT Brochure,* supra note 122, at 13.

[126] In his recently published paper, "Information Technology in the English National Health Service," 296 JAMA 2255-2258 (Nov. 8, 2006), Cyril Chantler reports 30% of GPs in England use electronic medical records (a figure obtained from a Connecting for Health official). Don Detmer, and Elaine Steen's paper, report 52% of English GPs use electronic medical records. See Detmer and Steen, *Learning from Abroad: Lessons and Questions on Personal Health Records for National Policy* (March 2006). Retrieved August, 15, 2006 from *http://www.aarp.org/research/health/carequality/2006_10_phr_abroad.html.* A recent study by the Commonwealth Fund reports that 89% of UK primary care physicians use electronic records. The Commonwealth Fund, *Survey of Primary Care Physicians in Seven Countries*. Presentation at 2006 International Symposium on Health Care Policy (November 2006.) Retrieved January 16, 2007 from

http://www.cmwf.org/newsroom/newsroom_show.htm?doc_id=420192]. Although this latter study encompasses all the UK, that difference alone does not appear to account for the discrepancy in figures.

[127] Connecting for Health, National Health Service, *Guide to NPfIT Brochure,* supra note 122, at 8.

[128] Ministerial Taskforce on the Summary Care Record, *Report of the Ministerial Taskforce on the NHS Summary Care Record* at 4 (December 6, 2006) [hereinafter *Ministerial Taskforce Report*]. Retrieved January 4, 2007, from http://www.connectingforhealth.nhs.uk/publications/care_record_taskforce_doc.pdf.

[129] *Id.*

[130] Connecting for Health, National Health Service, *NHS Personal Demographics Service (PDS)* (June 2005). Retrieved January 4, 2007 from www.connectingforhealth.**nhs**.uk/publications/comms_tkjune05/**NHSPDS**.pdf.

[131] "Patient Records May Only Be Shared Locally," 66 *e-Health Insider Primary Care* (May10, 2006). Retrieved January 4, 2006 from http://www.ehiprimarycare.com/news; Cyril Chantler et al., supra note 126, at 2.

[132] Connecting for Health, National Health Service, *Guide to NPfIT,* supra note 122, at 3.

[133] Daloni Carlisle, "Space Programme," *eHealth Insider* (April 10, 2006). Retrieved January 3, 2007 from http://www.e-health-insider.com/comment_and_analysis/index.cfm?ID=134; Connecting for Health, National Health Service, *HealthSpace FAQs*. Retrieved January 2, 2007 from http://www.connectingforhealth.nhs.uk/faq/healthspace.

[134] Information Standards Board, National Health Service *NHS ISB Inherited Information Standard Submission Personal Demographics Service (PDS) Dataset (version 1)* at 15 (August 11, 2006). Retrieved January 6, 2006 from http://www.isb.nhs.uk/docs/pds-dataset-inherited-standard-submission-v1-0.pdf.

[135] Mark Ferrar, *The NHS, Standards, Security & Identity Management*, Presentation for OASIS Adoption Forum, (November 28, 2006). Retrieved January 2, 2007 from http://www.oasis-open.org/events/adoptionforum2006/slides/ferrar.ppt.

[136] Connecting for Health, National Health Service. *GP Systems of Choice (GPSoC) Update* (October 2006). Retrieved January 3, 2007 from http://www.connectingforhealth.nhs.uk/publications/gpsoc.

[137] Connecting for Health, National Health Service, *Guide to NPfIT,* supra note 122, at 20-21.

[138] Connecting for Health, National Health Service *"Sealed Envelopes" Briefing Paper: "Selective Alerting" Approach*. (2006) [hereinafter Connecting for Health, *Sealed Envelopes Briefing Paper*]. Retrieved February 16, 2007 from http://www.connectingforhealth.nhs.uk/crdb/sealed_envelopes_briefing_paper.pdf.

[139] Lucy Sherriff, "NHS Record Access Pilot Due Next Year," *The Register.* November 26, 2006. Retrieved January 3, 2007 from http://www.theregister.co.uk/2006/11/25/online_access.

[140] Department of Health, *Data Protection Act of 1998* (March 27, 2000). Retrieved January 14, 2007 from http://www.dh.gov.uk/PolicyAndGuidance/OrganisationPolicy/RecordsManagement/fs/en.

[141] Cyril Chantler et al., supra note 126.

[142] Connecting for Health, National Health Service, *The Care Record Guarantee* (May 2006). Retrieved December 27, 2006 from http://www.connectingforhealth.nhs.uk/crdb/docs/crs_guarantee.pdf.

[143] Connecting for Health, *Sealed Envelopes Briefing Paper* supra note 138.

[144] NHS Connecting for Health. "Interview with CRDB Chair Harry Cayton," Retrieved January 6, 2006, from http://www.connectingforhealth.nhs.uk/crdb.; Cyril Chantler et al., supra note 126.

[145] Connecting for Health, National Health Service, *The Initial Generation and Continuing Refreshment of the GP Summary Care Record: The Way Forward* at 4 (May 2006) [hereinafter Connecting for Health, *Initial Generation of GP Summary Care Record*]. Retrieved December 28, 2006 from http://www.connectingforhealth.nhs.uk/crdb/SCR%20Briefing14.pdf.

[146] Harry Cayton, Speech to Connecting Americans to Their Healthcare Conference. Retrieved from http://www.rwjf.org/newsroom/activitydetail.jsp?id=10189&type=3.

[147] *Id.*; Cyril Chantler et al., supra note 126.

[148] *Ministerial Taskforce Report*, supra note 128 at 4.

[149] *Id.* at 6.

[150] *Id.* at 7-8.

[151] *Id.* at 4, 9; Connecting for Health, *Initial Generation of GP Summary Care Record,* supra note 145.

[152] *Ministerial Taskforce Report*, supra note 128; John Carvel, "Minister Admits U-Turn on NHS Database Amid Privacy Fears," The Guardian (London) page 6, Dec. 19, 2006. Retrieved January 6, 2007 from http://society.guardian.co.uk/e-public/story/0,,1975034,00.html.

[153] *Ministerial Taskforce Report*, supra note 128, at 9.

[154] *Ministerial Taskforce Report*, supra note 128; John Carvel, "Minister Admits U-Turn on NHS Database Amid Privacy Fears," The Guardian (London), page 6, Dec. 19, 2006. Retrieved January 6, 2007 from

http://society.guardian.co.uk/e-public/story/0,,1975034,00.html.

[155] *Ministerial Taskforce Report*, supra note 128, at Annex 3.

[156] Connecting for Health, *Initial Generation of GP Summary Care Record,* supra note 145 at 3.

[157] *Id.* at 2-3.

[158] Connecting for Health, *"Sealed Envelopes" Briefing Paper, supra note 138.*

[159] *Id*. at 3 and 5.

[160] See Connecting for Health, *Initial Generation of GP Summary Care Record*, supra note 145 at 4, note 3; See also, Chantler, Cyril, supra note 126, Table 1.

[161] Connecting for Health, National Health Service, *A Brief Guide to the Personal Demographics Service for General Practitioners* at 13. Retrieved December 28, 2006 from http://www.connectingforhealth.nhs.uk/demographics.

[162] *Id.* at 10.

[163] Netherlands Ministry of Health, Welfare and Sport. *Health Insurance in the Netherlands. The New Health Insurance System from 2006.* September 2005. Retrieved August 31, 2006, from http://www.minvws.nl/en/themes/health-insurance-system/default.asp; Commonwealth Fund, *Descriptions of Health Care System*, supra note 1.

[164] André den Exter, et. al.., *Health Care Systems in Transition: Netherlands,* Copenhagen, WHO Regional Office for Europe on behalf of the European Observancy on Health Systems and Policies, 2004. Retrieved Sept. 1, 2006 from http://www.euro.who.int/Document/E84949.pdf; Denis Protti and Coen Smit, "The Netherlands: Another European Country Where GPs Have Been Using EMRs for Over Twenty Years." *HCIM&C* 3rd Quarter, 2006. Retrieved January 9, 2007, from http://www.healthcareimc.com/bcovers/PDFS/TheNetherlands.pdf.

[165] Netherlands Ministry of Health, Welfare and Sport. *ICT in Dutch Healthcare: An International Perspective* (May 2006) [hereinafter Ministry of Health, *ICT in Dutch Healthcare*]. Retrieved January 7, 2007, from http://www.minvws.nl/en/themes/ict-in-healthcare/default.asp. An excellent description of the method by which the LSP will work can be found in René Spronk, *Act Reference Registries: An Infostructural Concept* (Dec. 8, 2006). Retrieved January 7, 2007, from http://ringholm.de/docs.

[166] Ministry of Health, *ICT in Dutch Healthcare,* supra note 165, at 9.

[167] René Spronk, *Act Reference Registries note 165, supra.*

[168] Netherlands Ministry of Health, Welfare and Sport. *ICT in Dutch Healthcare*, supra note 165.

[169] Netherlands Ministry of Health, Welfare and Sport. *ICT in Dutch Healthcare,* supra note 165, at 12-13.

[170] René Spronk, *AORTA, The National Dutch Infrastructure* (January 2007). Available at: http://www.ringholm.de/docs/00980_en.htm.

[171] NICTIZ, *Draft: Specification of the Basic infrastructure for Healthcare*, *Authorisation* at 4, 12 (August 11, 2006) [hereinafter NICTIZ, *Draft Authorisation Specification*]. [Note this is an English translation, kindly provided to us from NICTIZ, of an extract from the "Specification of the Basic Infrastructure for Healthcare version 2.4" available in Dutch, "Specificatie van de basisinfrastructuur in de zorg" at: http://nictiz.nl/uploaded/FILES/AORTA%20release%20augustus%202006/Specificatie%20Basisinfrastructuur%20in%20de%20Zorg%20v2.4.pdf.]

[172] Denis Protti and Coen Smit, supra note 165.

[173] Ministry of Health, *ICT in Dutch Healthcare,* supra note 157.

[174] Oliver Caudron, *Technologies at the Center of the NICTIZ Project*, Presentation to Intersystems Finnish Symposium 2006. Retrieved January 14, 2007 from http://209.61.190.221/finland/corporate/corporateBaseTemplate.csp?pageID=3728; Bob Schat, "The Dutch National Healthcare Information Hub," Presentation to Intersystems Finnish Symposium 2006. Retrieved January 14, 2007 from http://209.61.190.221/finland/corporate/corporateBaseTemplate.csp?pageID=3728.

[175] Theo Hooghiemstra, "The Implementation of Directive 95/46/EC in the Netherlands, with Special Regard to Medical Data," 9 *European Journal of Health Law*. 219-227 (2002); Dutch Data Protection Authority (College Berscherming Persoonsgegevens), *Confidentiality of Your Medical Data* ( June 2005). Retrieved January 9, 2007, from http://www.dutchdpa.nl/documenten/en_inf_subj_Confidentiality_Medical_Data.shtml?refer=true&theme=purple.

[176] NICTIZ, *Draft Authorisation Specification*, supra note 171, at 29.

[177] Dutch Unique Healthcare Provider Identification Register (UZI-register), Secretary for National Healthcare, *AORTA Introductory Video.* Retrieved January 5, 2007 from http://www.uzi-register.nl/media/EMD_WDH_EN_256K.wmv.

[178] NICTIZ, *Draft Authorisation Specification*, supra note 171, at 13.

[179] *Id.*, at 12-13.
[180] *Id*. at 15.
[181] *Id*. at 12.
[182] *Id*. at 28.
[183] *Id*.
[184] *Id*. at 29.
[185] *Id*. at 28-29.
[186] NICTIZ, *Draft Authorisation Specification*, supra note 171, at 14.
[187] NICTIZ, *Draft Authorisation Specification*, supra note 171, at 29; Spronk, *AORTA, The National Dutch Infrastructure* supra note 170.