

# POLICY BY PROCRASTINATION: SECONDARY USE OF ELECTRONIC HEALTH RECORDS FOR HEALTH RESEARCH PURPOSES

*Patricia Kosseim and Megan Brady\**

*Driven by government priorities and significant financial investments, stakeholders in Canada are working actively to develop and deploy pan-Canadian, interoperable electronic health record (EHR) systems. Efforts to date have concentrated primarily on health care purposes only. However, limiting the design and incremental roll out of such systems for this primary purpose now will only increase the complexity of allowing access to electronic health records for secondary research purposes later.*

*The likely effect of deferring questions concerning secondary uses will be an exacerbated policy dilemma that drives solutions further away from the well-established norm of voluntary and informed consent as a core component of privacy protection. We argue that such a shift—if or when it happens—should not occur without critical reflection, open policy debate, and a democratic decision-making process. In particular, a shift away from consent as a key pillar of privacy protection in the health system must not, in our view, be motivated solely by technological design and feasibility considerations—issues that arise as an automatic consequence of other, merely pragmatic choices being made today.*

*To avoid succumbing to technological pressures and letting practical expedience determine fundamental public policy choices, we need to examine what viable alternatives exist that could permit access to EHR data for research purposes, and under what conditions this might be accomplished. In this paper we outline what some of those policy alternatives might be, beginning with specific informed consent and moving towards broad consent, implied consent, no consent, consent waiver, and retroactive deemed consent. Through this spectrum of options we attempt to demonstrate why legal and policy considerations require early reflection and up-front integration into systems as they are being designed. By setting out a range of policy options to address research access to EHR systems and discussing their implications, this paper aims to support informed deliberations about available choices before technological imperatives pre-determine the selection for us.*

INTRODUCTION .....	6
I. BACKGROUND.....	6
A. The Expansive Vision of EHRs .....	6
B. The Incremental Approach to Implementation .....	8
C. Privacy Implications of the Incremental Approach .....	11
II. INFORMED CONSENT AS A DEFAULT STANDARD FOR RESEARCH.....	13
A. Clinical Research.....	14
B. Epidemiological Research.....	15
C. Creation of Research Platforms.....	17
III. POLICY OPTIONS FOR ALLOWING RESEARCH USE OF EHRs .....	19
A. Obtaining Informed Consent for Each Specific Research Study .....	20
B. Seeking Broad Consent For Future, Yet Unspecified Research Studies.....	22
C. Using De-Identification as a Means of Carving Out Research Activities Altogether .....	27
D. Relying on Implied Consent by Re-Conceptualizing Research as a Necessary Adjunct to the Primary Purpose of Health Care.....	31
E. Resorting to Existing Statutory Consent Exemptions for Research.....	35
F. Retroactively Deeming Consent by Legislative Amendment.....	39
CONCLUSION.....	43

---

\* Patricia Kosseim is General Counsel, and Megan Brady is Legal Counsel, with the Office of the Privacy Commissioner of Canada. The authors wish to thank Dr. Don Willison and Dr. Khaled El Emam for their helpful comments on earlier drafts of this paper, each from their respective area of expertise. The views expressed in this paper are those of the authors alone and do not necessarily reflect the views of the individuals who were consulted.

## INTRODUCTION

Driven by government-announced priorities and significant public and private sector investments, stakeholders in Canada are working actively on developing and deploying pan-Canadian, interoperable electronic health record (EHR) systems. Efforts to date have concentrated primarily on developing and deploying interoperable EHRs for care and treatment purposes only. The design and incremental roll out of EHR systems for this limited purpose *now* will increase the complexity of determining access rights to EHRs for secondary purposes *later*.

The likely effect of deferring questions concerning secondary uses is an exacerbated policy dilemma that drives solutions away from the current and well-established norm of voluntary and informed consent. We argue that such a shift should not occur without critical reflection, open policy debate, and a democratic decision-making process. In particular, a shift away from consent as a key pillar of privacy protection in the health system must not, in our view, be driven solely by technological expedience and design and feasibility considerations—issues that arise as an automatic consequence of other, merely pragmatic choices being made today.

There are many potential secondary uses for electronic health data. These include uses in furtherance of public health surveillance, health system planning and management, quality assessment, health research, mandatory reporting, employment, insurance, drug marketing, and law enforcement purposes. This article, however, will examine the specific case of health research as a secondary use. We focus primarily on the fundamental issue of consent.

## I

## BACKGROUND

## A. The Expansive Vision of EHRs

In 1997, an Advisory Council on Health Info-Structure was commissioned by the Federal Minister of Health. The purpose of the Advisory Council, made up of independent experts, was to provide strategic advice on how information technologies and systems could best support and promote more informed decision-making by health professionals, administrators, planners, policy-makers, and individual Canadians. Its mandate was to guide the development of an integrated Canadian health information info-structure by ensuring, among other things, that both health care and broader public health requirements would be addressed throughout Canada.<sup>1</sup> The pan-Canadian info-structure was envisaged as a broad, powerful, and seamless information resource that would facilitate the integration of health services and enable continuous improvement through evidence-based decision-making and more optimal policy choices resulting from enhanced empirical research.

In the press release dated September 30, 1998, which accompanied the Advisory Council's public call for comments on its interim report *Connecting for Better Health: Strategic Issues*, Alan Rock, the then Minister of Health, was quoted as saying:

We must harness information technology to create a coherent, seamless system, one that will collect, integrate, and provide reliable and consistent information – from clinical decisions to laboratory research, from policy development to disease prevention, and from hospital management to quality control. This, I believe, will contribute to more responsible decision making by all those involved in health care.<sup>2</sup>

---

<sup>1</sup> Health Canada, News Release, "Advisory Council on Health Info-Structure established" (August 20, 1997), online: Health Canada <[http://www.hc-sc.gc.ca/ahc-asc/media/nr-cp/1997/1997\\_49\\_e.html](http://www.hc-sc.gc.ca/ahc-asc/media/nr-cp/1997/1997_49_e.html)>.

<sup>2</sup> Health Canada, News Release, 1998-65, "Advisory Council on Health Info-Structure asks Canadians for comments on interim report" (30 September 1998), online: Health Canada <[http://www.hc-sc.gc.ca/ahc-asc/media/nr-cp/1998/1998\\_65\\_e.html](http://www.hc-sc.gc.ca/ahc-asc/media/nr-cp/1998/1998_65_e.html)> [emphasis added].

In its Final Report dated February 1999, titled *Canada Health Infoway: Paths to Better Health*, the Advisory Council articulated this holistic and multi-faceted vision of a pan-Canadian health info-structure as follows:

The Canada Health Infoway empowers individuals and communities to make informed choices about their own health, the health of others and Canada's health system. In an environment of strengthened privacy protection, it builds on federal, provincial and territorial infostructures to improve the quality and accessibility of health care and to enable integrated health services delivery. It provides the information and services that are the foundation for accountability, continuous improvement to health care and better understanding of the determinants of Canadians' health.<sup>3</sup>

The Advisory Council's vision was accompanied by four strategic goals which clearly contemplated the integration of strengthened health care services and enhanced health research:

1. To empower the public by providing Canadians with equitable and affordable access to credible information, helping them make health lifestyle choices and allowing them opportunities to become involved by holding the health system accountable and providing input into health policy.
2. To strengthen and integrate health care services by providing health care professionals and providers with communication and information tools, and the supporting environment they need to improve the quality, accessibility, portability and efficiency of health care services.
3. To create strategic information resources for ensuring that Canada's health system continues to improve and becomes accountable to Canadians, including integration of standardized data to allow comparisons and new insights, expanded or new data coverage, data exchange and connectivity, increased analytical expertise and dissemination of results.
4. To improve privacy protection by harmonizing legislative rules for the use of personal health information across public and private sectors, for health care treatment as well as secondary uses such as health research.

Central to the vision of a pan-Canadian health info-structure, and critical for the achievement of its strategic goals, was the EHR.

Subsequent policy documents continued to emphasize that the integrated purposes of interoperable EHR systems included both health care and health research purposes. This continued commitment to the holistic vision of a pan-Canadian health info-structure catalyzed ongoing support for the development of interoperable EHR systems.

For example, in October 2002, the Standing Senate Committee on Social Affairs, Science and Technology, chaired by Senator Michael Kirby, released its final report titled *The Health of Canadians – The Federal Role*.<sup>4</sup> The Committee commented on EHRs as follows:

An important characteristic of an EHR system is that it can make patient data available to health care providers and institutions anywhere on a need-to-know basis by connecting interoperable databases that have adopted the required data and technical standards. Not only can an EHR system greatly improve quality and timeliness in health care delivery, it can also enhance health care system management, efficiency

---

<sup>3</sup> Advisory Council on Health Infostructure, *Canada Health Infoway: Paths To Better Health* (Ottawa: Health Canada Publications, 1999) at 6, online: Health Canada <[http://www.hc-sc.gc.ca/hcs-sss/pubs/ehealth-esante/1999-paths-voies-fin/index\\_e.html](http://www.hc-sc.gc.ca/hcs-sss/pubs/ehealth-esante/1999-paths-voies-fin/index_e.html)> [*Paths To Better Health*] [emphasis omitted].

<sup>4</sup> Standing Senate Committee on Social Affairs, Science and Technology, *The Health of Canadians – The Federal Role: Recommendations for Reform*, vol. 6 (Ottawa: October 2002) (Chair: Michael Kirby).

and accountability. Moreover, the data collected from an EHR system can provide very useful information for the purpose of health research.<sup>5</sup>

A month later in November 2002, the Romanow Commission issued *Building on Values: The Future of Health Care in Canada*.<sup>6</sup> The Romanow Report committed an entire chapter to “Information, Evidence and Ideas” and described how different “pieces of the puzzle” were linked:

To take full advantage of the potential of information, evidence and ideas in the health care system, the necessary information infrastructure must be in place. This requires action on three important fronts: putting essential information management and technology systems in place, improving our ability to assess and manage the potential benefits of health care technologies, and expanding our applied research capacity across the country. These three aspects are clearly linked. Putting the information management and technology infrastructure in place means that essential information can be collected, compiled and used to make better decisions and improve quality and care within the system. Improving our ability to assess new technology means that only the most effective new treatments, prescription drugs or equipment would be purchased and used in Canada’s health care system. With better information management and technology in place, researchers can assess the impact and value of different treatments and approaches to delivering health care services in addition to developing and testing new discoveries and cures. Together, these three “pieces of the puzzle” can create a 21st century information and evidence infrastructure that will guide and inform the future of Canada’s health care system, improve its efficiency, and most importantly, improve the health of Canadians.<sup>7</sup>

The Romanow Report went on to emphasize the importance of EHRs as “one of the keys to modernizing Canada’s health care system and improving access and outcomes for Canadians.”<sup>8</sup> In addition to ensuring that health care providers would “have access to clinical decision support tools to assist them in making decisions based on the best available evidence”,<sup>9</sup> EHRs were touted as advantageous to the extent that they would “provide aggregate data that can be used in health research and in health surveillance, tracking disease trends and monitoring the health status of Canadians.”<sup>10</sup>

## B. The Incremental Approach to Implementation

In contrast to the strategic policy advice received since 1999, which has consistently promoted the creation of an integrated, holistic health info-structure, the government’s response to implementing that vision has been more narrowly focused and deliberately incremental.<sup>11</sup>

<sup>5</sup> *Ibid.* at 175.

<sup>6</sup> Commission on the Future of Health Care in Canada, *Building on Values: The Future of Health Care in Canada* (Ottawa: November 2002) (Roy Romanow, Commissioner), online: <<http://www.hc-sc.gc.ca/english/care/romanow/index1.html>> [*Romanow Report*].

<sup>7</sup> *Ibid.* at 76.

<sup>8</sup> *Ibid.* at 77.

<sup>9</sup> *Ibid.* at 79.

<sup>10</sup> *Ibid.* at 78.

<sup>11</sup> This incremental approach seems to be typical among various countries and provinces adopting EHR systems. This approach commences with the implementation of access rules for primary use purposes. It then addresses necessary rules for allowing secondary uses of anonymized data, followed by secondary uses of identifiable data. Roy & Fournier comment:

[R]ecent discussions and documents indicate, and not only in Canada, that multiple secondary uses of PHI [personal health information] are also a core objective, not just a to-be-hoped-for serendipitous spin-off, in the creation of [national] EHRS systems. The power and knowledge that will potentially derive from access to millions of interlinked health records underpins the high expectation within many circles of society and of the health care system for secondary uses of a [national] EHRS system.

David Roy & François Fournier, *Secondary Use of Personal Information Held on National Electronic Health Record Systems: Key Developments, Issues and Concerns* (Montreal: Centre for Bioethics, Clinical Research Institute of Montreal, 2007) at 29, online: *Institut de recherches cliniques de Montréal* <[http://www.ircm.qc.ca/bioethique/english/whatsnew/EHR\\_Secondary\\_Use\\_Report.pdf](http://www.ircm.qc.ca/bioethique/english/whatsnew/EHR_Secondary_Use_Report.pdf)>. This report was prepared with funding support from the Office of the Privacy Commissioner of Canada.

Following the Final Report of the Advisory Council, First Ministers across Canada committed in September 2000 to work together to strengthen a Canada-wide health infrastructure to improve quality, access, and timeliness of health care for Canadians. This included a pledge to develop EHRs.<sup>12</sup> Specifically, this commitment resulted in the creation of Canada Health Infoway Inc. (hereafter “Infoway”) in January 2001. Infoway was incorporated as an independent, not-for-profit organization. Its membership is comprised of federal, provincial, and territorial Deputy Ministers of Health. At its inception, Infoway was mandated to “foster and accelerate the development and adoption of electronic health information systems with compatible standards and communication technologies on a pan-Canadian basis, with tangible benefits to Canadians.”<sup>13</sup>

Infoway’s annual reports and business plans reveal that the federal government has strategically ear-marked funds to drive a deliberate incremental approach to the deployment of EHRs. For instance, initial funding of \$500 million was allotted to enable the creation of five initial building blocks or target investment programs, centered primarily on facilitating the development of EHRs for care and treatment purposes:

- A common architecture and standards to ensure interoperability between EHR systems;
- client, provider and location registries;
- drug information systems;
- diagnostic imaging systems; and
- laboratory information systems.<sup>14</sup>

In February 2003, the Government of Canada increased its investment in Infoway by another \$600 million. Its mandate was expanded to include the development of a tele-health strategy to encompass the provision of health information expertise and services in various settings over distances.<sup>15</sup>

In March 2004, the Government of Canada further increased its investment in Infoway by another \$100 million to develop in collaboration with federal, provincial, and territorial governments an integrated Public Health Surveillance System. This would signal a long-term, clinically robust and permanent approach to support Canada’s increasing public health needs.<sup>16</sup>

---

<sup>12</sup> Canadian Intergovernmental Conference Secretariat (CICS), News Release, 850-089/004, “First Ministers’ Accord On Sustaining and Renewing Health Care For Canadians” (23 January 2003), online: CICS <[http://www.scics.gc.ca/cinfo03/850089004\\_e.html](http://www.scics.gc.ca/cinfo03/850089004_e.html)>. First Ministers subsequently confirmed this commitment to prioritize, further invest in, and accelerate the development of EHRs in 2003 and in 2004: see 2003 First Ministers’ Accord on Health Care Renewal, online: Health Canada <[http://www.hc-sc.gc.ca/hcs-sss/delivery-prestation/fptcollab/2003accord/index\\_e.html](http://www.hc-sc.gc.ca/hcs-sss/delivery-prestation/fptcollab/2003accord/index_e.html)>; and 2004 First Minister’s Meeting on the Future of Health Care, online: Health Canada <[http://www.hc-sc.gc.ca/hcs-sss/delivery-prestation/fptcollab/2004-fimm-rpm/index\\_e.html](http://www.hc-sc.gc.ca/hcs-sss/delivery-prestation/fptcollab/2004-fimm-rpm/index_e.html)>.

<sup>13</sup> Canada Health Infoway Inc., online: Canada Health Infoway—Who We Are <<http://www.infoway-inforoute.ca/en/WhoWeAre/Overview.aspx>>.

<sup>14</sup> Canada Health Infoway Inc., *Annual Report 2002: Accelerating the Development of Electronic Health Information Systems for Canadians* at 7, online: Canada Health Infoway <<http://www.infoway-inforoute.ca/en/ResourceCenter/ResourceCenter.aspx>>.

<sup>15</sup> Canada Health Infoway Inc., *Building Momentum: 2003/04 Business Plan* at 9, online: Canada Health Infoway <<http://www.infoway-inforoute.ca/en/ResourceCenter/ResourceCenter.aspx>>.

<sup>16</sup> Canada Health Infoway Inc., *Coming Together (2003-2004 Annual Report, Corporate Plan Summary 2004-2005)* at 12, online: <<http://www.infowayinforoute.ca/en/ResourceCenter/ResourceCenter.aspx>>.

In 2007, the federal budget invested an additional \$400 million for Canada Health Infoway. These funds will support early movement towards patient wait times guarantees through the development of health information systems and EHRs.<sup>17</sup>

Looking forward to its future agenda, Infoway seeks to have established a baseline EHR for the entire Canadian population by 2015. This would contain registries, diagnostic imaging, laboratory, medication, hospital and clinical reports, and immunization data created for every Canadian.<sup>18</sup> After this goal is met, subsequent steps will include integrating and enabling the seamless flow of information across primary care settings, enabling advanced order entry and decision support in acute care settings, and empowering patients by enabling them to be active partners in their own care.<sup>19</sup>

As a result of the incremental mandate and funding it has been given to date, Infoway's primary and overarching priority is focused on deploying EHRs to enable the sharing of information among *providers* of direct patient care. Meanwhile, legislators, policy-makers, system vendors, and developers have yet to articulate, both in principle and in practice, how EHRs will eventually support and enable health research. Use of EHRs for secondary health research purposes was originally conceived of as a pillar and driver of improved health care and is still recognized as something that will eventually happen.<sup>20</sup> Indeed, health research has been identified as an eventual component of the overall architecture.<sup>21</sup> However, how that will be operationalized and under what conditions have yet to be worked out.<sup>22</sup>

A number of recent initiatives across the country have begun to address the secondary use of EHR data. A pan-Canadian Privacy Forum was launched in November 2007. The Forum,

---

<sup>17</sup> Department of Finance Canada, *The Budget Plan 2007: Aspire to a Stronger, Safer, Better Canada* (Ottawa: Public Works and Government Services Canada, 2007) at 59, online: Department of Finance Canada <<http://www.budget.gc.ca/2007/pdf/bp2007e.pdf>>.

<sup>18</sup> Canada Health Infoway Inc., *2015: Advancing Canada's Next Generation of Healthcare* (Toronto: Canada Health Infoway Inc., 2005) at 24, online: Canada Health Infoway Inc. <<http://www.infoway-inforoute.ca/en/ResourceCenter/ResourceCenter.aspx>> [Canada Health Infoway Inc., 2015].

<sup>19</sup> *Ibid.* at 16.

<sup>20</sup> Canada Health Infoway Inc., *Building on our Successes: Corporate Business Plan 2005-06* at 14, online: Canada Health Infoway <<http://www.infoway-inforoute.ca/en/ResourceCenter/ResourceCenter.aspx>>. The report suggests the need to continue to widen the circle by engaging "new stakeholder groups," such as patients and researchers, in order to extend the reach of electronic health record solutions. See also Canada Health Infoway Inc., *EHRs Blueprint: an interoperable EHR framework, Version 2*, April 2006, online: Canada Health Infoway <<http://www.infoway-inforoute.ca/en/WhatWeDo/Infostructure.aspx>> [Canada Health Infoway Inc., *EHRs Blueprint, version 2*] which recognizes at 5 that "[w]hile [patient care] is the primary goal of the EHR Infostructure, a lot can be said for the healthcare value derived from being able to use this information for research, analysis and health prevention initiatives." "[O]ne of the great dimensions of value of the EHR for the healthcare system", the *EHR Blueprint* further states at 41, "is its ability to provide data (de-identified or not) for authorised secondary uses such as surveillance, research ...".

<sup>21</sup> Canada Health Infoway Inc., *Electronic Health Records Infostructure (EHRi) Privacy and Security Conceptual Architecture, Version 1.1* (June 2005) at 62, online: Canada Health Infoway Inc. <<http://knowledge.infoway-inforoute.ca/EHRSRA/doc/EHR-Privacy-Security.pdf>>. See also Canada Health Infoway Inc., *EHRs Blueprint version 2*, *ibid.* at 5, which anticipates health research as a future potential application that will require a separate and interoperable deployment model with the capability of compiling, aggregating, and consolidating EHR data. The *Blueprint* document goes on to contemplate, at 10, that from an architectural standpoint, "[t]he data stored in the EHRi will be optimized for patient/client driven access performed by healthcare professionals in the context of providing services to individuals. This is usually not very conducive for research and statistical analysis types of applications that need to perform queries addressing large subsets of data. In most cases, to sustain the purposes of research and analysis, it is understood that the preferred approach would be to extract large sets of data from the EHRi and load such data into the Health Information Data Warehouse where it can be optimized and massaged for research purposes."

<sup>22</sup> See Canada Health Infoway Inc., *White Paper on Information Governance of the Interoperable Electronic Health Record (EHR)* (Toronto: Canada Health Infoway Inc., 2007) at 14, which identifies as an issue the fact that "there are no agreed-upon best practices for informing patients in a readily understandable manner about the secondary uses of their personal health information. Current practices vary among jurisdictions and healthcare institutions."

created and facilitated by Infoway, is comprised of representatives from privacy oversight bodies and ministries of health across various jurisdictions. The Forum is exploring a variety of information governance topics from a policy perspective, including the secondary use of EHR data. Moreover, legislators in some provinces have begun adopting mechanisms, such as the creation of special data stewardship committees, to manage disclosure of information contained in various health data banks for health planning and research purposes.<sup>23</sup>

Even as legislators, policy-makers, system developers and interested stakeholders are now beginning to turn their minds to health research after several years of silence on the issue, it appears as though a fissure has developed between access to EHRs by health care providers for the purpose of integrating the delivery of health care, and the related use of EHRs by health researchers for the purpose of improving the quality of Canadians' health and health care services.

### C. Privacy Implications of the Incremental Approach

While there are many sound business reasons for adopting an incremental approach to the development of a pan-Canadian health info-structure—indeed, some could plausibly argue there is simply no other practical, feasible way to implement such huge information technology initiatives—such an approach has important implications for privacy protection.

For one, privacy legislation typically requires that consent for the use of personal information, for any anticipated purpose, be provided at or before the time personal information is collected with full knowledge of the purposes for which the personal information will be used.<sup>24</sup> Yet, EHR data are currently being collected based solely on individuals' implied and potentially qualified<sup>25</sup> consent for health care purposes. These consent processes are completely silent with respect to the possible research uses that may be made of the data. Once research uses are eventually enabled, as it seems they inevitably will be, the opportunity to obtain consent up front at the time of collection will have been missed. This will require that individuals provide consent all over again *before* researchers can access the data, lest a fundamental data protection principle be violated. Given the sheer size of the Canadian population, re-contacting every individual in order to obtain his or her consent for research uses of their EHR data already seems pre-ordained as an impracticable option.

Additional complexity is introduced by the technological design choices that must presently be made as EHR solutions are developed and strategic investment funds are being committed and spent.<sup>26</sup> Deferring questions about the eventual use of EHR data for health research purposes, while at the same time accelerating the implementation of interoperable EHR systems, may require the costly re-engineering of existing or legacy information systems when these issues do eventually get addressed. Managing consent directives, creating consent registries, designating authorized researchers, controlling access rights based on pre-determined conditions, creating appropriate governance structures, and implementing de-identification capabilities are just some of the many outstanding design features that will be difficult to build in after the fact.

---

<sup>23</sup> See *e.g.* *E-Health (Personal Health Information Access and Protection of Privacy) Act*, S.B.C. 2008, c. 38.

<sup>24</sup> See *e.g.* *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5, Sch. 1, s. 4.3 Principle 3—Consent.

<sup>25</sup> Some jurisdictions permit individuals to qualify their consent to the collection, use, and disclosure of personal health information through the use of possible opt-out mechanisms such as masking, “lock-box,” and other options.

<sup>26</sup> Michael Wolfson, Assistant Chief Statistician of Statistics Canada, comments: “Secondary uses [of EHR data] should be co-equal with primary uses – they should be planned, for example in terms of architectures and functional requirements, just as much as primary uses.” Roy & Fournier, *supra* note 11 at 22.

While the law does allow consent exceptions for research under certain conditions, these conditions vary significantly from jurisdiction to jurisdiction. Infoway identifies privacy and consent legislation as a key enabler of its ultimate vision for health information technology in Canada.<sup>27</sup> This echoes the Advisory Council's 1999 indication that harmonizing legislative rules for the use of personal health information for both care and research purposes would be essential for realizing the vision of a Canadian health info-structure.<sup>28</sup> Yet to date, policy-makers have predominantly focused on harmonizing legal requirements around an implied or deemed consent model to enable the integration and interoperability of health care services. The need to harmonize legal rules around secondary uses such as health research continues to be overlooked, despite the fact that privacy and consent norms as currently conceived in Canadian law are neither amenable to, nor in some cases capable of, retrospective application.

Meanwhile, even as many of these legal and technological issues remain outstanding, the pressure to access what will eventually become invaluable "cradle to grave" EHR data for research purposes continues to mount. Several authors anticipate that the scale of secondary use of information will increase substantially as EHRs become more pervasive.<sup>29</sup> Some have described this trend as follows:

[I]n a context where "the volume of data in an EHR may lead to increased pressure by analysts and researchers to access the information", there may be mounting pressure to render health information governance – structures, legislation, policies, practices – more "flexible" to allow optimal exploitation of health information rich EHRs for the benefit of the 'common good' ....

...

The multipurpose value of health information stimulates the appetites of governments, researchers, health-care planners, administrators, insurers, and others for more and ever more data. This phenomenon is bound to become more apparent as EHR systems are more widely established and become more effectively interoperable.<sup>30</sup>

As long as the issue of consent for the use of EHRs for health research purposes remains outstanding, this massive treasure trove of valuable data for health research will linger in legal and ethical limbo.

In the remainder of this paper, we describe the legal rationale for consent as a means of controlling access to one's EHR data for health research purposes. We explain why informed consent remains the default legal standard for research use of personal information irrespective of the method used. In view of the growing recognition that informed consent may not always be a feasible standard for all types of health research, we then consider a number of other policy alternatives which deviate from the informed consent model and have yet to be more fully explored in an open, transparent, and inclusive public policy debate. These alternatives range from introducing a broad consent model for future, yet unspecified research purposes; de-identifying data and removing them altogether from the scope of application of data protection laws; extending the implied consent model by reconceptualizing research as

---

<sup>27</sup> Canada Health Infoway Inc., 2015, *supra* note 18 at 24.

<sup>28</sup> *Paths To Better Health*, *supra* note 3 at 11: "... legislation should define what constitutes informed consent, as well as provide a clear statement of principle to the effect that informed consent should be the basis for sharing information. It should define 'exemptions' to this requirement for informed consent and give clear guidance on how to balance the right of privacy with the public good for research purposes."

<sup>29</sup> Donald J. Willison *et al.*, "Alternatives to Project-specific Consent for Access to Personal Information for Health Research: What Is the Opinion of the Canadian Public?" (2007) 14:6 *Journal of the American Medical Informatics Association* 706 at 707. See also Khaled El Emam *et al.*, *Pan-Canadian De-Identification Guidelines for Personal Health Information* (Ottawa: Children's Hospital of Eastern Ontario Research Institute, 2007), at 3 and 6-7, online: Electronic Health Information Laboratory <<http://www.ehealthinformation.ca/documents/OPCReportv11.pdf>> [El Emam *et al.*, "Pan-Canadian"]. This report was prepared with funding support from the Office of the Privacy Commissioner of Canada.

<sup>30</sup> Roy & Fournier, *supra* note 11 at 28-29. See various excerpts cited by the authors at 32 for further support for this projected phenomenon.



part of the primary health care purpose; resorting to statutory consent exemptions for research purposes; and amending legislation to retroactively eradicate the need for consent altogether.

By setting out a range of policy options to address research use of EHR data and discussing the implications of these options, this paper aims to support informed deliberations about available choices before technological imperatives predetermine the selection for us.

## II

### INFORMED CONSENT AS A DEFAULT STANDARD FOR RESEARCH

Informed consent is a fundamental pillar of most, if not all, modern data protection regimes recognized internationally. In Canada, all federal, provincial, and territorial data protection laws start from the general proposition that personal information should only be collected, used, and disclosed with the consent of the individual to whom it relates.<sup>31</sup> In some cases, data protection legislation expressly specifies certain conditions that must be satisfied for consent to be valid. Typically, consent must be informed, revocable, given freely and obtained lawfully, and without deception.<sup>32</sup> While every regime incorporates various exemptions to this requirement, informed consent remains the default expectation whenever information that can identify persons will be collected, used, or disclosed.

Informed consent, as a key component of data protection legislation, represents a concrete and express manifestation of the fundamental principles of individual autonomy, dignity, and liberty that have emerged as the basis for the protection of personal information at common law<sup>33</sup> and the right to privacy under the *Canadian Charter of Rights and Freedoms*.<sup>34</sup> In this

---

<sup>31</sup> Patricia Kosseim, Adam Kardash & Antonella Penta, eds., *Compendium of Canadian Legislation Respecting the Protection of Personal Information in Health Research*, 2d ed. (Ottawa: Public Works and Government Services Canada, 2005) at 129-67, online: CIHR <[http://www.cihr-irsc.gc.ca/e/documents/ethics\\_privacy\\_compendium\\_june2005\\_e.pdf](http://www.cihr-irsc.gc.ca/e/documents/ethics_privacy_compendium_june2005_e.pdf)>.

<sup>32</sup> *Ibid.* at 129.

<sup>33</sup> The common law governing the confidentiality of the physician-patient relationship is particularly relevant here. EHR data, unlike other data sources, such as administrative databases for example, will always run up against the inescapable aura of confidence which surrounds this data at common law. EHR data by its inherent nature is highly sensitive, and will have originated in the context of the fiduciary relationship between patient and health service provider. This relationship of trust imports a clearly defined duty on the part of the health service provider to keep the information confidential, and a corresponding expectation on the part of the patient that this confidence will be respected—particularly if no discussion of other possible uses has taken place. By confiding personal information to their provider in this context, patients can reasonably expect that their interest in, and control over, their EHR data will continue no matter where the data ultimately flow.

<sup>34</sup> *Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (U.K.), 1982, c.11 [*Charter*]. *Charter* jurisprudence helps inform a consideration of the standard of consent that would apply to the use of personal health information in electronic health records for health research purposes for a number of reasons. First, *Charter* jurisprudence informs the acceptable limits on the reasonable expectation of privacy as balanced against other legitimate societal needs (*R. v. O'Connor*, [1995] 4 S.C.R. 411) [*O'Connor*]. Second, the *Charter* may apply directly to the actions of certain government actors involved in the health research enterprise such as government sponsors of health research and, where there are sufficient indicia of government control, hospitals or universities (*Eldridge v. British Columbia (Attorney General)*, [1997] 3 S.C.R. 624 at para. 43; *Douglas/Kwantlen Faculty Assn. v. Douglas College*, [1990] 3 S.C.R. 570). Third, the *Charter* may further apply to statutorily-created bodies charged with interpreting and applying data protection legislation, such as research ethics boards, since legislators cannot permit administrative decision-makers to do indirectly that which legislators cannot do directly (*Slaight Communications Inc. v. Davidson*, [1989] 1 S.C.R. 1038; see also *Blencoe v. British Columbia (Human Rights Commission)*, [2000] 2 S.C.R. 307). Fourth, *Charter* values will inform the interpretation and application of legislation or the common law where there is any ambiguity (*R. v. Rube*, [1992] 3 S.C.R. 159 at 160; *R. v. Salituro*, [1991] 3 S.C.R. 654 at 678). This may be particularly relevant given the ambiguity that exists in most data protection laws in respect of the conditions necessary for consent to be truly valid, and for the various research exemptions to apply. Finally, over and above the extent to which *Charter* values or the *Charter* itself may be invoked to inform the validity, interpretation, and application of data protection statutes, *Charter* values are relevant to the debate about access to EHRs for research purposes simply to the extent that they represent a concrete expression of fundamental social values and the reasonable expectation of privacy in modern society.

section, we set out to explain why informed consent constitutes the default statutory requirement for the collection, use, and disclosure of personal information for health research purposes, whatever the research method used.

#### A. Clinical Research

Clinical research typically involves an experimental intervention which deviates from the recognized standard of medical care. This could include the administration of a new drug, a new use of an existing drug, a novel medical device, or an innovative prophylactic, diagnostic, or surgical procedure in order to test for safety and efficacy in comparison with the standard course of diagnosis or treatment. Because clinical research tends to involve some physical interference with the human body, the legal requirement for informed consent is generally incontrovertible.<sup>35</sup>

Informed consent to medical interventions is a longstanding requirement of the traditional physician-patient relationship; it constitutes the legal means by which patients exercise their fundamental right to control what is done or not done with their body.<sup>36</sup> To render the necessary consent meaningful, a physician must answer any specific questions posed by the patient as to the risks involved and must disclose, without being asked, the nature of the proposed intervention, its gravity, any material risks and any special or unusual risks attendant upon the performance of the operation. The contours of the physician's duty of disclosure are defined by what a reasonable person in the patient's particular position would want to know and understand in order to make an informed choice about whether or not to undergo the proposed intervention.<sup>37</sup>

In the clinical research context, the proposed intervention is not carried out exclusively for the benefit of the individual patient, but for the potential benefit of society as a whole. In this context, a researcher's duty to disclose risks associated with a research intervention is even more exacting than the duty owed by the ordinary physician providing standard medical care. In one of the very few Canadian cases dealing with this question, the Saskatchewan Court of Appeal determined that:

... [t]here can be no exceptions to the ordinary requirements of disclosure in the case of research as there may well be in ordinary medical practice ... The subject of medical experimentation is entitled to a full and frank disclosure of all the facts, probabilities and opinions which a reasonable man might be expected to consider before giving his consent.<sup>38</sup>

In *Weiss v. Solomon*, the Quebec Superior Court held that the researcher conducting experimental treatment must specify *all* risks, no matter how rare or remote, especially when those risks may have grave consequences. This disclosure, of course, remains subject to review and approval by an institutional research ethics board charged with verifying whether or not the threshold is met for each research protocol.<sup>39</sup>

Clearly, for clinical research which potentially involves some intervention which is not the recognized standard diagnosis or treatment, and which is not carried out for the exclusive benefit of the individual, the doctrine of informed consent requires the researcher to meet that

---

<sup>35</sup> Although the requirement of informed consent in the context of clinical research is well-established and accepted as a matter of principle, its application in practice continues to preoccupy research ethics boards and regulators as they struggle to review lengthy and protracted consent forms.

<sup>36</sup> This principle was encapsulated in a well-known statement by Cardozo J. in *Schloendorff v. Society of New York Hospital*, 211 N.Y. 125, 105 N.E. 92 (1914): "Every human being of adult years and sound mind has a right to determine what shall be done with his own body; and a surgeon who performs an operation without his patient's consent commits an assault for which he is liable in damages."

<sup>37</sup> *Hopp v. Lepp*, [1980] 2 S.C.R. 192 and *Reibl v. Hughes*, [1980] 2 S.C.R. 880 at 899-900.

<sup>38</sup> *Halushka v. University of Saskatchewan et al.* (1965), 52 W.W.R. 608 at 616 (Sask. C.A.).

<sup>39</sup> *Weiss v. Solomon*, [1989] A.Q. 312 (Qc. Sup. Ct.).

higher threshold of disclosure before consent will be found to be valid.<sup>40</sup> Moreover, because clinical research aims to use information about the individual's health outcome in order to advance general societal knowledge, the additional risks to privacy and confidentiality have also become part of that higher cluster of risks which the researcher must impart to potential research subjects in order to inform their consent to participate in the research. In accordance with widely accepted international ethical principles for clinical research, researchers have a duty to protect not only the life and health of human research subjects, but their privacy and dignity as well: "[e]very precaution should be taken to respect the privacy of the subject, the confidentiality of the patient's information and to minimize the impact of the study on the subject's physical and mental integrity and on the personality of the subject."<sup>41</sup>

But what of research which involves solely the collection, use, or disclosure of personal information, with no clinical intervention *per se*? Does the same default requirement of informed consent apply or is a different standard of consent warranted in such circumstances?

### B. Epidemiological Research

Epidemiological studies are primarily designed to monitor health patterns or trends among large-scale populations; identify potential determinants of health or causes of disease; evaluate the cost-effectiveness of health services; assess the quality and impact of treatments, prevention strategies, or policies; and/or assemble study populations.<sup>42</sup> These types of studies typically depend on access to already-existing health records originally created for treatment purposes, such as hospital, physician, laboratory, or pharmaceutical records. These health records might then be linked with other existing administrative databases originally created for other purposes, such as provincial and federal billing and registration data; birth and death records; socio-demographic data; cancer registry data; and employment records. This research method involves mostly data analyses with no need to enter into direct contact with the individuals involved. In some cases, however, individuals may be contacted in order to carry out a survey either by telephone, in writing, or in person, to collect further qualitative data from research participants about their perceptions of their own health, their assessment of the health system, their quality of life, behavioural or lifestyle factors, or other relevant information.

Even though this research method does not typically involve any physical intervention, like in clinical research, informed consent remains the default legal requirement. This is because the courts have recognized, both at common law and under the *Charter*, that every individual has the fundamental right to control not only what shall be done with his or her body, but also *the right to control what is done with his or her personal information*.

At common law, medical records are recognized as repositories of highly private personal information to which legitimate expectations of privacy and confidentiality attach. Control over

---

<sup>40</sup> Ellen I. Picard & Gerald B. Robertson, *Legal Liability of Doctors and Hospitals in Canada*, 3rd ed. (Toronto: Carswell, 1996) at 150.

<sup>41</sup> World Medical Association, *World Medical Association Declaration of Helsinki: Ethical Principles for Medical Research Involving Human Subjects*, adopted by the 18th WMA General Assembly, Helsinki, Finland, June 1964, and amended by the 29th WMA General Assembly, Tokyo, Japan, October 1975, 35th WMA General Assembly, Venice, Italy, October 1983, 41st WMA General Assembly, Hong Kong, September 1989, 48th WMA General Assembly, Somerset West, Republic of South Africa, October 1996 and the 52nd WMA General Assembly, Edinburgh, Scotland, October 2000, note of clarification on Paragraph 29 added by the WMA General Assembly, Washington 2002, and note of clarification on Paragraph 30 added by the WMA General Assembly, Tokyo 2004 [*Declaration of Helsinki*], online: World Medical Association <<http://www.wma.net/e/policy/pdf/17c.pdf>>.

<sup>42</sup> See Canadian Institutes of Health Research, *Secondary Use of Personal Information in Health Research: Case Studies* (Ottawa: Public Works and Government Services Canada, 2002) for a fuller description and concrete examples of research studies which rely on secondary use of data, online: Canadian Institutes of Health Research <[http://www.cihr-irsc.gc.ca/e/pdf\\_15568.htm](http://www.cihr-irsc.gc.ca/e/pdf_15568.htm)>.

one's personal information is a defining principle of the doctor-patient relationship. It underlies a patient's rights and a health provider's corresponding obligations in Canadian medical law. In 1928, the Supreme Court of Canada had little difficulty confirming that a patient has a *prima facie* right to confidentiality in the medical "secrets" kept between himself and his physician. The Court held that "that right is absolute, unless there is some paramount reason which overrides it."<sup>43</sup>

In the seminal case of *McInerney v. MacDonald*,<sup>44</sup> the Supreme Court of Canada elevated the legal protection afforded to medical information by recognizing the doctor-patient relationship as a special relationship of trust. The physician's fiduciary duties include the duty to act with utmost good faith and loyalty in the best interests of his patients, to keep patients' personal information confidential, and to provide patients with access to their own personal information. The patient who entrusts highly sensitive and personal information to a physician does so with the legitimate expectation that the physician will respect these duties. The patient has a continuing interest in what happens to the personal information he shares with his physician and in retaining control over others' access to it; this personal information remains in a fundamental way his own and his interest in that personal information continues even as his physician shares it with other health providers.<sup>45</sup>

The case of *R. v. Dyment* is also instructive with respect to the question of non-consensual secondary uses of personal health information originally collected for medical treatment and subsequently used for a different purpose. In *R. v. Dyment*, a physician collected, for medical purposes, a vial of free-flowing blood from a car accident victim. Mr. Dyment, who was unconscious at the time, did not consent to the taking of his blood sample. When the patient later explained that he had consumed a beer and medication before the accident, the physician offered the blood sample to police in the absence of a warrant. In determining that this transaction resulted in an unconstitutional search and seizure within the meaning of section 8 of the *Charter*, Justice La Forest held that Mr. Dyment

may, for some purposes perhaps, be deemed to have impliedly consented to a sample being taken for medical purposes, but he retained an expectation that his privacy interest in the sample continue past the time of its taking. Indeed, the doctor, in extracting the blood, placed himself in a situation where, pursuant to professional ethics and likely to hospital management regulations as well, he was charged with a duty to use the blood only for medical purposes. Under these circumstances, the sample was surrounded by an aura of privacy ...<sup>46</sup>

In so finding, La Forest J. considered and adopted what was then the novel proposition that there are three equally important zones of privacy—territorial, personal, and informational. An individual has not only the right to assert autonomous control over her own property or person, she also has the right to assert autonomous control over her personal information. La Forest J., borrowing from the work of a 1972 Task Force established jointly by the Departments of Communications and Justice,<sup>47</sup> concluded that information, like one's property or person, warrants privacy protection:

Finally, there is privacy in relation to information. This too is based on the notion of the dignity and integrity of the individual. As the Task Force put it (p. 13): "This notion of privacy derives from the assumption that all information about a person is in a fundamental way his own, for him to communicate or retain for himself as he sees fit." In modern society, especially, retention of information about oneself is extremely important. We may, for one reason or another, wish or be compelled to reveal such information, but situations abound where the reasonable expectations of the individual that the information shall remain confidential to the persons to whom, and restricted to the purposes for which it is divulged, must be

---

<sup>43</sup> *Halls v. Mitchell*, [1928] S.C.R. 125 at 136.

<sup>44</sup> [1992] 2 S.C.R. 138 [*McInerney v. MacDonald*].

<sup>45</sup> *Ibid.* at para. 22.

<sup>46</sup> [1988] 2 S.C.R. 417 at para. 31 [*Dyment*].

<sup>47</sup> Canada, Report of a Task Force established jointly by the Department of Communications/Department of Justice, *Privacy and Computers* (Ottawa: Information Canada, 1972) [*Privacy and Computers*].

protected. Governments at all levels have in recent years recognized this and have devised rules and regulations to restrict the uses of information collected by them to those for which it was obtained. See, for example, the *Privacy Act*, S.C. 1980-81-82-83, c. 111.<sup>48</sup>

From this line of reasoning, a legal conception of privacy has emerged that may be best crystallized as the *prima facie* right to choose for oneself what is done with one's information. As the Supreme Court of Canada stated in the 1990 decision *R. v. Duarte*: “[p]rivacy may be defined as the right of the individual to determine for himself when, how, and to what extent he will release personal information about himself.”<sup>49</sup> This right attaches to “all information about a person”<sup>50</sup> and not merely information that may objectively be deemed to be sensitive or worthy of privacy protection.

Also of note is the fact that the right to assert autonomous control over one's personal information, like one's personal space and effects, requires preemptive protection. The Supreme Court has emphasized that section 8 of the *Charter* “requires a means of preventing unjustified searches before they happen, not simply of determining, after the fact, whether they ought to have occurred in the first place. This, in [the Court's] view, can only be accomplished by a system of prior authorization, not one of subsequent validation.”<sup>51</sup> Like the need to obtain a warrant in the law enforcement context, the requirement to obtain prior informed consent to the collection, use, and disclosure of personal information has evolved as a legal safeguard intended to proactively protect privacy and protect against unauthorized and unjustified intrusions that may not be remediable.

In various contexts, Canadian jurisprudence has clearly and consistently recognized that individuals maintain a legitimate expectation of privacy in and control over their personal health information and health records. This standard of autonomous control is manifested in data protection regimes as the legal requirement to obtain prior informed consent to the collection, use, and disclosure of personal information. Though deviation from this recognized legal standard may be desirable for certain types of health research, such as epidemiological research for instance, it must be justified and warranted in law according to clear terms and conditions.

### C. Creation of Research Platforms

Given rapid advances in information technology, the explosion of genomic research and the growing movement towards data sharing and integration, the health research enterprise is increasingly turning towards the creation of large-scale research registries, repositories, or data warehouses which collect data on whole populations or sub-populations and serve as platforms for future research. Once these platforms are created, they enable researchers to subsequently draw on the same source of data to carry out what could be hundreds of individual research projects and/or to assemble study cohorts—for yet further potential research. These platforms could be national or sub-national in scope; they could be of a specialized nature to study potential determinants of a specific disease or more wide-ranging in nature to assess the health status of populations in general. They could be designed on a cross-sectional basis, which would involve the collection of data at a single point in time, or on a longitudinal basis, which would involve ongoing data collection in order to study health changes in the cohort population over long periods of time. Finally, these research platforms may involve the additional collection of biological samples, particularly given the increasing importance of understanding underlying genetic factors and their impact on the health status and/or disease susceptibility of populations.

---

<sup>48</sup> *Dyment, supra* note 46 at 429.

<sup>49</sup> *R. v. Duarte*, [1990] 1 S.C.R. 30 at 46.

<sup>50</sup> *Dyment, supra* note 46 at 429.

<sup>51</sup> *Ibid.* at 430, citing Dickson J. in *Hunter v. Southam Inc.*, [1984] 2 S.C.R. 145 at para. 27 [emphasis omitted].

In our view, and for the reasons set out above, the requirement to obtain informed consent for the prospective collection of data (including biological samples) directly from the study population for inclusion in a research platform continues to apply as the default legal standard. However, the issue which arises in this context is whether broad, general consent for all future research purposes is sufficient, or whether specific, informed consent is legally required each time an individual research project is carried out using data from the research platform. As will be canvassed below, there may be valid policy reasons not to require specific, informed consent for each individual research project, given the difficulty inherent in re-contacting individuals and the significant impediment this may have on important research. Nonetheless, a review of the common law and *Charter* jurisprudence may help us to understand why informed consent appears to be the default standard for each research project, and why any departure from this standard must be justified.<sup>52</sup>

An individual's freedom to make decisions of fundamental personal importance free from state interference is protected under s. 7 of the *Charter*. In *R. v. Morgentaler*, Wilson J. explored the contours of the section 7 right to liberty. Adopting an expansive and purposive approach, Wilson J. described the right to liberty as being linked to human dignity and the right to exercise autonomy in making private choices:

[A]n aspect of the respect for human dignity on which the *Charter* is founded is the right to make fundamental personal decisions without interference from the state. This right is a critical component of the right to liberty. Liberty, as was noted in *Singh*, is a phrase capable of a broad range of meaning. In my view, this right, properly construed, grants the individual a degree of autonomy in making decisions of fundamental personal importance.<sup>53</sup>

I would conclude, therefore, that the right to liberty contained in s. 7 guarantees to every individual a degree of personal autonomy over important decisions intimately affecting their private lives.<sup>54</sup>

In subsequent cases, the Supreme Court further specified that the relevant sphere of personal autonomy encompasses those matters that can be characterized as being “fundamentally or inherently personal such that, by their very nature, they implicate basic choices going to the core of what it means to enjoy individual dignity and independence.”<sup>55</sup>

EHRs contain data which are fundamentally and inherently personal.<sup>56</sup> They reveal sensitive information about highly personal issues like one's physical health, mental health, family situation, and genetic make-up. The decision to disclose such highly sensitive information, including biological samples, for some research purposes and not others may in

---

<sup>52</sup> Timothy Caulfield and Nola Ries likewise conclude from their review of Canadian common law that “given the ever expanding details required in order to make a consent properly informed, especially in relation to research, and given that it will be impossible for the initial consent to contain information about specific research projects, it seems fair to conclude that, from a technical legal perspective, a re-consent will often be required.” See Caulfield & Ries, “Consent, Privacy and Confidentiality in Longitudinal, Population Health Research: The Canadian Legal Context” (Supplement, 2004) Health L.J. 1 at 29.

<sup>53</sup> *R. v. Morgentaler*, [1988] 1 S.C.R. 30 at 166.

<sup>54</sup> *Ibid.* at 171.

<sup>55</sup> *Godbout v. Longueuil (City)*, [1997] 3 S.C.R. 844 at para. 66 [*Godbout*]. See also *R. v. Malm-Levine*; *R. v. Caine*, 2003 SCC 74, [2003] 3 S.C.R. 571 [*Malm-Levine*].

<sup>56</sup> See *McInerney v. MacDonald*, *supra* note 44 at 148: “Of primary significance is the fact that the records consist of information that is highly private and personal to the individual. It is information that goes to the personal integrity and autonomy of the patient.” See also *O'Connor*, *supra* note 34 at para. 118, citing *R. v. Plant*, [1993] 3 S.C.R. 281 at 293: “[Section] 8 of the Charter should seek to protect a biographical core of personal information in which individuals in a free and democratic society would wish to maintain and control from dissemination to the state. This would include information which tends to reveal intimate details of the lifestyle and personal choices of the individual.’ Although I prefer not to decide today whether this definition is exhaustive of the right to privacy in respect of all manners of documents and records, I am satisfied that the nature of the private records which are the subject matter of this appeal properly brings them within that rubric. Such items may consequently be viewed as disclosing a reasonable expectation of privacy which is worthy of protection under s. 7 of the Charter.” [Emphasis omitted.]

some cases be based on one's deeply personal and moral beliefs. Such decisions could be regarded as falling within that "irreducible sphere of personal autonomy wherein individuals may make inherently private choices free from state interference" and which, by their very nature, implicate basic choices "going to the core of what it means to enjoy individual dignity and independence."<sup>57</sup>

Accepting this premise, the jurisprudence surrounding the liberty interest in section 7 may serve as a guide for giving meaningful effect to individuals' reasonable expectations of privacy and control over decisions of such fundamental personal importance. In order for individuals to exercise their right to make such personal and private choices about what research can be carried out or not with their personal information, they must be able to turn their minds to each specific research study and evaluate for themselves the worthiness of the research aim, the legitimacy of the hypothesis, the potential uses to which the results will be put, and the degree to which they themselves wish to personally contribute to that particular research venture. Will the research be for commercial or non-commercial purposes? Could it have as a possible outcome the denial of coverage and accessibility to certain treatments that prove to be economically non-viable and highly risky, but for some, represent their only hope for survival? Could the research possibly result in the development of standardized genetic screening tests that might over time affect the biological diversity of human life as we presently know it? Does the research involve controversial reproductive technologies that some might find acceptable and even necessary, while others might find morally reprehensible? Will the research have the potential of uprooting communities, disrupting their self-dependence and exploiting their traditional ways of life? Might research results pertaining to the health characteristics of certain groups lead to possible discriminatory practices?

One option is to obtain from individuals a single, broad consent to the use of personal data for research and then entrust to research ethics boards the responsibility for reviewing and approving specific projects in accordance with widely accepted ethical principles and governing conditions of the research platform. Such a broad consent, however, though made freely, may not constitute informed consent in law. Research participants cannot provide their informed consent if they have no knowledge of what they are consenting *to*. One cannot truly consent to that which is unascertained and thus unknown.

As will be discussed below, there may be persuasive public policy reasons for moving towards a broad consent model—not the least of which are the sheer practical issues associated with informed consent processes on a project-specific basis. However, the liberty interest engaged by such fundamentally and inherently personal choices regarding what use may be made of one's highly sensitive personal information is sufficiently strong that it must, in our view, continue to inform the default standard of consent, and any departure therefrom must be legally justifiable.

### III

#### POLICY OPTIONS FOR ALLOWING RESEARCH USE OF EHRs

The common law and *Charter* jurisprudence governing the privacy and confidentiality of personal information surveyed above relies directly or inferentially on informed consent as a proxy for the legal protection afforded to fundamental principles of autonomy, human dignity, and liberty. These foundational principles of human dignity, liberty, and autonomous control over personal information inhere in the rights of the individual. Their relevance and application seem to persist irrespective of the proposed research use or method.

---

<sup>57</sup> *Godbout*, *supra* note 55 at para. 66.

As canvassed above, informed consent in the context of *clinical* research is grounded in the right to control what shall be done with one's body and to limit undue physical intrusions upon the person. In the context of *retrospective* research involving secondary use of data originally collected for a purpose unrelated to the objective of the secondary use research, informed consent is grounded in the *right to control what is done with one's personal information and to limit unjustified invasions of one's reasonable expectation of privacy*. In the context of *prospective* research studies based on data collected for the purpose of creating a research registry or platform, informed consent arguably remains the default standard as well, based on the *right to exercise autonomy over decisions affecting fundamentally important aspects of one's life*.

As a result, the jurisprudence suggests that it may be difficult, as a matter of principle and absent justifiable reasons, to shift away from the concept of "informed consent" as the default standard for access to EHR data for research purposes, even absent clinical intervention.

We now turn to a discussion of a range of policy options that may be available to address the dual need to respect the fundamental principle of informed consent, while at the same time, enable access to EHR data for health research purposes. We begin with the option of informed consent which is most closely aligned with the current state of the law. We then explore other, more feasible, policy alternatives that may inevitably be required by the continued, incremental deployment of EHRs. Each of these policy alternatives has significant implications that need to be carefully considered.

#### A. Obtaining Informed Consent for Each Specific Research Study

In keeping most closely with the prevailing standards set out above, the first policy option is maintaining and complying with the current default rule, informed consent.

As we have seen, this standard of consent would require the researcher to provide, at a minimum, the information necessary for an individual to maintain a continuing interest in what happens to his personal information. In order to provide individuals with a meaningful opportunity to exercise their right to consent or withhold or revoke consent on an ongoing basis, the health researcher would have a corresponding and continuing duty to disclose sufficient information about the specific research study being proposed and its evolution.<sup>58</sup>

The informed consent model seems to require that researchers create and maintain the conditions required for individuals to retain control over access to their personal information. The researcher must give practical meaning to the legal imperative which asserts that the individual's "information remains in a fundamental way his own, for him to communicate or retain for himself as he sees fit."<sup>59</sup> The individual must be able to decide for himself, with sufficient autonomy and without interference by others, when, how, and to what extent he will release his personal information for a specific purpose that cannot be extended to other

---

<sup>58</sup> Prior to researchers establishing direct contact with patients, many health information statutes and ethics guidelines require that health service providers or health information custodians obtain *prior* consent in order to permit the disclosure of contact and other identifiable information to researchers before they may enter into communications with patients for the purposes of recruitment. See e.g. *Health Information Act*, R.S.A. 2000, c. H-5, s. 55 [HIA]; *Personal Health Information Protection Act*, S.O. 2004, c. 3, s. 44(6)(e) [PHIPA]. Canadian Institutes of Health Research, Natural Sciences and Engineering Research Council & Social Sciences and Humanities Research Council, *Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans* (1998, with 2000, 2002, and 2005 amendments), online: Interagency Advisory Panel on Research Ethics <[http://www.pre.ethics.gc.ca/english/pdf/TCPS%20October%202005\\_E.pdf](http://www.pre.ethics.gc.ca/english/pdf/TCPS%20October%202005_E.pdf)>; and Canadian Institutes of Health Research, *Best Practices for Protecting Privacy in Health Research* (Ottawa: Public Works and Government Services Canada, 2005), Element 6: Recruiting Potential Research Participants at p. 63, online: <[http://www.cihr-irsc.gc.ca/e/documents/et\\_pbp\\_nov05\\_sept2005\\_e.pdf](http://www.cihr-irsc.gc.ca/e/documents/et_pbp_nov05_sept2005_e.pdf)>.

<sup>59</sup> *Dyment*, *supra* note 46 at 429, citing *Privacy and Computers*, *supra* note 47.



purposes or disclosed to third parties without his consent. As EHR data in particular clearly relate to matters that are fundamentally and inherently personal and go to the core of what it means to enjoy individual dignity and independence, the individual must be provided with sufficient freedom to exercise these rights autonomously.

Where participation involves some physical intervention, as in clinical research, the law clearly requires specification of all risks, no matter how rare or remote, especially when the materialization of those risks may have grave consequences. In light of the evolving privacy and confidentiality principles set out above, informed consent for research involving use of personal information, even with no clinical intervention *per se*, would still appear to require an elevated duty of disclosure in order to be meaningful. That might include information about the following:

1. the researchers, their affiliation, their contact details, and the source of funds or sponsorship;
2. what the specific purpose of the research is, what personal information is needed for that purpose and why;
3. what exact EHR data elements will be collected, what use will be made of said data, and what further uses may be made of the data in future (*e.g.* any potential follow-up or spin-off studies);
4. whether the researcher has a plan to link the data with other datasets, and if so, which ones, under what conditions, and for what purpose;
5. which third parties may potentially gain access to personal data (*e.g.* sponsors, regulators, university administrators, research ethics boards, law enforcement);
6. how long the research data will be retained, and whether it will be anonymized or destroyed afterwards and if so, when and how;
7. how the data will be safeguarded against risk of privacy or security breach, and what will happen in the event of breach;
8. how the research results will be reported, and where and in what form;
9. how one can exercise one's right to withdraw consent and what the exact implications of such withdrawal are;
10. contact information to obtain more information about the study at any time; and
11. anything else the individual asks about.

Legally, this policy choice would not require many—if any—amendment to existing legislative schemes. While data protection regimes in some jurisdictions expressly require consent to be *informed*, others do not state this requirement explicitly. Nonetheless, for reasons explained in our survey of the current state of the law above, it is our view that, even in these other jurisdictions, consent would be afforded the same significance ascribed at common law and interpreted in accordance with *Charter* values, and thus, would have to be meaningfully informed.

Though this policy option would provide individuals with the greatest effective control over their personal information and likely engender the greatest public trust, particularly in the context of clinical trials, there is some evidence to suggest that the adverse impact on epidemiological or population-based research could be significant.<sup>60</sup> This is because of the reduced amount of data that would be available for research due to the elevated cost and

---

<sup>60</sup> See Khaled El Emam *et al.*, “Pan-Canadian”, *supra* note 29 at 59-70.

practical difficulty of recruiting participants and obtaining individual consent, particularly for large-scale studies. This model could further impede research by introducing potential bias into results, due to general attitudinal or other characteristic differences between individuals who tend to agree to the use of their EHR data for research and those who tend to refuse or not respond. Moreover, some could say that by limiting the integration of data that was envisaged as part of the pan-Canadian info-structure, the informed consent model defies the significant advantages that EHRs could potentially offer to enhance research capacity and improve the quality of health and health services in Canada.

While in our view “informed” consent is most consistent with established and fundamental legal principles, we recognize that there are other plausible policy choices which we, as a society, can make in respect of consent requirements for access to EHR data for different types of health research. This is particularly so if we recognize that privacy is not absolute and if we value—as we clearly do—the important public benefits health research can contribute to our health and the future sustainability and continued improvement in the quality of our health care services. Hence, we may certainly choose to deviate from specific, informed consent as the “gold standard,”<sup>61</sup> but in doing so, we must remain ever mindful of the fundamental values which we have come to recognize at common law and under our *Charter*; we must remember the level of sensitivity of EHR data and the reasonable expectation people have that it will be kept private and confidential; we must deviate from specific, informed consent *only* to the extent necessary to allow for those public health purposes which we clearly and universally cherish as a society; and, we must proceed in a manner that is honest and transparent, and accords with the principles of a free and democratic society. We now turn to discuss alternatives to specific informed consent.

#### B. Seeking Broad Consent For Future, Yet Unspecified Research Studies

In a first possible deviation from the existing legal standard, policy-makers could recognize the practical limitations of specific, informed consent for non-clinical research and move towards the concept of broad consent, a more practical, yet lesser form of informed consent.<sup>62</sup> This policy choice would—at least conceptually—liken the data contained in pan-Canadian interoperable EHR systems to large-scale national data registries or research platforms. Instead of obtaining informed consent for each specific research study, broad or general consent would be sought from each individual to permit their EHR data to be uploaded from the info-structure into interoperable health information data warehouses to support future, yet unspecified research uses. These research data warehouses would be governed by specially designated data custodians through appropriate rules, structures, and processes. As research uses become defined over time, the data custodians would govern the release of the EHR data contained in the data warehouse to health researchers for specific research projects under

---

<sup>61</sup> We have chosen to benchmark specific, informed consent as our gold standard. In our view, informed consent is most closely aligned with the spirit of individual autonomy, a foundational principle in our free and democratic society. Others, however, have not been so generous. As Chassigneux, Trudel & Knoppers argue:

Though a significant part of the legal community remains attached to the supremacy of consent, it appears poorly adapted to protect rights in the univers [*sic*] of networks. As practiced, consent seems more and more like a decoy since it seems to ensure individuals' control over their own data. The considerable number of exceptions as well as the way data circulate make consent naive at best, and at worst, an inadvisable instrument if we really do want to protect the privacy of participants.

Cynthia Chassigneux, Pierre Trudel & Bartha Maria Knoppers, “The Legal Framing of Computerized Processing of Health Data: A European and Canadian Perspective” (2006) 4:1 GenEdit 1 at 3, online: HumGen International <<http://www.humgen.umontreal.ca/int/GE/en/2006-1.pdf>>.

<sup>62</sup> Roy & Fournier ask: “With the probable quantitative expansion of secondary uses [of EHRs], for multiple and diverse purposes, is the model of informed, express and project-specific consent doomed to evolve towards a model of ‘broad consent’ where consent is less, rather than more, informed?” Roy & Fournier, *supra* note 11 at 25.

specified conditions, subject to proper research ethics review and oversight, and in accordance with special research agreements.

The broad consent could be obtained from individuals preferably at the same time as EHRs are being created and implemented. This way, at least, individuals could know and understand up front all of the terms, conditions, and potential research uses of their EHR data, *albeit* in a broad, general way. Although researchers would not be able to disclose as much detail to support truly informed consent, they would need to provide enough information to describe the general purpose of the research platform and the terms and conditions for subsequent use:

1. which EHR data elements will be uploaded into the research data warehouse;
2. what entity is responsible for managing the data warehouse, subject to what governance rules, structures and processes, and how the entity can be contacted;
3. what general types of research studies the EHR data will help support and whether or not this might include commercial research;
4. under what conditions will researchers be able to gain access to the EHR data within the terms of the broad consent being given, and to what degree the data will be de-identified before release (including details about the de-identification process);
5. under what conditions the individual will be re-contacted to obtain specific informed consent before data is released to researchers;
6. what safeguards does the data custodian have in place to protect the data against risk of privacy or security breach, and what happens in the event of breach;
7. who else will or may potentially gain access to it (*e.g.* third party auditors, regulators, law enforcement, *etc.*);
8. whether the data in the warehouse will be linked with other datasets, and if so, which;
9. how long the data will be retained and whether certain data elements will eventually be completely anonymized and/or destroyed, and if so, how;
10. how the individual can exercise his or her right to withdraw consent and what the implications of such a withdrawal are;
11. who should be contacted, and where and how to obtain more information at any time; and
12. anything else the individual asks about.

Broad consent obtained up front would allow several transactions to occur without having to re-contact individuals. First, broad consent would permit the roll-up of certain EHR data elements from the health service provider at the local point of service, through what has been conceived of architecturally as “the health information access layer,” into an interoperable research data warehouse. Such a warehouse would be governed by specially designated custodians that would essentially act as gatekeepers to the data. Second, a broad consent policy could permit these specially designated custodians to screen EHR data contained in the warehouse against specific entry criteria upon researchers’ request to select potential participants for a particular project. Third, broad consent would allow the research data custodian to manipulate the EHR data of screened-in participants in order to effectively de-identify them (by a process of anonymization, pseudonymization, aggregation, coding, or double-coding) and release them to researchers for specific research projects under certain conditions and subject to special agreements.

Although broad consent would allow significantly more flexibility than the specific, informed consent model, it should not extend to allow indefinite uses of EHR data. In certain special situations, individuals would need to be re-contacted to obtain their informed consent for participation in specific research studies. This may be the case, for example, if the researchers were requesting access to data that identified individuals, if the research method required the ongoing, active involvement of the individual, or if the research study involved highly sensitive data or a high level of risk above a certain threshold.

In these cases, a process for exceptionally allowing disclosure of identifiable information from the data custodian to the researchers for the purpose of re-contacting individuals to obtain specific consent would need to be established, properly managed, and duly recorded. Moreover, the specific risk conditions and threshold levels would need to be clearly defined, at which point the requirement for re-contact and re-consent would be triggered. Possibly, in the interest of greater openness and transparency, policy-makers might consider the creation of a public research registry to publicize, on an annual basis, specific research studies that are using EHR data contained in the data warehouse, with an appropriate level of detail as they become defined, and a description of the research results to facilitate knowledge transfer and benefit-sharing for all.

The broad consent model would appear to provide greater flexibility than the specific, informed consent model, as well as being more practically feasible. Yet, as we have seen with the creation of national bio-banks or large national research platforms around the world, the adoption of even the broad consent model takes a significant amount of time, resources, public consultation, public trust, and public support.

Interestingly, a recent study on the use of personal information for research purposes found that, while a majority of respondents were supportive of research and willing to consider alternatives to conventional study-by-study consent, they still wished to maintain some level of control over the use of their information:

The Canadian public is supportive of health research and open to alternatives to a conventional project-by-project consent. However, they do not wish to completely relinquish control over use of their personal health information. Given the heterogeneity of consent choices, any long-run solution must take this into account to maintain public confidence in the confidentiality of the information they share with their physicians. Although the EMR may play a role here, the outstanding challenge is how best to elicit and keep up to date the individuals' consent preferences. There are no easy solutions.<sup>63</sup>

From a legal perspective, some argue that broad consent is too far removed from the true concept of individual autonomy to be valid. Without details about each specific research project, individuals are not in a position to really turn their minds to the situation at hand and make a truly informed, autonomous choice. General, uninformed consent may simply not be a viable or cognizable type of consent under the current law.

Such an approach [broad consent] would undoubtedly make it easier to do longitudinal health research with large cohorts of participants. It would allow researchers to resolve consent issues with a single consent at the time individuals are recruited into the [research platform]. There is, however, little or no *legal* support for the use of blanket consents in Canada. Such consents are, by definition, far too general to have much legal weight.<sup>64</sup>

Others may argue that true autonomous choice includes the right to waive one's right to more specific information and make decisions whenever and on whatever basis one chooses.

---

<sup>63</sup> Donald J. Willison *et al.*, *supra* note 29 at 711-712.

<sup>64</sup> See Caulfield & Ries, *supra* note 52 at 30 [footnote omitted]. The authors cite Vilhjálmur Árnason, who posits: "There is no such thing as 'general informed consent.' The more general the consent is, the less informed it becomes. It is misleading to use the notion of informed consent for participation in research that is unforeseen and has not been specified in a research protocol." See "Coding and Consent: Moral Challenges of the Database Project in Iceland" (2004) 18:1 *Bioethics* 27 at 42.

This includes the right to waive more specific information so as not to be hassled by researchers' calls and/or the right to selflessly exercise altruism for the public good in the fullest and truest sense, without condition or paternalistic restraint. Still, most commentators recognize that even though broad consent may be a departure from the gold standard of specific, informed consent and the principles of autonomy in the truest sense, this shift is critically necessary to alleviate the costs, burdens, and impediments of reaffirming consent for each individual, for each specific research project. Only by accepting to move away from specific, informed consent, could valuable health research—particular large-scale, longitudinal, population-based research—be allowed to proceed in the public interest.<sup>65</sup>

This latter view is gaining increasing traction internationally, particularly in the evolving area of bio-banks, which provides us with a good analogy for considering interoperable EHR systems that could, once integrated, likewise serve as a significant national research platform.

For example, UNESCO offers the following commentary on research using human genetic databases:

The consent requirements in the research context are more rigorous. A difficult question in this area is that of whether fresh consent has to be obtained if new research of a different nature is to be conducted on samples originally given for another form of research. A system which required fresh consent would be extremely cumbersome and could seriously inhibit research and it is for this reason that a system of "blanket consent" covering all forms of future medical research might be preferable, provided that the consent given in the first instance explicitly recognizes this.<sup>66</sup>

The HUGO Statement on Human Genomic Databases, recognizing the public good of research, recommended that "[i]nformed consent may include notification of uses (actual or future), or opting out, or, in some cases, blanket consent."<sup>67</sup>

In 1997, a World Health Organization (WHO) report recommended that "blanket informed consent that would allow use of a sample for genetic research in general, including future as yet unspecified projects, appears to be the most efficient and economical approach, avoiding costly re-contact before each new research project."<sup>68</sup> However, the WHO, in a 2003 report titled *Genetic Databases: Assessing the Benefits and Impact on Human and Patient Rights* recommended the following protections and limitations to the concept of broad consent:

In some cases it might be desirable to seek broad, open-ended consent to future research, the purposes, limits or consequences of which are currently unknown. In such cases, blanket future consent is only permissible where anonymity can be guaranteed, and there is no risk that unexpected results will filter back to the subjects concerned. If this guarantee is not possible, or if linking of data is necessary for the research, then specific consent to the specific research must be obtained. The use of sunset clauses, whereby consent will only be valid during a finite period of time, might be considered as a means to ensure adequate protection of individual interests.<sup>69</sup>

---

<sup>65</sup> For an in-depth discussion of the different views, perspectives, and rationales underlying the selection of broad consent as a policy choice, see Timothy Caulfield, "Biobanks and Blanket Consent: The Proper Place of the Public Good and Public Perception Rationales" (2007) 18:2 *The King's College Law Journal* 9 [Caulfield, "Biobanks"].

<sup>66</sup> Sylvia Rumball & Alexander McCall Smith, *Human Genetic Data: Preliminary Study by the IBC on its Collection, Processing, Storage and Use* (Paris: UNESCO, 2002) at 16, online: UNESCO <[http://portal.unesco.org/shs/en/files/2138/10563744931Rapfinal\\_gendata\\_en.pdf/Rapfinal\\_gendata\\_en.pdf](http://portal.unesco.org/shs/en/files/2138/10563744931Rapfinal_gendata_en.pdf/Rapfinal_gendata_en.pdf)>.

<sup>67</sup> Human Genome Organization (HUGO), *HUGO Ethics Committee: Statement on Human Genomic Databases* (London: HUGO, December 2002), online: Human Genome Organization <[http://www.hugo-international.org/img/genomic\\_2002.pdf](http://www.hugo-international.org/img/genomic_2002.pdf)>.

<sup>68</sup> World Health Organization, *Proposed International Guidelines on Ethical Issues in Medical Genetics and Genetic Services*, Report of a WHO Meeting on Ethical Issues in Medical Genetics, Doc. No. WHO/HGN/GL/ETH/98.1 (Geneva: World Health Organization, 1997) at 13, online: World Health Organization <<http://www.who.int/genomics/publications/en/ethicalguidelines1998.pdf>>.

<sup>69</sup> Fons Dekkers *et al.*, *Genetic Databases: Assessing the Benefits and Impact on Human and Patient Rights*, Report of the Working Group of the World Health Organization's European Partnership on Patients' Rights and Citizens' Empowerment (Geneva: World Health Organization, 2003) at 14, online: World Health Organization <<http://www.law.ed.ac.uk/ahrb/publications/online/whofinalreport.pdf>>.

Many might contend that this broad consent model would allow greater integration of data between health care and health research so as to maximize the broader public benefits that were originally envisaged of the expansive purposes of the pan-Canadian health info-structure. Researchers could gain access to more comprehensive data, with greater ease and reduced potential for biased results in order to ultimately improve the quality of health care services. Individuals, too, could participate more fully in the research enterprise knowing that they are doing good for others, and future generations, without the need to provide specific consent in every case. Were this policy option adopted for observational health research, relevant laws would need to be amended accordingly. Arguably, to reflect this policy in law, the requirement for *informed* consent would perhaps have to be re-framed more accurately as prior authorization for future, yet unspecified research uses of personal data.<sup>70</sup> In the context of biobanks, Professor Bartha Knoppers has sounded the clarion call for the adoption of broad consent, with the appropriate protections, as the preferred policy option to enable longitudinal research studies in the public interest:

[T]he increasing complexity of choices and issues, and the legalistic nature of informed "choice" and the consent "process" could undermine the very act of communication and consensualism so necessary to ethically sound research. Moreover, in the future, can truly public resources and infrastructures such as population biobanks, be built to gird a universal health care system—one that promotes open access where the applicable norms are extrapolated only from personal data or health information legislation? The latter presumes that personal privacy is inimical to participating as a citizen in the public interest. In revisiting consent, researchers should ... consider ... the challenges they pose to mindsets forged by the polarization of setting up consent and confidentiality barriers for individuals that impede their participation as citizens in society for the benefit of others, including future "others" without an explicit consent in every case.<sup>71</sup>

Others, however, are more reticent to embrace such a policy shift too quickly, lest we be swayed by persuasive rationales for which we have much sympathy, while omitting to reflect carefully on the core legal and ethical principles at stake. Professor Caulfield cautions as follows:

These are, no doubt, challenging issues, and reasonable people can disagree over how they might best be resolved. However, we should be careful not to succumb to arguments that are not grounded in (or, at least, not reconciled with) foundational principles. It is easy to call for the protection of a principle when the threat to it is blatantly nefarious; it is less so when the incursion is supposedly being made for the greater good. But it is in this latter situation that a careful understanding and scrutiny of the principle – here, respect for autonomy – seems most crucial. This is particularly the case when the principle at stake flows from universally accepted, fundamental human rights. The ad hoc modification of standard consent principles in favour of a blanket consent model undertaken in the name of near-future scientific goals, no matter how worthwhile, seems a dangerous path.<sup>72</sup>

We should not mistake such policy debates simplistically as pitting the ideal of personal autonomy underlying an individual's right to control the collection, use, and disclosure of her personal health information against utilitarian arguments about society's interests in health research and the collective right to share in its benefits. In the current context, such a clean dichotomy between the individual and the collective would not be possible. On the one hand, the protection of privacy is as much a collective interest as it is an individual one. The concept of public interest in the protection of privacy is finding increasing support in third generation privacy laws.<sup>73</sup> On the other hand, the individual's opportunity to participate in research may serve as an expression of her individual right to participate meaningfully in society as a contributing citizen, as has been suggested above. Moreover, with such rapid advances in science, health research is increasingly of immediate and direct benefit to individuals, and not merely to future generations.

---

<sup>70</sup> Timothy Caulfield, Ross E.G. Upshur & Abdallah Daar, "DNA Databanks and Consent: A Suggested Policy Option Involving an Authorization Model" (2003) 4 BMC Medical Ethics E1.

<sup>71</sup> Bartha Maria Knoppers, "Consent Revisited: Points to Consider" (2005) 13:2&3 Health Law Review 33 at 36.

<sup>72</sup> Caulfield, "Biobanks", *supra* note 65 at 24.

<sup>73</sup> See e.g. PHIPA, *supra* note 58, s. 44(3)(c); HIA, *supra* note 58, s. 50(1)(b)(i).

### C. Using De-Identification as a Means of Carving Out Research Activities Altogether

To the extent that it is possible to completely de-identify personal information in EHRs, de-identification of personal information required for health research purposes may provide a partial solution. Where personal information is genuinely rendered de-identified, that information will fall outside the scope of existing privacy regimes altogether.

Early proponents of EHRs who foresaw their usefulness for health research purposes viewed de-identification as a means of making EHRs readily available to researchers. Roy Romanow, for one, suggested that researchers could have ready access to data “extracted generically for health research purposes, without being linked to any individual electronic health record.”<sup>74</sup>

Canada Health Infoway appears to favour this approach. It has developed a conceptual architecture that articulates an overview of the necessary component parts of a pan-Canadian electronic health info-structure, one of which is an anonymization service.<sup>75</sup> The anonymization service it contemplates as a necessary component of Canada’s health info-structure would enable both the use of pseudonyms and the removal of all personal identifiers from an EHR to enable use of the data for secondary analysis and research purposes.<sup>76</sup>

A recent EKOS Research Associates Inc. survey commissioned by Canada Health Infoway, Health Canada, and the Office of the Privacy Commissioner of Canada indicates that a strong majority of Canadians are also comfortable with the use of de-identified EHRs for secondary health research purposes. This survey revealed that 84 per cent of Canadians support the use of EHRs for secondary health research purposes, provided that personally identifying information is not disclosed to researchers.<sup>77</sup> This is consistent with earlier findings resulting from studies conducted on this similar question.<sup>78</sup>

De-identification of data for research use is strongly encouraged as a crucial and practical form of protection.<sup>79</sup> However, to render EHR data truly de-identifiable for research purposes is, from a technological and organizational standpoint, an elusive, relative, and ever-shifting objective.

First, the specifications required of EHR systems must be clear and consistent to preserve their interoperability and their potential value for health research purposes. Whether the goal will be to de-identify data or to render the data truly de-identifiable has very different implications for privacy protection. For example, will the data be coded or double-coded? Will the code be reversible or irreversible, on a temporary or permanent basis? Will the data remain linkable or un-linkable and will individuals’ identities be ultimately traceable or untraceable? All of these specific choices will have significant impact on privacy protection. The

---

<sup>74</sup> *Romanow Report*, *supra* note 6 at 79.

<sup>75</sup> Canada Health Infoway, *An Overview of the Electronic Health Record Privacy and Security Conceptual Architecture* (2006) at 7, online: Canada Health Infoway <<http://knowledge.infoway-inforoute.ca/EHRSRA/doc/EHR-Privacy-Security-Overview.pdf>>.

<sup>76</sup> *Ibid.*

<sup>77</sup> EKOS Research Associates Inc., *Canadians and the Privacy Landscape* (Ottawa: EKOS Research Associates Inc., 2007) at 6, online: Office of the Privacy Commissioner of Canada <[http://www.privcom.gc.ca/information/survey/2007/ekos\\_2007\\_02\\_e.asp](http://www.privcom.gc.ca/information/survey/2007/ekos_2007_02_e.asp)>.

<sup>78</sup> Kalpana Nair *et al.*, “Patients’ consent preferences regarding the use of their health information for research purposes: a qualitative study” (2004) 9:1 *Journal of Health Services Research & Policy* 22; Nandini Saxena *et al.*, *Understanding Canadians’ Attitudes and Expectations: Citizens’ Dialogue on Privacy and the Use of Personal Information for Health Research in Canada* (Ottawa: Canadian Policy Research Networks, 2006), online: Canadian Policy Research Networks <<http://www.cprn.com/doc.cfm?doc=1428&l=en>>; Donald J. Willison *et al.*, “Patients’ consent preferences for research uses of information in electronic medical records: interview and survey data” (2003) 326 *B.M.J.* 373.

<sup>79</sup> William W. Lowrance & Francis S. Collins, “Ethics: Identifiability in Genomic Research” (2007) 317 *Science* 600.

nomenclature around de-identification in the literature is inherently confusing,<sup>80</sup> and several attempts have been made to clarify these concepts for Canadian researchers through research ethics guidelines and best practices.<sup>81</sup> Despite the current confusion, definitions themselves are not an insurmountable problem if what they refer to substantively is commonly understood by all those who use and apply them. System requirements and specifications must be made very clear and explicit from the outset, lest this policy option become an obtuse way of providing misleading assurances to Canadians who believe they are meaningfully contributing to research in the false confidence that there is little or no technical risk to their privacy.

Second, de-identification is a relative concept in that data may be completely de-identifiable in the hands of one person or entity, and yet remain readily re-identifiable in the hands of another person or institution holding the key to re-linkage. Resorting to de-identification as a solution requires a sophisticated governance structure to determine which entity or entities will carry out the de-identification, who will be the key-holder, and who will retain the potential to re-identify EHR data and/or link it to other personal data at the request of researchers. While systems could be configured to disclose only de-identifiable data—however defined—to individual researchers for specific research projects, many researchers might eventually need to re-identify individuals in order to fulfill the verification requirements of regulators, sponsors, or publishers; link the data with other datasets in order to examine the influence of other health, socio-economic, and environmental determinants; track changes in data over time in longitudinal-type research; and/or possibly contact individuals down the road to seek consent to collect physical measures and/or carry out a subsequent qualitative arm of the research, such as a quality of life survey, for example. Who will bear responsibility for de-identifying the data, and then retaining the ability to re-identify it as needed? Will this responsibility remain with health information custodians on the front line? Will it be transferred to specially designated research data custodians charged with maintaining interoperable research data warehouses? Or will it be entrusted to a recognized, independent third party trustee? Who will be the key-holder? These are critical decisions that will have major implications for accountability, capacity, and resources.

Third, the difficulty inherent in ensuring a sufficient degree of de-identification is exacerbated by the fact that an adequate standard of de-identifiability will inevitably be a moving target. That is, as more and more personal information is collected about individuals and disseminated in various public sources and fora, there is an increasing likelihood that the information could be aggregated, cross-referenced, and linked in order to re-identify previously de-identified records.<sup>82</sup> The fiasco surrounding the release of de-identified search query records by AOL aptly demonstrates why this is so.<sup>83</sup> Even where obvious or common personal

---

<sup>80</sup> Bartha Maria Knoppers & Madelaine Saginur, "The Babel of Genetic Data Terminology" (2005) 23 *Nature Biotechnology* 925.

<sup>81</sup> See e.g. Canadian Institutes of Health Research, *CIHR Best Practices for Protecting Privacy in Health Research* (Ottawa: Public Works and Government Services Canada, 2005) at 33, online: Canadian Institutes of Health Research <[http://www.cihr-irsc.gc.ca/e/documents/et\\_pbp\\_nov05\\_sept2005\\_e.pdf](http://www.cihr-irsc.gc.ca/e/documents/et_pbp_nov05_sept2005_e.pdf)> [*CIHR Best Practices*]; see also Canadian Institutes of Health Research, Natural Sciences and Engineering Research Council of Canada & Social Sciences and Humanities Research Council of Canada, *Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans* 1998 (with 2000, 2002, 2005 amendments) (Ottawa: 2005), art. 3.2, online: Interagency Advisory Panel on Research Ethics <[http://pre.ethics.gc.ca/english/pdf/TCPS%20October%202005\\_E.pdf](http://pre.ethics.gc.ca/english/pdf/TCPS%20October%202005_E.pdf)>.

<sup>82</sup> See Khaled El Emam *et al.*, "Evaluating Common De-Identification Heuristics for Personal Health Information" (2006) 8 *Journal of Medical Internet Research*, online: *Journal of Medical Internet Research* <<http://www.jmir.org/2006/4/e28>>.

<sup>83</sup> "Just how personally revealing such data can be became evident last year, when AOL released records of the searches conducted by 657,000 Americans for the benefit of researchers. While AOL did not identify the people behind the searches, reporters from The New York Times were able to track down some of them quickly through their search requests": Miguel Helft, "Google Adds a Safeguard on Privacy for Searchers" *The New York Times* (15 March 2007) C4, online: *New York Times Online* <<http://www.nytimes.com/2007/03/15/technology/15googles.html>>.



identifiers are stripped from the data, information may in some cases be linked back to the individual in question, particularly where sub-optimal de-identification techniques were used.<sup>84</sup> Hence, from a technological perspective, the effectiveness of de-identification features must be measured by the residual risk for data to be re-linked at the individual level through external re-identification attacks, and not merely by the extent to which direct and/or quasi-personal identifiers have been removed.<sup>85</sup> The complexity and variability of existing standards, which already recognize a spectrum of acceptable degrees of de-identification, will only be augmented by the fact that the potential for re-identification continues to increase as more and more personal information is made publicly available. This does not lead necessarily to the conclusion that de-identification can never be effective, but rather that de-identification techniques and practices must be continually upgraded to keep pace with the rising potential for re-identifiability.

Under existing statutory privacy regimes in Canada, personal information must be de-identified, with no serious possibility of re-identification, before it would fall completely outside the scope of legislated privacy protections, including the requirement to obtain consent for its use. This is necessarily implied from the fact that most, if not all, data protection regimes apply to *identifiable* data. Legislative definitions that would place health information outside of legal regimes are, however, inconsistent or non-existent and thus extremely difficult to apply in practice.

For example, section 3(2) of Saskatchewan's *Health Information Protection Act* defines "de-identified health information" as "personal health information from which any information that may *reasonably be expected* to identify an individual has been removed".<sup>86</sup> Compare this to Alberta's *Health Information Act*, in which the term "non-identifying," in reference to health information, "means that the identity of the individual who is the subject of the information *cannot be readily ascertained* from the information".<sup>87</sup> Under Ontario's *Personal Health Information Protection Act*, "identifying information means information that identifies an individual or for which it is *reasonably foreseeable* in the circumstances that it could be utilized, either alone or with other information, to identify an individual."<sup>88</sup> Section 1(3) of the New Brunswick *Protection of Personal Information Act* stipulates that personal information will be considered identifiable for the purposes of that *Act* if it includes a name, makes an individual's identity obvious, or does not itself include the name of an individual or make his or her identity obvious but is likely in the circumstances to be combined with other information that does. New Brunswick exempts de-identified data from its data protection regime without articulating any test for what constitutes de-identification.<sup>89</sup>

A 1997 European data protection directive provides that an "individual shall not be regarded as identifiable if identification requires an unreasonable amount of time and manpower".<sup>90</sup> More recently, the Article 29 Data Protection Working Party has expressed the

---

<sup>84</sup> Latanya Sweeney, "k-Anonymity: A Model for Protecting Privacy" (2002) 10 *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems* 557; Salvador Ochoa *et al.*, *Reidentification of Individuals in Chicago's Homicide Database: A Technical and Legal Study* (2001) [unpublished, archived online: Massachusetts Institute of Technology <<http://web.mit.edu/msalib/www/writings/classes/6.805/reid.pdf>>].

<sup>85</sup> See El Emam *et al.*, "Pan-Canadian", *supra* note 29 to determine the risks, in the Canadian context, of re-identification of anonymized data based on publicly available information.

<sup>86</sup> *Health Information Protection Act*, S.S. 1999, c. H-0.021, s. 3(2) [*HIPA*] [emphasis added].

<sup>87</sup> *HIA*, *supra* note 58, s. 1(1)(r) [emphasis added].

<sup>88</sup> *PHIPA*, *supra* note 58, s. 4(2) [emphasis added].

<sup>89</sup> See *Protection of Personal Information Act*, S.N.B. 1998, c. P-19.1, s. 1(2), which states: "information that relates to an identifiable individual but is collected, used or disclosed in a form in which the individual is not identifiable is not personal information when so collected, used or disclosed."

<sup>90</sup> Council of Europe, Committee of Ministers, Recommendation No. R (97) 5 (1997), online: Council of Europe—Human Rights and Legal Affairs <[http://www.coe.int/t/e/legal\\_affairs/legal\\_co-operation/data\\_protection/documents/international\\_legal\\_instruments/Rec\(97\)5\\_EN.pdf](http://www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/documents/international_legal_instruments/Rec(97)5_EN.pdf)>.

view that a mere hypothetical possibility of singling out an identifiable individual from a larger data set is not enough to consider that person “identifiable” for the purpose of data protection regimes. One must consider “all the means likely reasonably to be used” and if, taking into account “all the means likely reasonably to be used”, the possibility for re-identification “does not exist or is negligible, the person should not be considered as “identifiable,” and the information would not be considered as “personal data” subject to data protection regimes.<sup>91</sup>

The United States has rejected, in large measure, a speculative approach to assessing the likelihood of re-identification in favour of an explicit de-identification protocol. Under the *Health Insurance Portability and Accountability Act*,<sup>92</sup> data may be considered de-identified when it does not contain any of eighteen specified data elements and there is no knowledge that the remaining information could, on its own or in combination with other information, be used to identify the subject of the information. However, *HIPAA* also permits data to be considered de-identified if an individual with knowledge and expertise in de-identification has certified that there is a “very small risk” of re-identification.

Canadian courts are just beginning to struggle with the question of when data may legally be said to be adequately de-identified so as not to constitute personal information caught by access to information and data protection regimes. The Federal Court of Appeal has found that data will constitute personal information “if it is ‘about’ an individual and if it permits or leads to the possible identification of the individual.”<sup>93</sup> More recently, the Federal Court has further specified that “[i]nformation will be about an identifiable individual where there is a serious possibility that an individual could be identified through the use of that information, alone or in combination with other available information.”<sup>94</sup>

Given that the legal test turns on possibilities that are difficult to ascertain in practice, it is not clear that removal of personal identifiers alone will constitute an adequate substitute for consent. In order for de-identification to provide workable and effective protection, clear standards and protocols may be required in order to meet or surpass the applicable threshold of risk.

Quite apart from the legal complexity inherent in ascertaining what constitutes de-identifiable data for the purposes of interpreting a given statute, it is not clear that individuals’ legal and moral interests in their personal information dissipate simply because it is de-identified and falls outside the scope of data protection regimes. Though it may be premature to base public policy decisions on this controversial line of argument, at least one author has tentatively argued that an individual may have a continuing privacy interest in his or her personal health information under Canadian common law, even if it has been de-identified.<sup>95</sup> This continuing interest, to the extent it exists, would no doubt be enhanced if one or more parties retained the capacity to re-identify personal information somewhere along the chain of transactions involving the data.

In *Re Source Informatics Ltd.*,<sup>96</sup> the English Court of Appeal determined that an action for breach of confidence was not available to restrict the non-consensual sale of de-identified prescription data from pharmacists to Source Informatics Ltd., since there was no significant

---

<sup>91</sup> Article 29 Data Protection Working Party, *Opinion 4/2007 on the concept of personal data* (20 June 2007) at 15, online: European Commission—Justice and Home Affairs <[http://ec.europa.eu/justice\\_home/fsj/privacy/docs/wpdocs/2007/wp136\\_en.pdf](http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf)>.

<sup>92</sup> *Health Insurance Portability and Accountability Act of 1996*, Pub. L. No. 104-191, 110 Stat. 1936 [HIPAA].

<sup>93</sup> *Information Commissioner v. Canada (Transportation Accident Investigation and Safety Board)*, 2006 FCA 157 ¶ 43, [2007] 1 F.C.R. 203.

<sup>94</sup> *Gordon v. Canada (Health)*, 2008 FC 258 at para 34.

<sup>95</sup> See Elaine Gibson, “Is There a Privacy Interest in Anonymized Personal Health Information?” (2003) Health L.J. 97 for an interesting discussion of this issue.

<sup>96</sup> [1999], E.W.J. No. 6880 (C.A.) (QL).

risk of re-identifying individual patients from the prescription data in question. The Court of Appeal looked to equity and held that an individual does not maintain a privacy interest in personal information that has been anonymized. The Court acknowledged that pharmacists owe patients a duty of confidentiality in respect of their personal health data, but reasoned that “pharmacists’ consciences ought not reasonably to be troubled”<sup>97</sup> by the disclosure of their patients’ data once de-identified. In Canada, however, liberty, autonomy, and *prima facie* control over personal information have been recognized as the fundamental underpinnings of privacy rights. The constitutional nature of these rights suggests that if interests implicating section 7 of the *Charter* are engaged, a different result could obtain in Canada. An assessment of the machinations of the data custodian’s conscience, therefore, is not necessarily an appropriate proxy for the principles of fundamental justice.<sup>98</sup>

It seems clear then that de-identification, while often heralded as the answer to the consent dilemma, cannot provide a universal solution for many forms of valuable health research. While de-identification may, in some cases, provide an effective means of managing privacy risks, it cannot be relied upon as the only viable policy option. It will likely be necessary to refocus the debate away from technological solutions like de-identification toward first legal and ethical principles in order to find complementary forms of protection.

#### D. Relying on Implied Consent by Re-Conceptualizing Research as a Necessary Adjunct to the Primary Purpose of Health Care

In existing legal regimes, transfers of electronic health information for health care purposes depend largely on implied or deemed consent. Once consent for the initial collection, use, and disclosure of personal health information for primary health purposes has been sought and obtained, health care providers within what is colloquially known as an individual’s “circle of care”<sup>99</sup> are typically able to use and disclose that individual’s personal information as necessary for treatment and other primary health purposes. Even within the circle of care, however, personal information remains subject to the specific access rights depending on the health care provider’s role, as well as to possible exceptions in those jurisdictions in which masking, lock-box, or other opt-out mechanisms exist.

Consent issues usually arise more acutely where transfers of personal information outside a circle of care are contemplated. Within a circle of care, consent is deemed or implied. Outside a circle of care, there is no deemed or implied consent for secondary uses of personal information unrelated to the purposes for which consent was originally provided, typically health care.

Traditionally, health care was understood as having as its sole purpose the provision of *direct* benefits to the individual patient. By contrast, health research was understood as having as its purpose *future* benefits that would accrue, not to the individual, but to society as a whole. The use of personal information for health research has therefore been conceptualized as a secondary use.

First principles of research ethics, which developed at the time of the *Nuremberg Code* of 1949<sup>100</sup> and the *Declaration of Helsinki* of 1964,<sup>101</sup> have contributed to codifying this conceptual distinction. These seminal ethical codes developed as a means of protecting the individual against the encroachment of utilitarian interests seeking to advance collective

---

<sup>97</sup> *Ibid.* at 35.

<sup>98</sup> *Supra* note 95.

<sup>99</sup> The “circle of care” is a core concept defined as the individuals and activities directly related to the health care and treatment of an individual.

<sup>100</sup> *Trials of War Criminals before the Nuremberg Military Tribunals under Control Council Law No. 10*, vol. 2 (Washington D.C.: U.S. Government Printing Office, 1949) at 181-182.

<sup>101</sup> *Declaration of Helsinki*, *supra* note 41.

interests in health research at the expense of fundamental rights to autonomy, bodily integrity, and human dignity.

More recent developments in the Canadian context have come to challenge the notion that the purposes motivating health care and publicly funded health research are so diametrically opposed.

For several decades now, we have seen a sustained commitment to maintaining Canada's system of universal, publicly funded health care. Though an increased role for the private sector within our publicly funded health care system has been contemplated and permitted in recent years,<sup>102</sup> the fundamental commitment to ensuring a baseline level of access to publicly funded health care for all has not been questioned. Access to health care data, prescription data, billing information, and other personal data has been indispensable for the purpose of administering a publicly funded health care system. Health system managers and health services researchers must be able to rely on these data in order to plan the appropriate allocation of public resources and work to improve the quality of, and access to, health care services. Canadians benefit directly from enabling publicly-funded research which operates to ensure the economic viability of their health care system for the universal benefit of all. Over time, this uniquely Canadian reality has necessarily blurred the philosophical divide between publicly funded health care and publicly funded health research.

The gap between the role of health care provider and health researcher has also begun to close on both ends. Health care providers are increasingly being encouraged to make treatment decisions based on all available and accessible research evidence, which we see being incorporated into relevant professional standards of care.<sup>103</sup> Health researchers, for their part, are being encouraged through funding requirements and knowledge transfer incentives to translate their research results into effective practice through improved policies and/or clinical care for the direct benefit of Canadians.<sup>104</sup>

Moreover, progress in the fields of information technology, genomics, and nanotechnology has resulted in such rapid advances in health care that the traditional assumption that health research will not likely result in any direct benefit for research participants or their families within their lifetimes may be outdated. Indeed, it is increasingly likely that individuals will see benefits from their participation in research accrue to themselves and their genetically related next of kin.

---

<sup>102</sup> *Chaoulli v. Quebec (A.G.)*, 2005 SCC 35, [2005] 1 S.C.R. 791.

<sup>103</sup> “[I]nformation, evidence and ideas have the potential to unlock the cures to many of today’s illnesses, identify the genetic source of chronic illnesses, give health care providers access to the latest and best information on new treatments or drugs, improve the quality and safety of care within the health care system, and most importantly, empower patients to manage and maintain their own health .... With a complete system of electronic health records in place ... [h]ealth care providers would have access to clinical decision support tools to assist them in making decisions based on the best available evidence. Health care providers would be able to access patient records at the point of a clinical encounter. It would help manage the massive amounts of complex health information and ensure that health care providers have complete and accurate information about patients’ health and health care histories. It also would improve physicians’ ability to access the latest information, select the best course of action, and use evidence to guide their decisions.” *Romanow Report*, *supra* note 6 at 75 and 78-9.

<sup>104</sup> The *Canadian Institutes of Health Research Act*, S.C. 2000, c. 6, which created the Canadian Institutes of Health Research (CIHR), Canada’s leading federal health research agency, clearly states at s. 4: “The objective of the CIHR is to excel, according to internationally accepted standards of scientific excellence, in the creation of new knowledge and its translation into improved health for Canadians, more effective health services and products and a strengthened Canadian health care system ...” [emphasis added]. For example, in one of its many initiatives aimed at meeting this objective, CIHR is investing significant resources to ensure that knowledge gained from its clinical research efforts is translated into health innovations that are applied in practice and for which Canadians themselves will be the immediate beneficiaries of improved health. See also Canadian Institutes of Health Research, *A Partnership for Clinical Research*, online: Canadian Institutes of Health Research <<http://www.cihr-irsc.gc.ca/e/22113.html>>.

In light of this evolving reality, Dr. Khaled El Emam, Canada Research Chair in Electronic Health Information at the University of Ottawa, contends that “research and clinical applications are merging and researchers are increasingly turning to EHRs as a source of clinically relevant data.”<sup>105</sup> Canada Health Infoway has also implicitly espoused similar reasoning. While it recognizes that patient-centric access to EHRs by caregivers and other types of end-users is the primary goal of the EHR Info-Structure, Infoway has noted that a lot can be said for the health care value derived from being able to use this information for research, analysis, and health prevention initiatives.<sup>106</sup>

Elsewhere, the UK Clinical Research Collaboration argued before the British House of Commons Health Committee that “[f]acilitating access by the research and public health communities to electronic patient records has substantial benefits for patients and the health service. Since research shares a mission of improving patient care and patient safety it is integral to patient benefit. Access to patient data for this purpose should be considered a primary and not a secondary use.”<sup>107</sup> In the U.S., Henry Lowe, Chief Information Officer at Stanford University School of Medicine, has argued that, “[i]f we want to improve outcomes and develop an evidence-based model of healthcare, we have to eliminate the dichotomy between patient care and research. EMR systems”, he said, “provide a tremendous opportunity to bridge that gap.”<sup>108</sup>

What then would be the implications of formally re-conceptualizing publicly funded health research as a necessary adjunct to health care as the primary use of EHRs? Could health researchers realistically be brought together with providers into that trusted circle of care within which we have come to accept an implied consent model for data sharing?

This policy option depends on re-conceptualizing not only health research, but health researchers too, as a class of professionals that requires comprehensive, coherent, and effective regulation, with proper training and certification, ethical codes of conduct, accountability mechanisms, and appropriate disciplinary sanctions. As a profession, health researchers are currently not regulated as closely or rigorously as health care providers. If health researchers are allowed to enter the circle of trusted health professionals, they too would require an appropriate level of scrutiny over their work.

A complex system of user-based privileges for health researchers, running parallel to those currently being developed for health care providers, would be required. These user-based privileges would be required to tailor degrees of access commensurate with area of specialization, research method, and role-based variables, among other factors. A shift from the current disclosure-based regime to an access-based model for research purposes would no doubt also be required. That is, this policy option would necessitate a move away from existing privacy protection models which seek to limit the uses and disclosures of personal data vis-à-vis outside third parties, including health researchers, towards the adoption of new “security perimeter models”<sup>109</sup> which would allow health researchers to come within the permissible zone of role-based access rights.

---

<sup>105</sup> El Emam *et al.*, “Pan-Canadian”, *supra* note 29 at 3.

<sup>106</sup> Canada Health Infoway Inc., *EHRs Blueprint, version 2*, *supra* note 20 at 5.

<sup>107</sup> U.K., H.C. Select Committee on Health, “Evidence submitted by the UK Clinical Research Collaboration (EPR 52)” (25 April 2007), online: House of Commons - Health - Written Evidence <<http://www.publications.parliament.uk/pa/cm200607/cmselect/cmhealth/422/422we47.htm>>, cited in Roy & Fournier, *supra* note 11 at 7.

<sup>108</sup> FasterCures, *Think Research: Using Electronic Medical Records to Bridge Patient Care and Research* (Washington D.C.: FasterCures, 2005) at 12, online: FasterCures <[http://www.fastercures.org/pdf/emr\\_whitepaper.pdf](http://www.fastercures.org/pdf/emr_whitepaper.pdf)>.

<sup>109</sup> For an in-depth discussion of the security perimeter of EHRs and the policy implications of making such technological choices, see E. Brown *et al.*, *Technology Choices and Privacy Policy in Health Care* (2007), online: Memorial University of Newfoundland <<http://cpig.cs.mun.ca/TechnologyChoices.pdf>>.

This policy option would add to the organizational complexity of a pan-Canadian interoperable EHR system and the management challenges already associated with its adoption by health care providers. Re-conceptualizing health research as a necessary adjunct to the primary purpose of the collection, use, and disclosure of personal health information also has the potential to affect the current dynamic between patients and their physicians. Privacy guidelines with a clear basis in health ethics promulgated by the Canadian Medical Association recognize that a patient's "ability to decide with whom he or she will share information is crucial for the protection of the right of privacy and for the preservation of trust in the therapeutic context."<sup>110</sup> If the proposed re-conceptualization of health research as an integral part of the health care circle is not closely aligned with the views of Canadians, distrust and unintended schisms between health care providers and their patients could result, threatening the traditional underpinnings of that confidential relationship:

Fidelity of health care professionals, of health care institutions, and of the health care system itself to patients will be brought into question if patients believe they have been deceived by multiple secondary uses of their PHI [personal health information], particularly if these uses occur without their knowledge. Patients, whatever their degree of vulnerability may be, may rightfully expect that effective measures exist to protect their privacy, and the confidentiality of their health information, particularly when that information is circulating in identifiable form.<sup>111</sup>

The Canadian Medical Association has expressed the view that "[m]any laws, practices and initiatives may not withstand the kind of scrutiny deemed necessary and reasonable for the protection of privacy and the trust and integrity of the therapeutic relationship."<sup>112</sup> Re-conceptualizing health research as an integral part of the primary purpose of the collection, use, and disclosure of personal health information may be one such initiative that would no doubt be met with some notable resistance.

Nevertheless, evidence of a willingness to collapse health research and health care purposes is extant in some Canadian legal regimes. For example, Manitoba's *The Personal Health Information Act* permits an information trustee to disclose, without an individual's consent, personal health information to specified public bodies for "research and planning that *relates to* the provision of health care or payment for health care by the trustee".<sup>113</sup> The requirement that research and planning "relate to" the provision of health care or payment for health care is sufficiently broad in scope that it can authorize the disclosure of personal health information for research purposes unlikely to result in direct care or treatment benefits to individuals affected. Indeed, such a provision would appear to catch a wide range of secondary research purposes including quality control, audit and financial planning that, while related to the provision of health care, may not directly improve quality of care.

Similarly, in Ontario's *Personal Health Information Protection Act*, a health information custodian may disclose personal information to a prescribed person or entity "who compiles or maintains a registry of personal health information for purposes of facilitating or improving the provision of health care"<sup>114</sup> or "for the purpose of analysis or compiling statistical information with respect to the management of, evaluation or monitoring of, the allocation of resources to or planning for all or part of the health system, including the delivery of services".<sup>115</sup> Such prescribed persons or entities must have in place practices and procedures to protect the privacy of the individuals whose personal health information they receive and to maintain the

---

<sup>110</sup> Canadian Medical Association, *CMA Health Information Privacy Code* (Ottawa: Canadian Medical Association, 1998), Principle 5, online: Canadian Medical Association <[http://www.cma.ca/index.cfm/ci\\_id/3216/la\\_id/1.htm](http://www.cma.ca/index.cfm/ci_id/3216/la_id/1.htm)>.

<sup>111</sup> Roy & Fournier, *supra* note 11 at 5.

<sup>112</sup> *Supra* note 110.

<sup>113</sup> S.M. 1997, c. 51, C.C.S.M. c. P33.5, s. 22(2)(g)(ii).

<sup>114</sup> *PHIPA*, *supra* note 58, s. 39(1)(c).

<sup>115</sup> *Ibid.*, s. 45(1).

confidentiality of the information. Moreover, those practices and procedures must be approved by the Privacy Commissioner. Interestingly, once prescribed and approved, these entities are permitted under the terms of the *Act* and its accompanying regulations to use personal health information for research purposes as *though they were a health information custodian* under the *Act*, effectively assimilating them to other health care providers within the “inner circle,” and therefore subjecting them to the same rules regarding research use.<sup>116</sup>

What these existing legislative regimes appear to effectively do is allow prescribed entities to be regarded as equivalent to health providers for the purpose of permitting access to data, subject to the same rules and conditions. However, they do not go as far as assimilating health research to health care purposes within the permissible circle of care uses based on implied consent.

Though controversial, this policy option for addressing the consent requirements for research access to EHR data may gradually gain traction as a viable alternative to specific, informed consent. The reasons surveyed above that would seem to support a re-conceptualization of health research and health researchers within the “inner circle,” however, are clearly limited to publicly funded research carried out for the common good. In the current context, the common good, as we conjecture, is increasingly likely to result in good for the individual as well, in his or her lifetime, or that of the immediate next of kin. An attempt to argue that commercial research should also be included within that same circle is nowhere nearly as clear or likely to be persuasive. Hence, the viability of any policy option that would recognize health research as a primary purpose would depend on a sophisticated ability to distinguish between non-commercial, academic, publicly sponsored health research which benefits all, from commercially sponsored research that is primarily profit-driven. It is questionable whether such a distinction could ever be realistically delineated today, given the high degree of public-private research integration:

Furthermore, the activities of health researchers themselves will be difficult to categorize as either commercial or noncommercial in nature. Increasingly, academia, private sector, voluntary charitable organizations and government are joining forces to engage in innovative research partnerships and to transform this new knowledge into forms which are beneficial to the population. In an era where such partnerships are actively encouraged, a whole spectrum of public-private arrangements have begun to emerge. More and more often, university researchers receive salary support and/or funding from various sponsors. In some cases, the support is provided to conduct research that may directly or indirectly enhance the competitiveness of Canadian businesses; in other cases, it is provided to support peer-reviewed, academic research to advance general knowledge about the health and/or health system of Canadians; more commonly, support is intended to sustain both these objectives.<sup>117</sup>

#### E. Resorting to Existing Statutory Consent Exemptions for Research

The departure from informed consent and the foundational principle of individual autonomy is significantly marked in the case of consent exemptions. In this policy option, the design and development of EHRs would continue to focus strictly on health care purposes, with no up front discussion of potential research uses of the data. Later, when EHR systems are eventually made available for use in support of research purposes, resort would be had to existing legislative exemptions that exceptionally allow disclosure of personal information for research purposes without consent.

---

<sup>116</sup> O. Reg. 329/04, ss. 13(4) and 18(3).

<sup>117</sup> Canadian Institutes of Health Research & Canadian Institute of Health Information, *Personal Information Protection and Electronic Documents Act: Questions and Answers for Health Researchers* (Ottawa: Public Works and Government Services Canada, 2001), online: Canadian Institutes of Health Research <[http://www.cihr-irsc.gc.ca/e/pdf\\_14391.htm](http://www.cihr-irsc.gc.ca/e/pdf_14391.htm)>.

Most data protection statutes contain research exceptions for the collection, use, or disclosure of personal information without the consent of the individuals that the information pertains to, subject to several, any, or all of the following conditions:

- the research plan must outline the nature, objectives, and anticipated benefit of the research, as well as the qualifications and affiliations of the researchers;
- the objectives of the research cannot otherwise be reasonably accomplished without the data being requested, at some necessary level of identifiability;
- obtaining the consent of each individual must be shown to be impracticable;
- the research must meet some public interest test or pass some harm/benefit analysis;
- there must be review and approval by a research ethics board, and in some cases, notification and/or approval by a data protection authority;
- the research must be conducted with adequate safeguards in place to protect the privacy and confidentiality of the data, with additional safeguards and protections in the case of data matching or data linkage;
- there must be in place procedures to remove all identifying information at the earliest opportunity consistent with the purposes of the research;
- the researcher must use the personal information only for the purposes set out in the research plan, and not use or disclose the data for any other purpose, unless required by law;
- the researcher must not contact or attempt to contact the individuals, unless the data custodian obtains prior consent from the individuals for such contact to occur;
- the researcher must not publish the research results in a way that may identify individuals;
- the researcher must notify the custodian immediately in the event of a privacy or security breach; and,
- the researchers must enter into a research agreement with the data custodian, wherein the researcher expressly agrees to a number of the above conditions, as well as other conditions imposed by the data custodian, including requirements for security, return, retention, or disposal of the data, and requirements to submit to on-site audits to ensure compliance with the agreement.<sup>118</sup>

While many, if not all, data protection statutes in Canada exceptionally allow non-consensual research use of personal information subject to a number of conditions listed above, these conditions are by no means the same—let alone similar—across different jurisdictions. In fact, there are significant differences, both in their formulation and combination, which may impede the interoperability of systems and inter-jurisdictional research.

In view of this variability, reliance on legislated exemptions after the fact to allow disclosure of personal information to researchers without consent may prove to be difficult to reconcile from one jurisdiction to another. This was similarly the case for consent rules in respect of the collection, use, and disclosure of personal information for health care purposes—particularly in electronic form—until policy-makers undertook concerted efforts to reduce the gap by harmonizing and consolidating legislative solutions. The Federal/Provincial/Territorial

---

<sup>118</sup> For an overview of relevant statutory conditions for allowing access to personal information for research purposes without consent, see Kosseim, Kardash & Penta, *supra* note 31 at 60-128.



(FPT) Conference of Deputy Ministers of Health mandated its Advisory Committee on Information and Emerging Technologies to develop a *Pan-Canadian Health Information Privacy and Confidentiality Framework*.<sup>119</sup> The objective of the *Framework* was:

... to respond to Canadians' privacy and confidentiality expectations and to suggest a harmonized set of core provisions for the collection, use and disclosure of personal health information in both the publicly and privately funded sectors. Consistent, or at least more consistent, privacy regimes among jurisdictions would facilitate health care renewal, including the development of electronic health record systems and primary health care reform.

The *Framework*, endorsed by a majority of members of the FPT Conference of Deputy Ministers of Health in January 2005,<sup>120</sup> recommended, as part of its core provisions, harmonized rules for *both* health care treatment and health research. However, jurisdictions, during and since the development of the *Framework*, appear to have focused primarily—if not exclusively—on developing and/or revamping legal rules around an implied knowledgeable consent model for the collection, use, and disclosure of personal health information within the circle of care.<sup>121</sup> These efforts have been motivated by a common objective to facilitate the rapid development and deployment of EHRs for treatment purposes,<sup>122</sup> but unless sustained legislative efforts are similarly undertaken now to harmonize the disparity of existing conditions for research purposes, this “wait and see” policy option may not turn out to be the panacea it is hoped to be. Several examples of critical disparity illustrate the point.

For one, the harm-benefit analysis and public interest test are fundamentally different, both legally and philosophically, in different statutes. In several jurisdictions, the analysis of whether the consent exception applies to the proposed research turns on weighing the potential harm to an individual's privacy with the anticipated public benefit of the research. That is, the analysis in some jurisdictions requires consideration of the individual's private interest in protecting his or her privacy versus the public interest in conducting the research.<sup>123</sup> Other jurisdictions have devised different tests. For example, Ontario's health information protection regime requires consideration of two competing public interests, “the public interest in conducting the research and the public interest in protecting the privacy of the individuals whose personal health information is being disclosed”.<sup>124</sup> Similarly, Alberta law requires that “the proposed research is of sufficient importance that the public interest in the proposed research outweighs to a substantial degree the public interest in protecting the privacy of the individuals who are the subjects of the health information to be used in the research”.<sup>125</sup>

Another significant difference in the conditions required for non-consensual research use of personal information across jurisdictions is the level of oversight required. Some jurisdictions expressly provide for the role of the research ethics board,<sup>126</sup> while others also require notification and/or review and approval of the relevant data protection authority in

---

<sup>119</sup> Health Canada, *Pan-Canadian Health Information Privacy and Confidentiality Framework* (Ottawa: 2005), online: Health Canada <[http://www.hc-sc.gc.ca/hcs-sss/pubs/ehealth-esante/2005-pancanad-priv/index\\_e.html](http://www.hc-sc.gc.ca/hcs-sss/pubs/ehealth-esante/2005-pancanad-priv/index_e.html)>.

<sup>120</sup> Quebec and Saskatchewan did not endorse the *Framework*.

<sup>121</sup> For example, Ontario developed and adopted its health information law in 2004 consistent with the emerging consensus at the time around an implied consent model within the circle of care, whereas Saskatchewan and Alberta had to amend their respective health information laws to better harmonize themselves in accordance with this consolidated legal rule.

<sup>122</sup> Nola M. Ries, “Patient Privacy in a Wired (and Wireless) World: Approaches to Consent in the Context of Electronic Health Records” (2006) 43 Alta. L. Rev. 681.

<sup>123</sup> See e.g. *Freedom of Information and Protection of Privacy Act*, R.S.B.C. 1996, c. 165, s. 35(b); *HIPA*, *supra* note 86, s. 29(2)(c); *Personal Health Information Act*, C.C.S.M., c. P-33.5, s. 24(3)(a) [*PHIA*].

<sup>124</sup> *PHIPA*, *supra* note 121, s. 44(3)(c).

<sup>125</sup> *HIA*, *supra* note 58, s. 50(1)(b)(i).

<sup>126</sup> See e.g. *PHIA*, *supra* note 123, s. 24(2)(b); *HIA*, *supra* note 58, ss. 49 and 64(2); *HIPA*, *supra* note 86, s. 29(1)(b); *PHIPA*, *supra* note 58, s. 44, and accompanying regulations, O. Reg 329/04, s. 15.

that jurisdiction.<sup>127</sup> Still others envisage some degree of oversight by the health data custodian who releases the data to the researcher without consent under conditions which must be specified in a research data agreement to varying degrees of specificity.<sup>128</sup>

Yet a further example of the significant differences between laws is the requirement that consent be impracticable to obtain. In some jurisdictions, the requirement is stated differently in terms of being impracticable, impractical, or impossible.<sup>129</sup> For present purposes, this condition is critical. An attempt to concretely flesh out what is meant by “impracticable” has been made in best practice guidelines for health researchers. It demonstrates a range of factors that lie somewhere between sheer impossibility and mere inconvenience.<sup>130</sup>

The term “impracticable” has been interpreted in a recent decision of the Ontario Superior Court of Justice. Having considered various dictionary meanings of the term “impracticable,” as distinguished from the terms “impractical” and “impossible,” Molloy J. concluded as follows:

In my view, the word “impracticable” ... should be given its plain and ordinary meaning. Based on the standard dictionary definitions of the word, I conclude that the word “impracticable” is not synonymous with “impossible”, although it may be closely related. Neither is it synonymous with the word “impractical”. Rather, “impracticable” should be interpreted as meaning “practically impossible” or “not feasible”. In my opinion, this imports a measure of reasonableness and proportionality ...<sup>131</sup>

If consent exemptions for research are going to be resorted to as the preferred policy choice, it will be somewhat disingenuous to wait until 2015—after an incremental roll-out of these massive, interoperable EHR systems covering the entire Canadian population for purposes of care and treatment, and after billions of dollars will have been invested—to argue then that it is impracticable to go back to each individual to obtain consent for research.

Moreover, it is conceivable—but not a certainty—that in 2015 it will be impracticable to re-contact every individual in Canada to obtain his or her consent for the use of their EHR data for research. To proceed now to develop EHR systems prospectively, while knowingly deferring the research issues and ignoring the present consent opportunities, is neither valid nor justifiable as a public policy option. Surely, the spirit and intent of the existing consent exemptions was not to avoid the legal obligation to obtain consent for anticipated research uses by postponing its execution until such time as it has *become* impracticable.

EHR systems are presently being designed and developed prospectively to take into account patients’ consent preferences for the use of their EHR data for health care purposes, including the creation of consent registries and the implementation of masking features, lock-boxes, and the like. In addition to the obvious direct and immediate benefits accruing to health care, the use of EHRs to facilitate health research and support evidence-based health care has been envisaged as an integral component and key justification for the creation of a pan-Canadian interoperable health info-structure since 1999. Yet, as complex consent directives for health care purposes are presently being introduced by system developers, it is not clear why the consent directives would not also, at the same time, inquire into patients’ consent preferences for the use of their EHR data for research purposes that are eminently foreseeable, if not inevitable.

---

<sup>127</sup> See e.g. *Personal Health Information Protection and Electronic Documents Act*, S.C. 2000, c. 5, s. 7(3)(f); *HIA*, *supra* note 58, s. 50(4); *PHIPA*, *supra* note 58, s. 47(4); *An Act respecting Access to documents held by public bodies and the Protection of personal information*, R.S.Q., c. A-2.1, s. 125.

<sup>128</sup> See e.g. *HIA*, *supra* note 58, s. 54; *Freedom of Information and Protection of Privacy Act*, R.S.A. 2000, c. F-25, s. 42(d) and accompanying regulations, Alta. Reg. 200/95 s. 8; s. 35; *PHIPA*, *supra* note 58, s. 44(5); *Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c. F.31, s. 21(1)(e), and accompanying regulations, R.R.O. 1990, Reg. 460, s. 10.

<sup>129</sup> For a review of different formulations across relevant statutory provisions see Kosseim, Kardash & Penta, *supra* note 31, c. 4.

<sup>130</sup> See *CIHR Best Practices*, *supra* note 81 at 40.

<sup>131</sup> *Kinglip Holdings Inc. v. Novak Graphics Inc.*, [2000] 100 A.C.W.S. (3d) 148 at para. 9.

Nor is it necessarily clear that the existing research exemptions would constitute a sufficiently clear source of authority to disclose identifiable EHRs in circumstances where consent could have been sought prospectively, but was not. Notwithstanding the social utility associated with valuable health research, it may be difficult to legally sustain a claim that it would be “impracticable” to obtain consent in these circumstances, especially if *Charter* values are invoked to help interpret and resolve any ambiguity in the term.

The Supreme Court of Canada has confirmed that in the absence of specific legal authorization that would, itself, be subject to *Charter* scrutiny, physicians ought not to collect personal medical information from individuals seeking treatment and disclose that information to third parties for unrelated purposes.<sup>132</sup> While it arose in the context of a *Charter* challenge in the course of a criminal prosecution under section 8, this finding echoed the Court’s earlier indication that “the patient has the right to require that the secret shall not be divulged; and that right is absolute, unless there is some paramount reason which overrides it.”<sup>133</sup> The view that personal information to which a reasonable expectation of privacy attaches should not be disclosed without consent has found further support in evolving jurisprudence under section 7, which has expanded the application of this principle beyond the criminal context and, indeed, elevated it to the level of a principle of fundamental justice.<sup>134</sup>

From a public interest perspective, the benefits of resorting to consent exemptions for research are obvious. Epidemiological or population-based researchers could gain access to even more comprehensive, valuable sources of data, unimpeded by potential bias concerns. The knowledge gained by such research efforts could be translated and directly re-invested into improved health care services for Canadians.

Notwithstanding these clear public benefits, the negative impact on privacy protection and public trust in the health care system could be significant. Users’ confidence in their health care providers could be eroded if and when it came to their attention that their EHR data will be or has been released for research purposes without their knowledge and consent in a manner that completely undermines their autonomous control over the use and disclosure of sensitive personal information. The impact on public trust is not to be underestimated, according to some studies. Canadians’ concern about how widely their personal health information is shared or how it is used may reduce the quantity and accuracy of the data they give their health care provider, which, in turn, can result in treatment errors, patient safety issues, under-reporting of disease prevalence, and underestimation of compliance statistics.<sup>135</sup>

#### F. Retroactively Deeming Consent by Legislative Amendment

Rather than require researchers, ethics review boards, and health custodians to undertake a case-by-case analysis of whether it is impracticable (or impractical or impossible) to obtain consent, legislators could choose, as a matter of general public policy, to retroactively deem consent to have existed or remove the legislative requirement for consent altogether. Effectively, this would open up access to certain designated data elements of EHR records for health research purposes after the fact. In such a model, legislators would be replacing consent obtained from each user of the health system on an individual basis, with a public, retroactive, and omnibus “consent” obtained from the Canadian population through a legislative process. Such deemed consent would fill in where no consent ever existed, or might even go so far as to override express objections that the individual may have expressed at the time.

---

<sup>132</sup> *Dyment, supra* note 46.

<sup>133</sup> *Halls v. Mitchell, supra* note 43 at 136.

<sup>134</sup> *Cheskes v. Ontario (Attorney General)*, [2007] 87 O.R. (3d) 581, O.J. No. 3515 (Ont. Sup. Ct.) [*Cheskes*].

<sup>135</sup> El Emam *et al.*, “Pan-Canadian”, *supra* note 29 at 5-6.

While a retroactive legislative solution of this type may seem far-fetched, it is not entirely without precedent. In a recent decision of the Ontario Superior Court of Justice, *Cheskes v. Ontario (Attorney General)*,<sup>136</sup> Mr. Justice Belobaba considered amendments to the *Vital Statistics Act*.<sup>137</sup> The impugned provisions would have had the retroactive effect of allowing the Ontario government to disclose birth and adoption records without the consent of the birth parents or adult adoptees involved, contrary to the promise of confidentiality that had been originally made in respect of those records when they were sealed.

Belobaba J. found (with “no difficulty”) that these amendments violated the applicants’ right to liberty pursuant to section 7 of the *Charter*. Belobaba J. held that the non-consensual disclosure of private records violated a privacy interest that extended beyond the actual documents themselves and inhered in the very dignity and self-worth of the individuals:

In this case, to track the language of the Supreme Court ... , the disclosure of the birth and adoption records under the new law, in circumstances where a reasonable expectation of privacy has been created ... constitutes an invasion of the dignity and self-worth of each of the individual applicants, and their right to privacy as an essential aspect of their right to liberty in a free and democratic society has been violated.<sup>138</sup>

Belobaba J. further found that the decision made by the applicants to keep the birth and adoption records confidential and not have their identity revealed came within what the Supreme Court of Canada has referred to as an “irreducible sphere of personal autonomy wherein individuals may make inherently private choices free from state interference.”<sup>139</sup> By its very nature, this implicated a basic choice “going to the core of what it means to enjoy individual dignity and independence”.<sup>140</sup>

Having found that the applicants’ right to liberty within the meaning of section 7 of the *Charter* was engaged, Belobaba J. went on to decide that the infringement of the applicants’ right to liberty was in violation of a principle of fundamental justice. In so doing, the right to control disclosure of one’s confidential personal information was elevated to the level of a principle of fundamental justice, which was crystallized in the following terms: “Where an individual has a reasonable expectation of privacy in personal and confidential information that information may not be disclosed to third parties without his or her consent.”<sup>141</sup>

Of particular interest for present purposes was Belobaba J.’s consideration of the two safeguards that had been built into the legislation. One was the no-contact provision. Where an individual affected by the *Act* filed a “no contact notice,” the retroactive amendments would have only permitted disclosure of the birth and adoption records if the individual or entity requesting the records undertook in writing *not* to contact the biological kin who filed the “no contact notice.” The other safeguard, the non-disclosure procedure, would have allowed individuals to apply to the Child and Family Services Review Board for a non-disclosure order. However, a mere objection to disclosure on the part of birth parents or adult adoptees would not suffice. According to the legislative scheme, the Board could only grant such an order in exceptional circumstances if it were satisfied that “the order is appropriate to prevent sexual harm or significant physical or emotional harm to [the adopted person or birth parent].”<sup>142</sup> The Court held that these so-called safeguards were insufficient to temper the privacy breach and save the impugned provisions.

---

<sup>136</sup> *Cheskes*, *supra* note 134.

<sup>137</sup> R.S.O. 1990, c. V.4.

<sup>138</sup> *Cheskes*, *supra* note 134 at para. 83.

<sup>139</sup> *Malmo-Levine*, *supra* note 55 at para. 85, quoting *Godbout*, *supra* note 55 at para. 66.

<sup>140</sup> *Ibid.*

<sup>141</sup> *Ibid.* at para. 127.

<sup>142</sup> *Cheskes*, *supra* note 134 at para. 23.

Transposed to the health research context, this case seems to suggest that any legislative amendment that would retroactively open up confidential EHR records for research purposes could remain vulnerable under a section 7 *Charter* analysis, even if the researcher undertook in writing not to contact individual patients, and even if a special procedure were built in (equivalent to a lock-box or other mechanism) to permit individuals to object to disclosure if the threshold for such a procedure were set too high.

We have seen another relevant example of the retroactive, legislative approach when Parliament amended the *Statistics Act* in 2005 to retroactively remove a legislative guarantee of confidentiality that had applied to census records collected after 1918.<sup>143</sup> This legislative promise of confidentiality served to codify prior assurances of confidentiality set out in historical census manuals of instructions.<sup>144</sup> The 2005 amendments now permit census records collected between 1911 and 2001 to be released in their entirety to the public via Library and Archives Canada after ninety-two years. Interestingly, the *Statistics Act* was also amended to provide that census records collected prospectively after 2001 would not be released to the public after ninety-two years unless the individual to whom the information related consented to such a release.

Proponents of the 2005 amendments to the *Statistics Act* argued that the public benefits of genealogical research outweighed the privacy interests individuals maintained in census records collected ninety-two years earlier. They argued that critical information about the history of Canada and individual families' ancestors would be lost if census records were not made available to the public. The research community expressed the view that information collected through the census is not particularly sensitive and that any personal information that could be construed as sensitive was considerably less so ninety-two years after its collection. Historical guarantees of confidentiality were read narrowly. It was argued that these assurances of confidentiality did not and were not intended to provide a perpetual guarantee of confidentiality. It was felt that evidence of the intent to preserve census records for the use of future generations, namely the fact census records were stored at National Library and Archives Canada, rebutted such an interpretation.

Detractors of the 2005 amendments disagreed. Citing the highly sensitive and intrusive nature of many census questions, those who opposed the 2005 amendments to the *Statistics Act* felt that the needs and interests of historical and genealogical researchers ought not be permitted to trump assurances of confidentiality that were made, particularly after these informal assurances were codified in statute in 1918. In their view, privacy rights did not end with death. Also troubling to those who opposed the 2005 amendments to the *Statistics Act* was the fact that Canadians had a legal obligation to participate in the census. The amendments eliminated the assurance of confidentiality that census respondents had received in return for their coerced participation. Stakeholders were particularly concerned that retroactively eliminating a legislative promise of confidentiality to previous generations of Canadians would undermine Canadians' willingness to be honest and forthright in the future.

---

<sup>143</sup> R.S.C. 1985, c. S-19, s. 18.1, as am. by *An Act to amend the Statistics Act*, S.C. 2005, c. 31.

<sup>144</sup> In 1871, census takers were advised that "[p]ersons having apprehensions, or showing hesitation in giving their answers, must be assured that no information they may give, and that nothing taken down in the schedules, can possibly injure, or in any way affect their standing or their business." In 1918, sub-section 15(1) of the *Statistics Act*, S.C. 1918, c. 43 provided: "No individual return, and no part of an individual return made, and no answer to any question put, for the purposes of the Act, except as hereinafter set forth, shall without the previous consent in writing of the person or of the owner for the time being of the undertaking in relation to which the return or answer was made or given, be published, nor, except for the purposes of a prosecution under this Act, shall any person not engaged in connection with the census be permitted to see any such individual return or any part of any individual return." See Statistics Canada, *Final Report of the Expert Panel on Access to Historical Census Records*, online: Statistics Canada <<http://www.statcan.ca/english/census96/finalrep.htm>>.

The 2005 amendments to the *Statistics Act* have not been constitutionally challenged to date. Whether a *Charter* challenge would succeed as in the *Cheskes* case is debatable given several distinguishing features that might play into the analysis. For example, it could be argued that information contained in census records is relatively less personal and sensitive than that contained in birth and adoption records. The passage of time before the census records could be opened up (ninety-two years) lends support to this view as does the fact that the real impact of disclosure on people's lives may be relatively less serious and profound. Finally, the *Statistics Act* amendments are more limited in scope in that they apply only to existing census records, and continue to require informed consent for eventual release of any prospectively collected census information after 2001.

Arguably, however, the reasoning employed in *Cheskes* could find more direct and relevant application to a legislative amendment that would purport to retroactively open up EHRs for health research purposes without consent. It is possible that such an amendment could run afoul of section 7 of the *Charter*.

First, Canadians confide sensitive personal health information to health providers in the confines of a therapeutic relationship that gives rise to a legitimate and strong expectation of confidentiality. This expectation of trust and confidence is widely affirmed in existing legal and ethical frameworks governing relationships between health care providers and patients. Personal health information is imparted to health providers for inclusion in EHRs on the clear understanding that it will not be disclosed to third parties without consent, particularly since research purposes are not being integrated or even discussed in the current design and architecture processes.

Second, EHRs reflect not only a passive, static picture about an individual's *de facto* health status as he or she may have inherited or developed it, but more fundamentally, may contain highly personal information about the most intimate and fundamental decisions individuals may actively choose to make as a result of their health condition. These decisions, including decisions about reproductive and family planning, lifestyle choices, drug prescriptions, genetic tests, psychological therapies, elective surgeries, medical use of marijuana, and enrollment in controversial clinical trials, may reflect one's personal philosophy and moral values about private affairs which extend far beyond one's physiological state.

Third, because EHRs may potentially contain personal information about individuals from "cradle to grave," they provide an evolving and continually relevant window into people's lives. Opening up these records may have a serious and profound impact on individuals at any point in their lifetimes. Because these records are continuously updated with each encounter between an individual and the health system, the passage of time and evolution of one's personal circumstances will not necessarily nullify or dampen the enormous implications that disclosure may have or the psychological stress individuals may feel as a result.

In view of the significance the judiciary has attached to the right to control disclosures of one's personal information, a retroactive, legislative amendment mandating non-consensual disclosure for research could interfere with the liberty interest protected under s. 7 of the *Charter*. If the principle of fundamental justice, as articulated by Belobaba J. in the *Cheskes* case stands,<sup>145</sup> it is difficult to see how any such interference could be construed as either in accordance with the principles of fundamental justice or demonstrably justified in a free and

---

<sup>145</sup> *Cheskes*, *supra* note 134 at para. 107: "In my view, the principle being suggested by the applicants can be stated more directly as follows: *where a reasonable expectation of privacy has been established in the collection and storage of one's personal and confidential information, one should have the ability to control the dissemination of this information.* Or, to put it even more plainly:

Where an individual has a reasonable expectation of privacy in personal and confidential information, that information may not be disclosed to third parties without his or her consent ... "

democratic society. Much would turn on the express rationale, means, limitations, and protections that would accompany such an amendment.

From a public interest perspective, the advantages of retroactively mandating disclosure of EHR data for research purposes are obvious. Researchers will no doubt point out that retroactivity is necessary and desirable to enable many types of valuable health research that require access to EHR data. For example, the integrity of longitudinal population health studies depends on seamless and consistent sources of data over time. This type of research would be severely compromised, if not precluded, if the data are subject to large temporal holes occasioned by a failure to obtain appropriate consent when the data were first collected, and by the sheer practical difficulty of re-contacting individuals to obtain consent for the secondary use of their data.

However, for the same reasons as discussed in the fifth policy option above, the public interest in privacy, trust, and confidence in the health care system could be seriously compromised by such a solution. Retroactive, legislative amendments that allow disclosure of personal information for research purposes despite promises of confidentiality would suffer from the same type of flaws affecting the application of existing consent exemptions discussed in the fifth policy option above.

On the one hand, it is arguable that the negative impact on privacy, public trust, and confidence could be considered worse in the case of a retroactive legislative amendment than in the application of existing consent exemptions. This is particularly so if the retroactive legislative amendment were allowed to override the clear objection expressed by individuals, and if such an amendment were only introduced after a deliberate and avoidable omission to seek people's consent upon the prospective creation of EHRs in a manner which respects their personal autonomy.

On the other hand, retroactive legislative amendment allowing access to EHRs for research purposes, if subject to a truly comprehensive, consultative, and democratic decision-making process, would necessitate a more inclusive and transparent public policy debate. Rather than distort the application of existing research exemptions subject to little or spotty and opaque oversight, a conscious legislative amendment would publicly highlight the relevant issues and cause them to be openly acknowledged and specifically confronted. The need for such open debate is particularly strong in a public policy dilemma such as this, where policy makers and legislators would be seeking to strike an appropriate balance between the public interest in protecting the individual right to control how personal information is used, and the public interest in facilitating health research to improve the quality of Canadian's health and their health care system.

#### CONCLUSION

More than fifteen years ago, the Supreme Court recognized the burgeoning size and complexity of the health care field:

The twentieth century has seen a vast expansion of the health care services. Rather than relying on one individual, a physician, the patient now looks directly and indirectly to dozens and sometimes hundreds of individuals to provide him with the services he requires. He is cared for not simply by his own physician but by a veritable army of nurses, numerous consulting physicians, technologists and technicians, other allied health personnel and administrative personnel.<sup>146</sup>

The increasing complexity of health care in the world of paper records foreshadowed the exponential changes that EHRs would bring to the confidential doctor-patient relationship:

---

<sup>146</sup> *McInerney v. MacDonald*, *supra* note 44 at 146, citing L.E. Rozovsky & F.A. Rozovsky, *The Canadian Law of Patient Records* (Toronto: Butterworths, 1984) at 73-74.

Recent trends in health care exacerbate the problems relating to privacy in the medical context, particularly in light of the health-team approach in an institutional setting and modern health information systems. If the health-team approach gives a patient easy access to a wide range of medical services, it inevitably results in the fragmentation of the classical doctor-patient relationship among a team of medical and para-medical personnel.<sup>147</sup>

A move toward electronic records to modernize, maximize, and integrate information-sharing in this increasingly complex health care context seems both inevitable and overdue. This evolution is not *per se* concerning. It is the subtle consequences of the manner in which EHRs have been developed and deployed in Canada that have been our focus.

EHRs in Canada represent much more than the simple transformation of paper records into electronic form. In addition to their role in the modernization of information systems in the health care system, EHRs seem—as a result of the manner in which they have been deployed and the vast potential they hold—to be fundamentally redefining an individual's right to control the use and dissemination of his or her personal information in the health context.

Specifically, the deployment of EHRs in Canada for health care purposes, in advance of addressing issues of secondary uses such as research, may effectively preclude the maintenance of well-established standards of consent. Current legislative regimes require express and informed consent to anticipated uses before or at the time personal information is collected. The incremental deployment of EHRs for health care purposes, without any contemplation of research uses, has ensured that this requirement will simply not be met at the time of collection as EHR systems are being built. Moreover, it seems that it will be technologically and organizationally impracticable, if not impossible, to re-contact all patients, after the initial creation of EHR systems, to seek their consent to use EHRs for health research and to record and manage the resultant responses in electronic consent management directives. Deployment in advance of addressing research uses is effectively undermining the likelihood that express and informed consent will be the selected policy choice, and thereby pre-determining a forced departure from that standard.

The fact that the current, accepted standard of express and informed consent in advance of collection will apparently be impossible to maintain will not cause research using EHRs to grind to a halt. Rather, the compelling public benefits associated with the use of EHRs for research purposes will serve as a catalyst for altering the standard of consent or, even more significantly, shifting away from consent as the default access control. There is already a growing consensus in the academic literature that some type of shift away from the existing standard of express and informed consent will be necessary to overcome inherent practical and technological difficulties and to facilitate the use of EHRs (or equivalent vast stores of valuable personal information) for health research purposes.<sup>148</sup>

To avoid “succumbing to a technological imperative”<sup>149</sup> and letting practical expedience further determine, by default, critical public policy choices that implicate human rights and human dignity, public debate is required about what viable alternatives exist to replace specific, informed consent. In this paper we have outlined what some of those policy alternatives might be, together with a range of possible implications, in order to stimulate such a debate. We have outlined options that began with specific, informed consent, and moved towards broad consent, implied consent, no need for consent, consent waiver, and retroactive override of previous consent regimes. Through this spectrum of options we have attempted to demonstrate

---

<sup>147</sup> *Dyment, supra* note 46 at 433.

<sup>148</sup> See e.g. J.V. Tu *et al.*, “Impracticability of Informed Consent in the Registry of the Canadian Stroke Network” (2004) 350 N. Eng. J. Med. 1414; Caulfield, Upshur & Daar, *supra* note 70; Peter Singleton & Michael Wadsworth, “Confidentiality and consent in medical research: Consent for the use of personal medical data in research” 333 B.M.J. (2006) 255; Ries, *supra* note 122.

<sup>149</sup> Glenn Griener, “Electronic Health Records as a Threat to Privacy” (2005) 1 Health Law Review 14 at 15.



that legal and policy ideals require early reflection and up-front integration into systems as they are being designed, since we can anticipate that technological and organizational aspects will become impossible to retrofit after the fact. Conversely, we have attempted to show that where policy options appear to be attractive from a practical perspective of ease and convenience, the underlying legal and policy implications show cause for concern and require further reflection and public debate before we gravitate too quickly to these proposed solutions.

Deploying EHRs in advance of addressing consent to secondary research uses of personal information has effectively stacked the deck against the maintenance of the *status quo*, which is express, informed, and specific consent. We must be mindful of this artificially created policy context *when* (as opposed to *if*) the time comes to determine whether an alternative to the existing standard of express and informed consent can be justified and what it would look like. Driven by the incremental deployment of EHRs designed exclusively for health care purposes, the case for moving away from the need to obtain express and informed consent presently rests on arguments that invoke speculative technological and pragmatic hurdles. The pragmatic hurdles, though speculative, are evident. The technological issues, doubtlessly made more complicated by the incremental deployment of EHRs designed to address only health care purposes, are, however, more difficult to accept, particularly when the opportunity is present *now* to avoid policy procrastination and effectively address some of these issues.

The legal, ethical, and policy difficulties inherent in the alternatives to express and informed consent that we have surveyed suggest that there is no easy or ready substitute for express and informed consent, despite their appearance as panaceas to difficult practical problems. It is not clear that when policy-makers eventually do turn their minds to research uses of EHRs, Canadians would be willing to cede all meaningful and ongoing control over their personal health information, even in support of researchers' pursuit of important public benefits. The case for why Canadians should be required to do so is even less clear and compelling, especially if they are not part of an open and inclusive policy debate over the available choices.

The policy options we have highlighted are not mutually exclusive. Their viability and appropriateness will vary by the type of research undertaken. For example, it would be difficult to cogently argue that anything less than specific and express informed consent could adequately authorize clinical trials involving human subjects. The same may not be true of retrospective epidemiological research that relies exclusively on pre-existing health records or prospective population-based studies using personal information contained in research registries or platforms originally created for that general purpose.

Moreover, none of the proposed policy options obviate the need to apply research ethics guidelines and seek review and approval from research ethics boards. Quite the contrary, all of the policy options we have canvassed reveal the need for strong and effective ethical governance regimes, particularly as policy-makers contemplate moving away from informed consent as the governing principle for some types of research.

The need for strong public and stakeholder approval is also equally pronounced in each of the policy options we have surveyed. It may be difficult to see how some of the policy options canvassed—especially the options of resorting to existing legislative exemptions or enacting new, retroactive legislation—are consistent with the critical need to maintain users' trust in their health care providers and in the system itself. Yet, public trust, which sits at the foundation of these critical relationships, must be continually nurtured and facilitated as a core component of any policy option that would permit researchers access to EHR data for secondary health research purposes, particularly in the absence of express and informed consent.