

APPENDIX C

Select Examples of Exchange in Other Developed Countries

Canada

Canada is currently developing interoperable electronic exchange for its 32 million residents. The system is being developed and funded primarily through Canada Health Infoway, a not-for-profit corporation whose members are the 14 federal, provincial, and territorial Deputy Ministers of Health.¹ Infoway supports HIT development by way of strategic investments in local and regional infrastructure projects. Specific consent policies are developed primarily at the provincial level and are largely *opt-out* systems with granularity.² The federal government has created a set of guidelines to promote further harmonization and development of consent policies nationwide – the Pan-Canadian Health Information Privacy and Confidentiality Framework³ – and is developing a nationwide system to track consent directives through the Consent Directive Management Service.⁴ Infoway plans to have fully interoperable EHRs for its entire population by 2016.⁵

In Canada, each of the 14 provinces is responsible for developing specific health privacy and security provisions. Almost all provinces are pursuing an *opt-out* system with varying levels of granularity, allowing implied consent to store and transmit health information for treatment purposes (the sole exception is Quebec, which requires a patient's express consent before sharing information).⁶ Many jurisdictions currently require that patients be informed that their health information is being collected and how it may be used, as well as be given information regarding the security safeguards in place to protect their data. This notice may be given at any time before or at the time that the information is being collected, and can be given either directly by a provider or by way of posters, brochures, websites, or other educational materials.⁷ It remains an open question what, if any, additional consent provisions are needed for secondary uses of health data, such as research and public health surveillance.⁸

¹ Canada Health Infoway. "2009-2010 Corporate Business plan," at 4-5 [hereinafter "Business plan"]. Available at: <http://www.infoway-inforoute.ca/lang-en/about-infoway/about/annual-reports-and-business-plans>.

² Canada Health Infoway. "White Paper on Information Governance of the Interoperable Electronic Health Record," March, 2007 [hereinafter "White Paper"]. Available at: http://www2.infoway-inforoute.ca/Documents/Information%20Governance%20Paper%20Final_20070328_EN.pdf.

³ Health Canada, "Pan-Canadian Health Information Privacy and Confidentiality Framework," January 27, 2005. Available at: <http://www.hc-sc.gc.ca/hcs-sss/pubs/ehealth-esante/2005-pancanad-priv/index-eng.php>.

⁴ Canada Health Infoway. "An Overview of the Electronic Health Record Privacy and Security Conceptual Architecture," March 2006, at 8 [hereinafter "Overview"].

⁵ Canada Health Infoway. "2015: Advancing Canada's Next Generation of Health Care" [hereinafter "Advancing"]. Available at: <http://www.v1.theglobeandmail.com/partners/free/infoway/pdf/2015%20Health%20care%20full%20report%20EN.pdf>.

⁶ Pritts, J. and K. Conner. "The Implementation of E-consent Mechanisms in Three Countries: Canada, England, and the Netherlands (the ability to mask or limit access to health data)." Prepared for: *Substance Abuse and Mental Health Services Administration, HHS*, February 16, 2007, at 17.

⁷ Canada Health Infoway, "White Paper," *supra* note 2, at 9-10.

⁸ *Id.* at 13-14.

Because Canadian privacy policy is set at both the federal and provincial levels, Infoway has developed the Pan-Canadian Health Information Privacy and Confidentiality Framework in order to harmonize consent requirements. The framework specifies a set of core privacy principles upon which provinces can develop consent requirements (as the framework itself is not legally binding). These principles specify that the individual patient should be permitted to mask data by content or provider, and have been endorsed by all provinces except for Quebec and Saskatchewan.⁹ Individual provinces are currently developing or updating their data segmentation rules to allow for as much or more granularity as specified in the Pan-Canadian Framework.¹⁰ At present, many provinces permit highly granular consent options, allowing individuals to mask discreet data elements in addition to categories of data.

As of the end of the 2009 fiscal year, Infoway had approved the allocation of \$1.58 billion (out of a total budget of \$1.64 billion) toward 283 infrastructure projects undertaken at the provincial and local levels for building core electronic exchange systems, including client and provider registries, diagnostic imaging, drug and laboratory information systems, clinical reports, and immunization records. As of March, 2009, these functionalities had been integrated into the EHRs of 17 percent of Canadian citizens.¹¹ Originally, Infoway had aimed at extending these basic functionalities to 50% of the population by 2010, but the organization recently acknowledged that this timetable is unlikely to be met, and that EHR infrastructure development remains highly varied among provinces.¹²

Although Canadian privacy standards are set and health data is stored at the local and provincial levels, a nationwide consent system – Consent Directive Management Services (CDMS) – is being developed to obtain and track consent directives nationwide. Consent may be obtained either electronically or at the point of service and stored within the national CDMS, while the records themselves are maintained at the practitioner or regional level (depending on whether there is an existing regional electronic exchange infrastructure in place). Consent data moves through the system along with health information, and it is incumbent upon individual data custodians to maintain data security and uphold consent directives in accordance with the rules of the particular jurisdiction in which data is collected or received.¹³ However, there remains some uncertainty as to how consent directives are maintained between provinces with differing granularity options.¹⁴

The Netherlands

The Dutch National Healthcare Information Hub (LSP), currently being implemented by the National Information and Communication Technology Institute for Healthcare (NICTIZ), is an *opt-out* system with granularity built around remote information hubs connected to a national, searchable database. This system, referred to as the “health care Google,” maintains patient records at the practitioner or regional level (where regional electronic exchange already exists), and makes them available through a searchable database accessible to eligible practitioners

⁹ Health Canada, *supra* note 3.

¹⁰ Pritts, J. and K. Conner, *supra* note 6, at 20.

¹¹ Canada Health Infoway, “Business plan,” *supra* note 1.

¹² Canada Health Infoway, “Advancing,” *supra* note 5.

¹³ Canada Health Infoway, “White paper,” *supra* note 2, at 7-8.

¹⁴ *Id.* at 11.

throughout the country (*i.e.*, those who meet a set of minimum security and functionality requirements).¹⁵ The country is currently debating whether to require all practices to connect to the LSP.¹⁶ While consent to share medical information is implied for treatment purposes, patients have the option of segmenting data based on provider, care delivery setting, and data type, and may even opt out of the exchange entirely.¹⁷

The vast majority of practitioners in the Netherlands (97%) currently utilize EHRs in their practice.¹⁸ The goal of the NICTIZ is to link all practices to the central database in the near future, although there has been delay due to many of the existing systems not meeting the LSP security requirements.¹⁹ At present, efforts are focused on nationwide implementation of two “front-runner” functionalities – electronic medication lists and general practitioner’s summary records.²⁰ Additional functionalities, such as acute care records and specialized systems chronic disease management, are currently being developed by NICTIZ.²¹

Within the Dutch LSP, citizens are identified by their Citizen Service Number (which functions as an analog to U.S. Social Security numbers).²² In order to participate in the LSP, a practitioner must satisfy a set of security requirements. The individual practitioner is then connected to the LSP through certified commercial entities known as Healthcare Service Providers, which act as intermediaries between the provider and the hub and are responsible for tracking consent data and maintaining data security.²³ The system allows the option of opting out of electronic exchange entirely, as well as a high degree of granularity. All information is available for treatment purposes only; private entities such as insurance companies and employers cannot access the system.²⁴

Months before the LSP became operational in November, 2008, a form was sent to Dutch citizens informing them of the system and giving them the choice to opt out. Some 330,000 (out of 16.5 million residents) did so, leading to concern over the implementation strategy, which was criticized for not adequately explaining the available granularity options and security measures in

¹⁵ Pritts, *supra* note 6, at 3.

¹⁶ HIMSS Enterprise Systems Steering Committee. “Electronic Health Records: A Global Perspective.” August 2009, at 25. Available at: http://www.himss.org/content/files/200808_EHRGlobalPerspective_whitepaper.pdf.

¹⁷ Pritts, *supra* note 6, at 42-45.

¹⁸ Schoen, C et al. “A Survey of Primary Care Physicians in Eleven Countries, 2009: Perspectives on Care, Costs, and Experience.” *Health Affairs Web Exclusive*, 5 November 2009, 1171-1183, at 1175. Available at: http://www.commonwealthfund.org/~media/Files/Publications/In%20the%20literature/2009/Nov/1336_Schoen_survey_primary_care_MDs_11_countries_HA_WebExcl_11052009_ITL_v2.pdf.

¹⁹ Reis, Leo van der. “Lessons for the U.S. from the Netherlands’ National Electronic Medical Records System.” *eHealth International*, Vol. 5, No. 1, March 2009, at 37. Available at: <http://www.ehealthinternational.org/vol5num1/Vol5Num1p35.pdf>.

²⁰ Ministry of Health, Welfare and Sport. “ICT in Healthcare.” Available at: <http://www.minvws.nl/en/themes/ict-in-healthcare/default.asp>.

²¹ Spronk, R. “AORTA, the Dutch National Infrastructure.” Available at: http://www.ringholm.de/docs/00980_en.htm.

²² NICTIZ. “The National Healthcare Information Hub,” February 15, 2006. Available at: <http://www.sanita.forumpa.it/documenti/0/200/240/242/nictizuk3.pdf>.

²³ National ICT Institute for Healthcare. “The National Healthcare Information Hub,” at 2. Available at: <http://www.sanita.forumpa.it/documenti/0/200/240/242/nictizuk3.pdf>.

²⁴ Laurens J. van Baardewijk. “Electronic Health Record in the Netherlands: Afraid of the Unknown.” *Amsterdam Law Forum*, August 2009, at 41.

place.²⁵ The system has also been criticized by both consumers and some physicians for not providing adequate security and privacy protections.²⁶

Sweden

Sweden has recently started to implement a national health information exchange. In pursuance of this goal, the Swedish Parliament passed the Patient Data Act on July 1, 2008. The law aims to allow patients to decide who can access their medical record, while allowing care providers to communicate permitted patient data in the exchange securely.²⁷ In Sweden, 100% of medical records related to primary care services are digitized and 80 to 90% of those related to hospital care services are digitized.²⁸ The focus of the new exchange (NPÖ) is to allow these records to be shared between providers with appropriate patient consent to allow for increased preventive health improvements and correct diagnosis.²⁹ The exchange will contain several “information volumes,” including diagnoses, care services, medicines, care contacts, care documents, status, care planning, and examination results.³⁰ It took one year after a contract was awarded for an HIT company to establish the legal context, patient consent, and technological capability for the system. These were completed on May 4, 2009.³¹

To meet the goal of the legislation, the Swedish system uses an *opt-in with restrictions* consent model. Sweden plans to place all digitized records on the central server for the exchange, but to allow patients to decide which physicians will ultimately be able to access their records in the database. A national level security database, “BIF,” was designed to parallel the new national patient records system. This system will act as the authorization management service for secure information-handling across organizations in the health care sector. A digital communication system, “Sjunet,” ensures that doctors use a special electronic ID card to log in, and keeps track of each instance that a health record is accessed. In order to view any healthcare record, health care professionals must have a “patient relation” with the patient, meaning the patient has given consent for them to look at his or her health record. Patients not only have the option of restricting which professionals can access their record, they can also restrict the period of time after the visit that the professional can continue to access it. Sweden also restricts health care professionals on how much of the record they can see. However, county councils and municipalities, not patients, designate which professionals can see which parts of the record. The system has a “break the glass” provision that allows health care professionals to access the record in an emergency, but the access will be logged and professionals will have to explain why they needed to view the information.³²

The Swedish government began to implement this system in May 2009 on a trial basis within the Municipality and County Council of Örebro. After evaluating its establishment and making

²⁵ *Id.* at 42.

²⁶ Reis, *supra* note 19, at 36.

²⁷ National Patientöversikt. “Focus on Delivery.” Available at: www.npo.nu.

²⁸ Elfgrén, E. L. “Prevention progression,” *Public Service Review: Health* 20, July 2009, p. 1.

²⁹ *Id.*

³⁰ National Patientöversikt, *supra* note 27.

³¹ Intersystems Press Release. “Tieto and InterSystems Create Swedish National Electronic Health Record,” June 3, 2009. Available at: http://www.intersystems.com/press/2009/sweden_print.html.

³² Elfgrén, *supra* note 28, at 1.

appropriate changes, the government's goal is to establish the system gradually in additional counties and municipalities before extending it to the rest of the country.³³

³³ National Patientöversikt, *supra* note 27.