Canadian Journal of Law and Technology

Volume 14 | Number 1 Article 8

1-1-2016

Protecting the Privacy of Canadians' Health Information in the Cloud

Adrian Thorogood

Howard Simkevitz

Mark Phillips

Edward S. Dove

Yann Joly

Protecting the Privacy of Canadians' Health Information in the Cloud

Adrian Thorogood[*], Howard Simkevitz[**], Mark Phillips[***], Edward S. Dove[†], Yann Joly[††]

We would like to thank the Office of the Privacy Commissioner of Canada for supporting this research through its Contributions Program 2014-2015.

INTRODUCTION

New computing, networking, IT security and outsourcing solutions are revolutionizing healthcare and health research. An important application of these technologies is the integration of genomic data into modern health systems. The staggering size of genomic datasets makes it difficult for healthcare providers and researchers to store, link and analyze them on any one server. Cloud computing—a diverse set of technologies and business practices that facilitate the storage, analysis and sharing of data—is already seen as essential for driving genomic research, which itself is driven by Big Data.[1] By the same logic, cloud computing may soon be needed to facilitate the integration of genomic data into healthcare contexts as molecular discoveries are translated into new clinical applications.

This article considers how Canadian health privacy laws apply to cloud computing in genomic research and medicine. We consider these laws because genomic datasets contain personal health information (PHI), including both genomic data (which is inherently individuating) and associated phenotypic and clinical data. Health privacy laws regulate the collection, use, and disclosure of personal health information,[2] including the outsourcing of PHI processing to service providers. While we focus on genomics in the cloud, our legal analysis

[*] Academic Associate, Centre of Genomics and Policy, Faculty of Medicine, McGill University, Montreal, Canada. adrian.thorogood@mcgill.ca

[**] General Counsel and Privacy Officer, Ontario Institute for Cancer Research, MaRS Centre Toronto, Canada. howard.simkevitz@oicr.on.ca

[***] Academic Associate, Centre of Genomics and Policy, Faculty of Medicine, McGill University, Montreal, Canada. mark.phillips2@mcgill.ca

[†] JK Mason Institute for Medicine, Life Sciences and the Law, School of Law, University of Edinburgh, United Kingdom. edward.dove@ed.ac.uk

[††] Associate Professor, Centre of Genomics and Policy, Faculty of Medicine, McGill University, Montreal, Canada. yann.joly@mcgill.ca

[1] Lincoln D. Stein et al, "Data Analysis: Create a Cloud Commons" (2015) 523:7559 Nature 149.

[2] We refer to PHI throughout and not personal information generally. Our discussion

applies generally to PHI in the cloud. As a general rule, a custodian requires the data subject's consent to disclose PHI to a third party. Exceptionally, custodians are permitted to transfer PHI to service providers, including cloud service providers (CSPs), without the data subject's consent. Such a transfer is only permitted if the custodian and service provider establish a service contract (e.g., a "cloud contract"). This contract must minimally ensure that the service provider protects the PHI and only uses it for authorized purposes. Some provincial laws impose additional requirements for such contracts.

We review the legal requirements for conducting genomic research and medicine in the cloud, identifying gaps in privacy protection, and variation in protection across provinces. Given the technological, organizational, and multi-jurisdictional complexity of cloud services, cloud contracts must address a host of privacy concerns. Technologically speaking, cloud services involve dynamic transfers between multiple data centres and endpoints, co-locate multiple clients on any given server, and deliver access over the public Internet. Cloud contracts must therefore ensure sophisticated security standards are met. Organizationally speaking, cloud services involve many hand-offs of responsibility for privacy and security as the data travel from custodian to data centre. Cloud contracts need to ensure responsibility is appropriately allocated along the chain of custody. Jurisdictionally, cloud services involve routine transfer and access across borders, raising concerns over surveillance and compelled disclosure under foreign law. These issues have come to a head with the European Court of Justice's decisions in *Schrems* on the adequacy of the EU-U.S. Safe Harbour data-sharing framework, which found that mass surveillance by the U.S. government undermined the European right to protection of personal data.[3] By contrast, Canadian policy debate on cross-border transfers remains relatively subdued. Additional concerns are whether cloud services can comply with the laws of multiple jurisdictions and whether individuals or responsible custodians can enforce privacy related obligations practically when data are stored and processed abroad. To reinforce our legislative review, we also review the Terms of Service of six CSPs with offerings in Canada. Our review of cloud contracts reveals that current contractual practices do not resolve adequately legislative gaps in privacy protection.

In this article, we argue that more detailed requirements are needed for cloud contracts involving the transfer of PHI if privacy is to be protected in cloud-based genomics. These requirements should either be incorporated into Canadian privacy laws, or issued as guidance by Canadian privacy commissioners. The enhancement of privacy protections in the cloud also needs to be coordinated nationally and internationally to minimize confusion

---

encompasses health sector laws that apply only to PHI, as well as public and private sector laws that apply to PHI by virtue of it being a subset of personal information.

3 *Schrems v. Data Protection Commissioner*, C-362/14, [unpublished], online: <curia.europa.eu> [*Schrems*].

and promote the interoperability of standard cloud contracts across jurisdictions. In the spirit of current regulation, new requirements would be drafted with enough technical neutrality and flexibility to address emerging concerns, reflect local contexts, and impose clear obligations while avoiding becoming mired in soon-to-be-obsolete technical detail. Without meaningful protections for PHI under cloud contracts, Canadian researchers and health care providers may be reluctant to take advantage of cloud services, which is likely to hinder progress in genomics and healthcare delivery.

This article presents results from a year-long research project reviewing health privacy issues in the cloud, funded by the Contributions Program of the Office of the Privacy Commissioner of Canada (OPC). Section I provides a brief primer on cloud computing and its applications in data-centric health research and health care. Section II reviews Canadian privacy and health privacy laws and how they apply to CSPs. Section III identifies privacy risks arising from the technological, organizational, and jurisdictional complexity of cloud computing. Section IV argues that Canadian health privacy laws fail to address difficulties custodians face in balancing responsibilities with CSPs, determining whether foreign laws offer comparable protection, and ensuring transparency is maintained as data migrates to the cloud. In Section V, we survey standard agreements (Terms of Service) and privacy policies of leading CSPs, arguing that cloud contracts do not sufficiently address gaps in legislative protection for privacy and security. In Section VI, we identify the discrepancies in Canadian laws that apply to PHI which threaten interoperability of cloud contracts across provinces. This review is the first comprehensive review of legal and contractual privacy protections in the Canadian health sector. By identifying potential gaps in protection, we aim to inform the business decisions and contractual practices of both custodians and CSPs in Canada. By identifying discrepancies across provinces, we also aim to stimulate cooperative reform and harmonization of health privacy governance across Canada.

I. A BRIEF PRIMER ON CLOUD COMPUTING

(i) Table 1: Terminology and Acronyms

Cloud contract: synonym for 'Terms of Service' agreement governing a cloud computing arrangement between a CSP and a custodian.
Cloud service provider (CSP): a company that offers some component of cloud computing.
Custodian: an entity which has custody or control of personal health information and is accountable under Canadian privacy law to protect that information
De-identified information: under Canadian law, information that has been rendered not identifiable.

Identifying information: information about identifiable individuals—i.e., "information that identifies an individual or for which it is reasonably foreseeable that it could be utilized, either alone or with other information, to identify an individual."[4]
Personal health information (PHI): identifying information about an individual that relates to physical or mental health—including the health history of the individual's family—or relates to the provision of health care to the individual. Intended to be broad, and typically includes diagnostic, treatment, and care information, health care provider information, registration information (demographics, address, etc.), and information derived from bodily materials.[5]
Service provider: an entity that processes personal information on behalf of a custodian.
Terms of Service: the complete agreement between custodian and CSP, usually stipulated through terms and conditions in multiple documents (e.g., service level agreement, privacy policy, acceptable use policy, terms of use).

(a) Cloud Computing

Cloud computing generally refers to technologies and business practices that offer scalable, on-demand access to a configurable pool of computing resources (e.g., networks, servers, storage, applications, and services) over the Internet.[6] Cloud computing is, relatively speaking, low cost in terms of allowing access to resources due to its "elasticity": its on-demand services allow subscribers to pay only for what they need and to automatically engage additional features.[7] It

---

4 Michael Power, *The Law of Privacy* (Markham, Ont.: LexisNexis, 2013) at 2.22 (this is a generic definition for Canada. For direct references and discussion of variation between statutes, see subsection "Definition of Identifiable," below). Also defined in research guidelines: 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* (Ottawa: Secretariat on Responsible Conduct of Research, 2014) at 57—59, online: <www.pre.ethics.gc.ca/pdf/eng/tcps2-2014/TCPS_2_FINAL_Web.pdf> [*TCPS*].

5 Power, *supra* note 4 at 2.22. See, e.g., *Health Information Act*, R.S.A. 2000, c. H-5, s. 1(1) [Alberta's *HIA*]; *Personal Health Information Privacy and Access Act*, S.N.B. 2009, c. P-7.05, s. 1 [New Brunswick's *PHIPA*]; *Personal Health Information Act*, S.N. 2008, c. P-7.01, s. 5(5) [Newfoundland's *PHIA*]; *Personal Health Information Protection Act*, S.O. 2004, c. 3, Schedule A, s. 4(2) [Ontario's *PHIPA*].

6 Jonathan J.M. Seddon & Wendy L. Currie, "Cloud Computing and Trans-Border Health Data: Unpacking U.S. and EU Healthcare Regulation and Compliance" (2013) 2:4 Health Policy & Technology 229; US, National Institute of Standards and Technology, *Guidelines on Security and Privacy in Public Cloud Computing* (Special Publication 800-144 by Wayne Jansen & Timothy Grance) (Gaithersburg, MD: US Department of Commerce, 2011) at vi, online: <nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf> [NIST, *Security & Privacy*].

7 Howard Simkevitz, "Privacy in the Cloud," online: (2013) 13:2 Ontario Bar Association Privacy L. Rev. <www.oba.org/en/pdf/sec_news_pri_may13_PrivacyCloud_Simkevitz.pdf>.

offers increased storage capacity and increasingly efficient processing.[8] Provision of services remotely allows multiple geographically dispersed collaborators to rapidly access the same data.

Genomic researchers hope to reap several advantages from moving to a cloud computing environment.[9] First, the growth of a given genomic database (which includes both genomic data derived from samples and associated health data) may proceed at a rapid and unpredictable rate as samples are collected and sequenced, or as the databases of smaller studies are aggregated. Cloud computing services can be flexibly scaled to match need, thereby reducing large upfront capital expenditures. Second, the cloud's ability to provide remote access benefits projects with multiple geographically disparate collaborators and databases designed as platforms (e.g., "genomic biobanks") for use by external researchers internationally.[10] Given the size of genomic databases, remote access may even become necessary for genomic research. Researchers accessing genomic databases already spend weeks downloading data to local servers. The cloud allows analytic tools to be uploaded to the cloud instead, quickly and securely.[11] Third, outsourcing computing services to commercial CSPs can relieve researchers from the cost and IT burden of establishing and managing an internal computing environment, including a significant measure of security oversight, potentially making research more cost-effective.

While a healthcare or research institution or university may have the capacity to launch its own "private" cloud, commercial services providing "public" clouds are more often associated with scalable, remotely accessible, and affordable cloud services. Cloud computing deployment models vary in ways that have significant implications for participant (i.e., data subject) privacy. This article focuses on public clouds because they already have established scale, international scope, cost efficiencies, and security expertise difficult for private clouds built from the ground up to rival—and because they raise more complex privacy issues.

Public CSPs offer a variety of service categories. A cloud computing environment is comprised of five conceptual layers. The bottom two layers are "physical": basic facilities and computing hardware. The top three layers are "logical" or virtual: the "platform architecture layer" for software development, and the "application layer" for end users.[12] The physical layers typically remain entirely under the control of the CSP, while the client can choose to interact to

---

8 *Ibid.*

9 See, e.g., Dov Greenbaum & Mark Gerstein, "The Role of Cloud Computing in Managing the Deluge of Potentially Private Genetic Data" (2011) 11:11 American J. Bioethics 39.

10 *Cf* Dov Greenbaum et al, "Genomics and Privacy: Implications of the New Reality of Closed Data for the Field" (2011) 7:12 PLoS Computational Biology Special Section 1.

11 Edward S. Dove et al, "Genomic Cloud Computing: Legal and Ethical Points to Consider" (2015) 23:10 European J. Human Genetics 1271.

12 NIST, *Security & Privacy*, *supra* note 6 at 5 [emphasis removed].

varying degrees with the logical layers. Depending on the degree of desired interaction, the form of cloud services can be described in one of three ways:

- Infrastructure-as-a-Service (IaaS): provides researchers access to raw computing hardware. They can upload their analytic software into the cloud, run the software, and download the compiled results.
- Platform-as-a-Service (PaaS): offers a platform on which researchers can develop and run applications to analyze research data.
- Software-as-a-Service (SaaS): offers researchers access to software applications they can run on the cloud.

Cloud services may also be layered. For example, a CSP offering a platform or application may be established on the infrastructure of another CSP. Again, the details ideally need not concern any particular downstream client. Various commercial cloud computing platforms have emerged for genomic researchers—such as Galaxy, Bionimbus, and DNAnexus—which allow researchers to perform genomic analyses using only a web browser.[13] In addition to public and private cloud computing models, so-called "hybrid" clouds exist.[14] These hybrid clouds can offer unique privacy advantages by allowing different pieces of information from the same source to be alternatively secured and made more accessible, depending on the information's sensitivity.[15]

(i) Table 2: Cloud Deployment Models

Private cloud: The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of both, and it may exist on or off premises.
Community Cloud: The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations with shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.
Public Cloud: The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business,

---

[13] Dove et al, *supra* note 11.

[14] US, *The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology* (Special Publication 800-145 by Peter Mell & Timothy Grance) (Gaithersburg, MD: US Department of Commerce, 2011) at 3, online: < nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf > .

[15] "Hybrid Cloud Computing: Establishing a Definition & Discovering the True Benefits of a Hybrid Approach," *Cybertrend: Technology for Business* 13:2 (February 2015) 8, online: < www/cybertrend.com > .

academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.
Hybrid Cloud: The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).[16]

To reiterate, commercial cloud services typically have five elements:

1. *On-demand self-service*: the client can automatically request computation and storage.
2. *Broad network access*: resources available over a network (i.e., the Internet) for access with standard devices.
3. *Resource pooling*: multi-tenant model (discussed below)
4. *Rapid elasticity*: of computing and storage capabilities.
5. *Measured service*: various aspects of use are measured for customer transparency and automatic service optimization.[17]

However, the benefits of the cloud coincide with drawbacks. The inner architecture of the full cloud computing environment[18] remains significantly more complicated than the virtual computing portal accessed by the client, who can remain ignorant of the robust "back-end" for which the CSP remains responsible. Although this model can advantageously insulate clients from the cloud's technical details, it also tends to place them at its mercy.[19]

(b) Cloud Services in Canadian Healthcare and Health Research

Commercial cloud services have many existing and potential applications to healthcare and health research. On the SaaS end of the spectrum, a number of generic and health services-specific uses of cloud services are used for document management, storage, patient-management, billing, webhosting, email, and teleconferencing.[20] However, the real pressure to adopt cloud computing is felt in data-centric health research and medicine, fueled by advances in genomic

[16] US, *Cloud Computing Synopsis and Recommendations: Recommendations of the National Institute of Standards and Technology* (Special Publication 800-146 by Lee Badger et al) (Gaithersburg, MD: US Department of Commerce, 2012), online: < nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-146.pdf > .

[17] Canada Health Infoway, "Cloud Computing in Health: White Paper" (2012) at 11, online: < https://www.infoway-inforoute.ca/en/component/edocman/545-cloud-computing-in-health-white-paper-full/view-document > .

[18] Irrespective of whether it takes the form of IaaS, PaaS, or SaaS.

[19] See generally David Lametti, "The Cloud: Boundless Digital Potential or Enclosure 3.0?" (2012) 17:3 Va. J.L. & Tech 190.

[20] Carolina A. Klein, "Cloudy Confidentiality: Clinical and Legal Implications of Cloud Computing in Health Care" (2011) 39:4 J. American Academy Psychiatry & L. Online 571.

sequencing, medical imaging and bioinformatics.[21] In this article, we focus on the expanding demand of cloud services in genomic research. Genome-wide association studies (GWAS), which compare genetic variants across many individuals, have proven to be an excellent way of identifying common genetic variants associated with health and disease.[22] Advances in computational biology and bioinformatics have accelerated the translation of genomic research findings into clinical applications.[23] Several trends in genomic research have led to the development of vast datasets, comprising genomic and associated health data from a large number of individuals: "[t]he confluence of cheap computing and high-throughput sequencing technologies is making genomic data increasingly easy to collect, store, and process. At the same time, genomic data is being integrated into a wide range of applications in diverse settings."[24]

While computing demand is currently acute in research, this will eventually also be the case for healthcare when it begins to integrate this deluge of genomic data into clinical decision-making. The cost of genomic sequencing has sharply declined in recent years, contributing to a significant increase in the amount of available genomic data.[25] A combination of inputs emanating from the personal genomics industry, grassroots patient projects, and academic research efforts have led to hundreds of thousands of genetic sequences being deposited and made accessible online.[26] Significant efforts have been made to make this data

---

21 Vivien Marx, "Genomics in the Clouds" (2013) 10:10 Nature Methods 941.

22 David Altshuler et al, "Creating a Global Alliance to Enable Responsible Sharing of Genomic and Clinical Data" (Proceedings of the Global Alliance for Genomics and Health Conference, New York, 3 June 2013) [unpublished], online: <https://www.broadinstitute.org/files/news/pdfs/GAWhitePaperJune3.pdf>; Heidi Ledford, "Genome hacker uncovers largest-ever family tree" *Nature News* (30 October 2013), online: <www.nature.com/news/genome-hacker-uncovers-largest-ever-family-tree-1.14037>; Erin M. Ramos et al, "A Mechanism for Controlled Access to GWAS Data: Experience of the GAIN Data Access Committee" (2013) 92:4 American J. Human Genetics 479.

23 Greenbaum et al, *supra* note 10; David Haussler et al, "A Million Cancer Genome Warehouse" (2012) Electrical Engineering and Computer Sciences, University of California at BerkeleyTechnical Report No. UCB/EECS-2012-211, online: <www.eecs.berkeley.edu/Pubs/TechRpts/2012/EECS-2012-211.html>; Lincoln D. Stein, "The Case for Cloud Computing in Genome Informatics" (2010) 11:5 Genome Biology 207.

24 Muhammad Naveed et al, "Privacy in the Genomic Era," online: (2015) arXiv at 29, <arXiv.org>.

25 Mark Gerstein & Dov Greenbaum, "Proceed with caution," *The Scientist* (1 October 1 2013), online: <www.the-scientist.com/?articles.view/articleNo/37592/title/Proceed-with-Caution>; Eilene Zimmerman, "The race to a $100 genome," *CNN Money* (25 June 2013), online: <money.cnn.com/2013/06/25/technology/enterprise/low-cost-genome-sequencing>; U.S., National Human Genome Research Institute, *DNA Sequencing Costs* (15 January 2016), online: <www.genome.gov/sequencingcosts>.

26 US, National Center for Biotechnology Information, *Human Genome Resources* (2013), online: <www.ncbi.nlm.nih.gov/genome/guide/human>.

available to the widest audiences possible, and an important amount of it is now even accessible online without restriction.[27] Some of this data is sensitive or clearly associated with an identifiable person. In order to compare genotypes, rich phenotypic data (such as disease outcomes in medical records) and environmental data are being increasingly collected, and Big Data analytics are now being adopted in health research. Researchers are reaching out beyond standard clinical and genomic health data to other sources of personal data.[28]

Effective genomic analysis requires, among other things, a significant amount of computing and storage capability to mine these research data. Existing research initiatives are becoming incapable of individually assembling the requisite technological tools and infrastructure necessary to perform such analyses. Many genomic researchers now feel that cloud computing is the only model that can provide the storage and processing power needed for Big Data genomic research.[29] It has become common for genomic research projects to require storage reaching multiple petabytes in size.[30] These data masses are problematic not only from the standpoint of storage space, but also from the standpoint of data analysis and data sharing between researchers. These limitations have been noted in the context of health-record storage,[31] and the provision of (open) access to genomic research databases.[32]

Big Data strategies and analytics are becoming common in genomic research and may significantly change the nature of healthcare. Big Data genomics involves "vast stores of information gathered from both traditional sources and, increasingly, new collection points."[33] As researchers turn to new sources for research data (e.g., genomic samples already collected in the context of clinical

---

[27] Canadian Institutes of Health Research, *Balancing Privacy Protections with Open, Collaborative, Biomedical Research: Implications for Updating the CIHR Privacy Best Practices Document*, by Yann Joly, Anne-Marie Tassé & Edward Dove (Ottawa: CIHR, 2011).

[28] Alex Pentland, Todd G. Reid & Tracy Heibeck, "Revolutionizing Medicine and Public Health: Report of the Big Data and Health Working Group" (2013), online: < https://kit.mit.edu/sites/default/files/documents/WISH_BigData_Report.pdf > .

[29] Jacqueline Vanacek, "How Cloud and Big Data are Impacting the Human Genome—-Touching 7 Billion Lives" (16 April 2012), *SAPVoice* (blog), online: < www.forbes.com/sites/sap/#6aba80d35a42 > .

[30] Dove et al, *supra* note 11.

[31] Amy L. McGuire et al, "Confidentiality, Privacy, and Security of Genetic and Genomic Test Information in Electronic health Records: Points to Consider" (2008) 10:7 Genetics in Medicine 495.

[32] Jane Kaye et al, "Data Sharing in Genomics—Re-shaping Scientific Practice" (2009) 10:5 Nature Reviews Genetics 331 at 334.

[33] Office of the Privacy Commissioner of Canada, "Privacy and Cyber Security: Emphasizing Privacy Protection in Cyber Security Activities" (Gatineau: OPC, December 2014) at 4, online: < https://www.priv.gc.ca/information/research-recherche/2014/cs_201412_e.pdf > [OPC, "Privacy & Computer Security"].

care) and combine multiple existing data sources into larger collections, several existing privacy concerns are intensified, while others newly emerge.

II. PRIVACY LAWS AND HEALTH PRIVACY LAWS IN CANADA

A complex assortment of legal and regulatory frameworks govern privacy in Canada.[34] This article focuses on the privacy laws that regulate the collection, use and disclosure of PHI by health custodians.[35] These laws apply to "custodians"—individuals or organizations with custody or control over personal information or PHI.[36] They also apply to service providers (including CSPs) who store, analyze, or otherwise process PHI on behalf of custodians. References to and acronyms for major Canadian privacy laws can be found in Appendix 1. Personal information generally refers to information about identifiable individuals, and is sometimes defined as identifying information—i.e., "information. . .for which it is reasonably foreseeable that it could. . .either alone or with other information. . .identify an individual."[37] Most provinces have health sector privacy laws that apply specifically to custodians of PHI. In Canada, PHI is a subset of personal information that relates to health. It is:

---

[34] David Krebs, "Regulating the Cloud: A Comparative Analysis of the Current and Proposed Privacy Frameworks in Canada and the European Union" (2012) 10:1 C.J.L.T. 29 at 50; Office of the Privacy Commissioner of Canada, "Reaching for the Cloud(s): Privacy Issues related to Cloud Computing" (Gatineau: OPC, March 2010), online: <https://www.priv.gc.ca/information/research-recherche/2010/cc_201003_e.pdf> [OPC, "Reaching for the Clouds"]; Christopher Kuner, *Transborder Data Flows and Data Privacy Law* (Oxford: Oxford University Press, 2013) at 174-175.

[35] See Appendix 1 for a list of Canadian privacy statutes. See also Power, *supra* note 4 at 5.104; Canadian Institutes of Health Research, by Patricia Kosseim, ed, 2nd ed by Adam Kardash & Antonella Penta (Ottawa: Public Works and Government Services Canada, 2005) at 211, online: <publications.gc.ca/collections/collection_2007/cihr-irsc/MR21-22-2005E.pdf>. Other statutory and common law regimes also govern privacy in the health context, but are not discussed here (e.g., An Act respecting health services and social services, R.S.Q. c. S-4.2; *Public Hospitals Act*, R.S.O. 1990, c. P.40) Health researchers are additionally bound by national ethics policies, and oversight from research community self-regulatory bodies (e.g., research ethics boards, data access committees).

[36] Power, *supra* note 4 at 5.13. See e.g., *Personal Information Protection and Electronic Documents* Act, S.C. 2000, c. 5, s. 4(1) [*PIPEDA*]; Alberta's *HIA*, *supra* note 5, s. 1(1)(f); *Health Information Protection Act*, S.S. 1999, c. H-0.021, s. 2(t) [Saskatchewan's *HIPA*]; *Personal Health Information Act*, S.M. 2008, c. 41, s. 1(1) [Manitoba's *PHIA*]; Ontario's *PHIPA*, *supra* note 5, s. 3; *An Act respecting the protection of personal information in the private sector*, R.S.Q., c. P-39.1, ss. 4ff [Quebec's *PPIPS*]; New Brunswick's *PHIPA*, *supra* note 5, s. 1; *Personal Health Information Act*, S.N.S. 2010, c. 41, s. 3(f) [Nova Scotia's *PHIA*]; *Health Information Act*, S.P.E.I. 2014, c. 31, s. 1(e) [not yet in force; Prince Edward Island's *HIA*]; Newfoundland's *PHIA*, *supra* note 5, s. 4; *Health Information Privacy and Management Act*, S.Y. 2013, c. 16, s. 2(1) [Yukon's *HIPMA*].

[37] For direct citations and variation between statutes, see subsection "Definition of Identifiable" *infra* .

> identifying information about an individual in oral or recorded form if it relates to the physical or mental health of the individual, including the health history of the individual's family, or relates to the provision of health care to the individual. This is meant to capture a broad swath of information, including diagnostic, treatment and care information...; health care provider information...; and registration information (e.g., patient demographic information, patient address and contact information, patient eligibility and billing information).[38]

Both federal and provincial laws may apply to the processing of personal information in the private sector. Constitutionally speaking, federal jurisdiction over personal information is grounded in the trade and commerce power, provincial jurisdiction in the property and civil rights power.[39] The *Privacy Act* governs federal public sector custodians (mainly government institutions).[40] The *Personal Information Protection and Electronic Documents Act* (*PIPEDA*) governs all federal and provincial private sector organizations by default.[41] In addition to their own public and private sector laws, provinces may also have health sector privacy laws, as provinces have general jurisdiction over health matters.[42] Provincial health sector laws apply specifically to custodians of PHI to the exclusion of provincial private or public sector statutes. In provinces without health sector laws, PHI is still protected by provincial public or private sector laws as a type of personal information.[43] Provincial health sector statutes and (in their absence) private sector statutes only displace federal law whenever they have been deemed to be "substantially similar" to *PIPEDA* by the federal government.[44] Even then, *PIPEDA* continues to apply whenever PHI travels

---

[38] Power, *supra* note 4 at 2.21. See e.g., Alberta's *HIA*, *supra* note 5, s. 1(1)(k); Saskatchewan's *HIPA*, *supra* note 36, s. 2(m); Manitoba's *PHIA*, *supra* note 36, s. 1(1); Ontario's *PHIPA*, *supra* note 5, s. 4; New Brunswick's *PHIPA*, *supra* note 5, s. 1; Nova Scotia's *PHIA*, *supra* note 36, s. 3(r); Prince Edward Island's *HIA*, *supra* note 36, s. 1(t).

[39] *Constitution Act, 1867* (U.K.), 30 & 31 Vict., c. 3, reprinted in R.S.C. 1985, Appendix II, No. 5, ss. 91—92.

[40] *Privacy Act*, R.S.C. 1985, c. P-21.

[41] *PIPEDA*, *supra* note 36.

[42] Interpretation under *Constitution Act, 1867*, *supra* note 39, s. 92(16). See *Schneider v. British Columbia*, 1982 CarswellBC 241, 1982 CarswellBC 741, [1982] 2 S.C.R. 112, 139 D.L.R. (3d) 417, [1982] S.C.J. No. 64 (S.C.C.).

[43] See *Rousseau v. Wyndowe*, 2006 CF 1312, 2006 FC 1312, 2006 CarswellNat 3486, 2006 CarswellNat 4832, 56 Admin. L.R. (4th) 92 , [2006] F.C.J. No. 1631 (F.C.), reversed 2008 CAF 39, 2008 FCA 39, 2008 CarswellNat 246, 2008 CarswellNat 1530, 373 N.R. 301, [2008] F.C.J. No. 151 (F.C.A.).

[44] As certified by a formal Order-in-Council, on the recommendation of the OPC, according to the following criteria: "[L]aws that are substantially similar: provide privacy protection that is consistent with and equivalent to that found under *PIPEDA*; incorporate the ten principles in Schedule 1 of *PIPEDA*; provide for an independent and effective oversight and redress mechanism with powers to investigate; and restrict the collection, use and disclosure of personal information to purposes that are appropriate

across provincial or national borders. Currently, eight provinces have health privacy laws. To date, three have been deemed substantially similar to *PIPEDA* (Ontario's *PHIPA*, New Brunswick's *PHIPA*, Newfoundland's *PHIA*); five have not (Alberta's *HIA*, Manitoba's *PHIA*, Nova Scotia's *PHIA*, Saskatchewan's *HIPA*, Prince Edward Island's *HIA*).

In short, Canada has a general private sector privacy framework (*PIPEDA*), as well as specific provincial rules that apply to the collection, use and disclosure of PHI in the health sector. By contrast, Europe has a general privacy framework, the EU Data Protection Directive, which applies to *any* entity (public or private, individual or organization) that is a "controller" of personal information or PHI.[45] The U.S. *Health Insurance Portability and Accountability Act* (*HIPAA*), and more specifically its Privacy Rule, applies federally across the U.S. health sector, but only to specific categories of health sector custodians (i.e., "covered entities"), including healthcare providers, health plans, and healthcare clearinghouses, as well as their business associates (e.g., CSPs).[46]

Canadian privacy laws limit collection, use and disclosure of PHI to purposes authorized by individual consent or by law. The drafting and interpretation of Canadian privacy laws were heavily influenced by the Fair Information Practice Principles originally set out in the 1980 OECD Guidelines[47] and incorporated formally or informally into Canadian privacy laws.[48] These principles require custodians to safeguard personal information, notify individuals of information handling practices, seek consent to processing, and to allow individuals to access their personal information, among others. If a custodian or CSP fails to respect privacy obligations, an individual may complain to the appropriate privacy commissioner, whose office is established through the relevant privacy statute. In response, privacy commissioners in Canada have varying powers to make recommendations or compliance orders, such as a cease-and-desist order, to address the complaint.[49]

---

or legitimate"(Office of the Privacy Commissioner of Canada, "Legal Information related to *PIPEDA*: Substantially Similar Provincial Legislation" (OPC, 2013), online: < priv.gc.ca/leg_c/legislation/ss_index_e.asp > .

45 EC, *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, [1995] O.J., L. 281/31 at art 2(d) [EC, *Directive 95/46*]. As we discuss below, the Directive is due to be replaced in mid-2018 with a General Data Protection Regulation.

46 *Health Insurance Portability and Accountability Act of 1996*, Pub. L. No. 104-191, 110 Stat. 1936 (1996), 45 C.F.R. § 160, 164 (1996) [*HIPAA Privacy Rule*].

47 OECD, Directorate for Science, Technology and Innovation, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, (1980), online: < www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm > [OECD, *1980 Guidelines*].

48 See, e.g., *PIPEDA*, *supra* note 36, Schedule 1.

49 Council of Canadian Academies, *Accessing Health and Health-Related Data in Canada: The Expert Panel on Timely Access to Health and Social Data for Health Research and*

Recognizing the necessity of data outsourcing, Canadian privacy laws permit custodians to transfer PHI to a service provider without individual consent.[50] The minimum conditions for such a transfer are that the custodian binds the service provider by contract to:

1. limit use of PHI to purposes authorized by the custodian, and
2. protect the privacy and security of the PHI (i.e., take reasonable steps to secure the PHI against loss, theft, or unauthorized use or disclosure).[51]

These minimum contractual requirements are reinforced by the accountability principle, which requires custodians to ensure a comparable level of protection for PHI processed by a third party.[52] Service providers who fail to respect these minimum conditions may be regulated directly as custodians. The OPC has opined that transfers of PHI to CSPs satisfying these conditions are permitted under *PIPEDA*.[53]

It should be noted that most major CSPs operating in Canada are based in the United States.[54] This can raise some legal challenges, as we discuss below,

---

Health System Innovation (Ottawa: CCA, 2015) at 197-198, online: <www.scienceadvice.ca/uploads/eng/assessments%20and%20publications%20and%20news%20releases/Health-data/HealthDataFullReportEn.pdf>. See e.g., *Personal Information Protection Act*, S.A. 2003, c. P-6.5, s. 54 [Alberta's *PIPA*]; *Personal Information Protection Act*, S.B.C. 2003, c. 63, s. 52 [British Columbia's *PIPA*]; Quebec's *PPIPS*, *supra* note 36, s. 55; Ontario's *PHIPA*, *supra* note 5, s. 61(4); Newfoundland's *PHIA*, *supra* note 5, ss.72, 74; New Brunswick's *PHIPA*, *supra* note 5, s. 75; Manitoba's *PHIA*, *supra* note 36, s. 48.1; Saskatchewan's *HIPA*, *supra* note 36, s. 48(1); Alberta's *HIA*, *supra* note 5, s. 80; Nova Scotia's *PHIA*, *supra* note 36, s. 92.

[50] Power, *supra* note 4 at 5.104; Kosseim, Kardash & Penta, *supra* note 35 at 211. Health privacy laws with explicit "information manager" provisions include Alberta's *HIA*, *supra* note 5, s. 66(1); Manitoba's *PHIA*, *supra* note 36, s. 1(1); New Brunswick's *PHIPA*, *supra* note 5, s. 1; Newfoundland's *PHIA*, *supra* note 5, s. 2(1)(1); Saskatchewan's *HIPA*, *supra* note 36, s. 2(j).

[51] Power, *supra* note 4 at 7.44. See e.g., Alberta's *HIA*, *supra* note 5, s. 66(2); Manitoba's *PHIA*, *supra* note 36, s. 25(3); New Brunswick's *PHIPA*, *supra* note 5, s. 52(1); Newfoundland's *PHIA*, *supra* note 5, s. 22(2). For the US approach, see *HIPAA Privacy Rule*, *supra* note 45, § 164.502(e), 164.532(d),(e), online: US Department of Health & Human Services <www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/businessassociates.html>; see also EC, Article 29 Data Protection Working Party, *Opinion 05/2012 on Cloud Computing* (Brussels: EC, 2012) at 3.3, online: <ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf> [EC, *Opinion 05/2012*].

[52] *PIPEDA*, *supra* note 36, Schedule 1, 4.1.3.

[53] OPC, "Reaching for the Clouds," *supra* note 34 at 13.

[54] Or at the very least, outside of Canada. The Canadian-based cloud data centre run by Digital Ocean, for example, remains relatively anomalous. See Digital Ocean, "Introducing Our New Canadian Datacenter: TOR1," online: <digitalocean.com/company/blog/introducing-our-new-canadian-datacenter-tor1>. From a health-sector perspective, the Canadian cloud infrastructure project the Cancer Genome Collaboratory is also worthy of mention. Among its goals are transferring control of a cloud from

because although Canadians may be adversely impacted by the application of U.S. practices such as government surveillance, Canada cannot easily exert jurisdiction over U.S.-based CSPs, and enforcing privacy rights in foreign jurisdictions presents practical challenges. The EU faces similar problems.[55] The centrepiece of the EU solution to this type of problem, sometimes referred to as the "adequacy" approach, is to prohibit personal data transfer outside the EU unless the EU Commission has ruled that the foreign legal framework to which the data are being transferred maintains adequate privacy protections.[56] No U.S. data-privacy law of general application has been deemed adequate, but EU-U.S. transfers have sometimes relied upon an industry self-certification program specifically designed for this purpose called the EU-U.S. Safe Harbour Framework.[57] As noted above, the EU Commission's finding that the Safe Harbour provided adequate protection for the purpose of personal data transfer outside the EU was recently invalidated by the European Court of Justice due to concerns over mass surveillance by U.S. law enforcement.[58] In Canada, considerably less attention has been paid to the robustness of foreign laws to which Canadians' data are sent. Two public sector acts in Canada that restrict cross-border transfers are discussed below.[59] Custodians, rather than government, are presumably responsible under the accountability principle to assess the adequacy of foreign laws. As we discuss below, the EU imposes strict contractual terms on transfers to service providers outside the EU. Given its market size, Europe may have more ability to dictate the terms of transfer to the cloud than Canada.

Yet, to ensure that privacy is sufficiently protected in the cloud, an effective legal privacy framework must ensure the respective obligations of custodians and CSPs are clearly defined. The framework must also provide meaningful mechanisms for regulators and individuals to enforce these obligations.

CSPs to the health research sector itself. See Cancer Genome Collaboratory, "Cloud computing for collaborative research," online: <cancercollaboratory.org>. In the interest of full disclosure, authors of this article have been directly involved in the Collaboratory project.

55 Although arguably to a decreasing degree, as cloud infrastructure has now begun to be developed in the European Union. See e.g., Jeff Barr, "Now Open—AWS Germany (Frankfurt) Region—EC2, DynamoDB, S3, and Much More" (23 October 2014), *AWS Official Blog* (blog), online: <aws.amazon.com/blogs/aws/aws-region-germany>.

56 See EC, *Directive 95/46*, *supra* note 45, art 25. This approach is being maintained in Article 41 of the General Data Protection Regulation (EC, *Proposal for a regulation of the European Parliament and of the council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)* [2012], online: <ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf>, which is set to supercede the *Directive*.

57 Export.gov, "Welcome to the U.S.-EU & U.S.-Swiss Safe Harbor Frameworks," online: <export.gov/safeharbor>.

58 See *Schrems*, *supra* note 3.

59 See section 5(b), below, "Assessing Protections under Foreign Laws."

Contracts between custodians and CSPs (i.e., "cloud contracts") are essential to ensuring effective protection of PHI in Canada. In the next section, we review the privacy and legal compliance issues in the cloud.

III. PRIVACY ISSUES IN THE CLOUD

While cloud computing promises to facilitate data-centric health research and healthcare,[60] it remains challenging for custodians to contractually ensure the security and privacy of PHI in the cloud.[61] Privacy and security risks in the cloud are not entirely novel, but come in new and complex combinations. They also present themselves to health custodians unfamiliar with advanced IT and service relationships.[62] Here, we review privacy concerns arising from the technological, organizational, and multi-jurisdictional complexity of cloud computing. Subsequent sections in this article will discuss whether existing statutory and contractual privacy protections sufficiently address these concerns.

(a) Technological

The cloud employs a complex computing and networking architecture in order to offer cost efficiency, flexible scale, and remote access over the public Internet. This complex architecture presents arcane security risks, belied by the simple interfaces presented to users.[63] CSPs typically store the data of multiple clients on a single server. An attack on or seizure of one client's data may affect others.[64] Delivering remote access over the public Internet risks online attacks, which are increasingly frequent and sophisticated.[65] The privacy silver lining is that the uniformity of the CSPs' computing environment enables better automation of security-management activities, and may centralize auditing and compliance functions.[66] In addition, switching away from direct download toward remote access has the benefit of sequestering data in the cloud and limiting the number of copies in circulation.[67] Risks associated with cloud

---

60 Krebs, *supra* note 34 at 34; Canada Health Infoway *supra* note 17 at 20—24.

61 Andrea Peterson, "All Your Medical Data in the Cloud? Not So Fast, Says HHS Privacy Official" *ThinkProgress* (9 January 2013), online: < thinkprogress.org/health/2013/01/09/1422081/medical-data-privacy > .

62 NIST, *Security & Privacy*, *supra* note 6 at 37; Krebs, *supra* note 34 at 34—35.

63 NIST, *Security & Privacy*, *supra* note 6 at 10—11.

64 Krebs, *supra* note 34 at 35. See also Yinqian Zhang et al, "Cross-VM Side Channels and Their Use to Extract Private Keys" in Ting Yu, CCS '12: The *Proceedings of the 2012 ACM Conference on Computer and Communications Security, October 16—18, 2012, New York* (New York: Association for Computing Machinery, 2012) 305.

65 OPC, "Privacy & Computer Security", *supra* note 33 at 1; International Organization for Standardization, "ISO/IEC 18028-2:2006: Information Technology—Security Techniques—IT Network Security—Part 2: Network Security Architecture" (ISO, 2006), online: < www.iso.org/iso/catalogue_detail.htm?csnumber = 40009 > .

66 NIST, *Security & Privacy*, *supra* note 6 at 9.

architecture should be considered against the existing risks of internal computing environments.

However, "[c]loud providers can be reluctant to provide details of their security and privacy measures and status, however, since such information is often considered proprietary and might otherwise be used to devise an avenue of attack."[68] Security through obscurity conflicts with the privacy principle of transparent data-handling practices.[69] Custodians cannot continuously monitor the CSP's security without its cooperation, as key aspects of the computing environment are under the CSP's exclusive control.[70] The industry has developed a number of privacy and security standards.[71] It is important that such standards are clearly addressed in cloud contracts.

(b) Organizational

The cloud may involve multiple hand-offs of personal information to subcontractors and between data centres, creating uncertainty about where data resides and who is responsible for ensuring privacy and security. Indeed, subcontracting is prevalent in the cloud.[72] Many providers layer their services on top of the infrastructure of others. In service relationships generally, PHI is exposed to an expanded risk environment. This may be particularly true in the cloud, where information is not only transferred to and from the cloud, but also between multiple intra-cloud locations. Outsourcing expands the circle of insiders on whom privacy protection depends to include the CSP staff and subcontractors, and potentially even other cloud clients when, for example, information is stored in a multi-tenant environment.[73] CSPs may also attract increased attention by entities that aim to breach safeguards as valuable information becomes concentrated in their data centres.[74] On the other hand, CSPs have a larger capacity to invest and specialize in IT security; to employ

---

67 *Ibid* at 10.

68 *Ibid* at 20; See also Nicholette Zeliadt, "Cryptographic Methods Enable Analyses without Privacy Breaches" (2014) 20:6 Nature Medicine 563.

69 Brad Smith, "Building Confidence in the Cloud: A Proposal for Industry and Government Action for Europe to Reap the Benefits of Cloud Computing" (Brussels: Microsoft, 2010), online: <ec.europa.eu/justice/news/consulting_public/0003/contributions/organisations/microsoft_corporation_2nd_document_en.pdf>.

70 NIST, *Security & Privacy*, *supra* note 6 at 20.

71 For further information, industry standards for cloud and network privacy and security are detailed in the Cloud Security Alliance, "Cloud Controls Matrix Working Group" (Cloud Security Alliance, 2014), online: <https://cloudsecurityalliance.org/group/cloud-controls-matrix>.

72 US, Executive Office of the President, President's Council of Advisors on Science and Technology, *Report to the President: Big Data and Privacy: A Technological Perspective* (Washington, D.C.: Executive Office of the President, 2015) at 3.3.1—3.3.2.

73 NIST, *Security & Privacy*, *supra* note 6 at 18.

74 *Ibid* at 29.

state-of-the-art encryption, firewall, and auditing techniques; to update practices to keep pace with ever-emerging vulnerabilities[75]; and to rely on personnel who can specialize in implementing internationally recognized good security and privacy practices.[76]

Outsourcing PHI processing and storage also raises questions about reliability of service and data integrity, especially when the service relationship terminates, either in the course of business or when the CSP goes bankrupt. Since at least 2007, cloud services such as Zimki, Nirvanix, and Google Health have withdrawn their services on short notice, forcing clients to quickly find a means to migrate their data to an alternative provider.[77] A Quebec lawsuit in 2014 was launched after a service provider deleted data belonging to a client who refused to pay an additional fee to have the dynamic cloud data exported to a usable file format.[78] Cloud clients need an exit strategy to ensure they are able to recover their data; to limit the CSP's data access rights; and to ensure that the CSP securely purges their data, including backup or redundant copies.[79]

The central privacy issue for custodians in a cloud service relationship is that they cede significant control to a CSP over:

i. the PHI,
ii. the privacy and security parameters, and
iii. the ability to verify and monitor the implementation and effectiveness of these parameters.[80]

The principal-agent problem arises in relationships where the client and the CSP's incentives or obligations to ensure privacy and security differ. The problem of divergent incentives is likely to be stark where the CSP imposes standard form Terms of Service, reserves the right to modify terms unilaterally, disclaims liability, or where its cost for failed enforcement is lower than the cost of meeting the contractual standards.[81] The client may be able to ensure that the information will receive comparable protection in the cloud as it would otherwise through contract, independent certification, compliance review, or by requiring a demonstration of the CSPs' capabilities.[82] Comprehensive best practices relating to the service relationship in the cloud are available from the Cloud Security

---

75 Dove et al, *supra* note 11.

76 NIST, *Security & Privacy*, *supra* note 6 at 48.

77 Tim Anderson, "Zimki closure shows the perils of hosted web platforms" (27 September 2007), *Tim Anderson's ITWriting* (blog), online: <itwriting.com/blog/337-zimki-closure-shows-the-perils-of-hosted-web-platforms.html>; Dove et al, *supra* note 11.

78 *Dcade Veloneige inc. c. 9230-3437 Québec inc. (Solutions Emerge)*, 2014 QCCQ 4721, 2014 CarswellQue 12673, EYB 2014-245172 (C.Q.).

79 NIST, *Security & Privacy*, *supra* note 6 at 50-51.

80 Canada Health Infoway, *supra* note 17.

81 NIST, *Security & Privacy*, *supra* note 6 at 17.

82 *Ibid* at vii, 48.

Alliance, a non-profit organization that develops best practices.[83] In short, the cloud contract is a key tool to ensure adequate safeguards and to re-establish custodian control and oversight.

(c) Jurisdictional

The "cloud" is an apt analogy for distributed, internationally dispersed, remotely accessible computing. Data may either cross borders when transferred to a foreign CSP, or cross "within" the cloud, between various facilities of a multi-national CSP and its subcontractors. These internal transfers are typically carried out for quality-of-service related reasons, namely for security, back-ups, support, and cost efficiency.[84] Transfers within the cloud can also occur between CSPs and subcontracted CSPs in foreign jurisdictions. Users from a foreign jurisdiction also may be allowed to download or remotely access data in the cloud. Taken individually, none of these cross-border transfers are new, and cross-border data transfer has been discussed in the legal literature for over 40 years.[85] Information has long been outsourced for processing, transferred within multinational corporations, and shared between researchers. But it is the routine automation, combination, and abstraction of such transfers that make the cloud a focal point for these concerns. The cloud also exacerbates confusion about categories of cross-border data flows because it is becoming difficult to distinguish between actively transmitting data and passively making it available.[86] International data sharing is also prominent in genomic research, where combining datasets across borders can increase sample size, improve statistical power, and accelerate findings. This data-sharing culture has been supported by a global infrastructure of international research consortia and public research platforms.[87] In a sense, it is borderless-ness itself that attracts health researchers to the cloud. But privacy concerns have led to restrictions on international flows in Canada and elsewhere, which present a serious barrier to international research collaborations.

PHI transferred to a foreign jurisdiction is vulnerable to compelled disclosure under that jurisdiction's law, notably for surveillance purposes by foreign law enforcement. Compelled disclosure cannot be prevented through contractual means.[88] CSPs are a key target of compelled disclosure because of their increasingly comprehensive stores of valuable information and because the

---

[83] Cloud Security Alliance, *supra* note 71 at 92.

[84] Dove et al, *supra* note 11.

[85] See e.g., Allan Gotlieb, Charles Dalfen & Kenneth Katz, "The Transborder Transfer of Information by Communications and Computer Systems: Issues and Approaches to Guiding Principles" (1974) 68:2 A.J.I.L. 227.

[86] Kuner, *supra* note 34 at 174-5.

[87] Patricia Kosseim et al, "Building a Data Sharing Model for Global Genomic Research" (2014) 15:8 Genome Biology 430 at 430.

[88] Katie Saulnier & Yann Joly, "Locating Biobanks in the Canadian Privacy Maze" (2016) 44:1 The Journal of Law, Medicine & Ethics 7-19.

"architecture of the Cloud allows. . .surveillance to be accomplished with less cost and effort, and more surreptitiously."[89] Because customer data is often separated logically rather than physically, seizure of hardware targeting one customer may, as a consequence, incidentally affect others. A recent trend among CSPs to mitigate their customers' fears is to publicly report on the degree to which they are affected by these practices.[90] More significant would be initiatives such as the EU—U.S. data protection "umbrella agreement", which aims to place at least minimal restrictions on compelled disclosure to authorities.[91]

Data transfer to a foreign jurisdiction also makes it difficult for individuals and custodians to enforce privacy related obligations, or for national privacy authorities to monitor and enforce compliance.[92] It may already be unclear what laws apply in multi-jurisdictional research, and the cloud's nascent stage and porous character adds to this uncertainty.[93] Cloud use complicates ascertaining the applicable law to settle contractual disputes (where the contract is silent) and for determining the proper jurisdictions for a participant to launch a complaint against a CSP.[94]

Privacy concerns may discourage CSPs from accepting uncertain liability, health sector custodians from adopting cloud services, and individuals from partaking in services or research involving the cloud. In the next section, we identify gaps where the Canadian privacy laws fail to address these privacy concerns.

IV. REGULATORY AND LEGISLATIVE GAPS IN PRIVACY PROTECTION

Accountable outsourcing to the cloud in the Canadian health sector is undermined by the limited role of legislation in specifying:

1. how responsibilities are divided between custodian and CSP;
2. when foreign legal regimes allow "comparable protection" to be provided at all; and
3. how the Fair Information Practice principle of transparency translates into specific duties in the cloud.

---

89 Krebs, *supra* note 34 at 46.

90 See e.g., Google, "Google Transparency Report," online: <google.com/transparencyreport/userdatarequests/legalprocess>.

91 EC, *Agreement between the United States of America and the European Union on the Protection of Personal Information Relating to the Prevention, Investigation, Detection, and Prosecution of Criminal Offences* (Draft) (EC), online: <ec.europa.eu/justice/data-protection/files/dp-umbrella-agreement_en.pdf>.

92 OECD, *Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (2013), online: <www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf> [OECD, *2013 Guidelines*].

93 Simkevitz, *supra* note 7.

94 Krebs, *supra* note 34 at 50; OPC, "Reaching for the Clouds," *supra* note 34.

A sophisticated cloud contract is essential to address these uncertainties.

(a) Balancing Custodian and CSP Responsibilities

The primary challenge to privacy and security in the cloud is appropriately dividing responsibility between custodians and CSPs. Depending on the deployment model (see Table 2), CSPs may exercise overwhelming control over personal information, privacy and security safeguards, and monitoring of those safeguards.[95] A fair balance of responsibilities is not guaranteed through cloud contracts where the researcher and CSP do not have equal bargaining power, and where the CSP reserves the right to unilaterally modify terms of their agreement.

A sharp distinction is drawn between custodian and service provider under Canadian laws. The minimal duties imposed on CSPs across Canada are to limit use to authorized purposes and to install privacy safeguards. Statutes may impose these conditions directly on CSPs, and/or indirectly by requiring custodians to establish outsourcing contracts. Where service providers illegally process PHI outside the custodian's instructions, they are regulated directly as custodians.[96] This follows the same principle as the one in play in the context of a limited partnership, where as soon as one of the limited partners begins to exert a managerial role within the partnership, that partner immediately becomes liable for the partnership's debts as a general partner.[97] The CSP becomes responsible for compliance with custodians' obligations.[98] But given the complex, dynamic exchange of data and provision of services in the cloud, it is difficult to assess when the CSP steps outside of authorized purposes.[99] Indeed, a CSP may unilaterally determine many of the technical processes carried out on data, such as creating copies and transferring them across borders for back-up purposes. When do such processes fall outside custodians' instructions?

One legislative approach for balancing obligations between custodians and service providers is to impose a distinct set of privacy duties on service providers directly. This approach is espoused by the European Commission, which recommends better balancing of legislative obligations for controllers and processors in the cloud context.[100] But direct statutory regulation tends to be inflexible, while an optimal allocation of responsibility will vary greatly

---

[95] Canada Health Infoway, *supra* note 17.

[96] OPC, "Reaching for the Clouds," *supra* note 34 at 7.

[97] See e.g., *Limited Partnerships Act*, R.S.O. 1990, c. L.16, s. 13(1): "[a] limited partner is not liable as a general partner unless . . . the limited partner takes part in the control of the business."

[98] EC, Article 29 Data Protection Working Party, *Opinion 1/2010 on the Concepts of "Controller" and "Processor,"* (Brussels, EC, 2010), online: <ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf>; EC, *Opinion 05/2012*, *supra* note 51 at 3.3.1.

[99] Krebs, *supra* note 34 at 42.

[100] EC, *Opinion 05/2012*, *supra* note 51 at 23.

depending on the context of the cloud relationship. In IaaS, the argument is stronger that clients should be primarily accountable. The challenge of appropriately dividing responsibility is further complicated by fast-moving technological change, and the prevalence of subcontracting in the cloud industry. The effectiveness of direct regulation of CSPs is also limited across borders.

The current Canadian approach relies heavily on the "accountability principle".[101] Under *PIPEDA*, this principle requires that when a custodian transfers PHI to a third party, the custodian must employ "contractual or other means to provide a comparable level of protection" to that which is owed by the custodian.[102] Provincial health statutes mandate that custodians must conclude a contract with the CSP. As a consequence, accountability prohibits custodians from using the cloud where comparable protection cannot be provided. It requires custodians to make a number of choices in the cloud context:

- whether to use the cloud at all;
- what types of data to move to the cloud;
- what deployment model to adopt; and
- what specific CSP(s) to engage.[103]

More guidance or requirements are needed to inform such decisions.[104] Specific statutory requirements—e.g., requiring custodians to conduct privacy impact assessments before adopting a new practice—can reinforce accountability.[105] On a second level, accountability requires the establishment of the custodian-CSP agreement that ensures comparable safeguards are in place and that custodial control and oversight are maintained. Given the possible longevity of such relationships, periodic privacy impact assessments, monitoring, and audits might also be needed as contractual terms.

---

[101] See especially OECD, *1980 Guidelines*, *supra* note 47.

[102] See e.g., *PIPEDA*, *supra* note 36, Schedule 1, 4.1.3. For other laws, see subsection on "*Accountability Standard*" below.

[103] UK, Information Commissioner's Office, *Guidance on the Use of Cloud Computing* (2012) at 8, online: <https://ico.org.uk/media/for-organisations/documents/1540/cloud_computing_guidance_for_organisations.pdf>.

[104] Some guidance is available, see e.g., OPC, "Reaching for the Clouds," *supra* note 34; Information and Privacy Commissioner of Ontario, "Privacy in the Clouds: A White Paper on Privacy and Digital Identity: Implications for the Internet," by Ann Cavoukian (Toronto: Information and Privacy Commissioner of Ontario, 2008), online: <https://www.ipc.on.ca/images/resources/privacyintheclouds.pdf>; Office of the Privacy Commissioner of Canada, Office of the Information and Privacy Commissioner of Alberta & Office of the Information and Privacy Commissioner for British Columbia, "Cloud Computing for Small- and Medium-Sized Enterprises: Privacy Responsibilities and Considerations" (OPC, OIPCAB, OIPCBC, 2012), online: OIPCBC <https://www.oipc.bc.ca/guidance-documents/1437>.

[105] See e.g., Alberta's *HIA*, *supra* note 5, s. 64.

(b) Assessing Protections under Foreign Laws

Transfer of PHI not only to another organization, but to one in a foreign jurisdiction, raises distinct accountability issues. First, it may be practically more difficult for custodians to enforce agreements with CSPs governed under foreign laws and courts. Second, determining the jurisdiction of the Canadian Privacy Commissioner over organizations based outside Canada is complex.[106] Third, PHI transferred to foreign jurisdictions is subject to compelled disclosure provisions under foreign laws, most notably in the context of government surveillance. These provisions typically trump contractual safeguards and could adversely affect the privacy of Canadians. In addition, the very notion of a cloud company or PHI being in a foreign jurisdiction is blurred. Is it the jurisdiction in which the CSP does most of its work? Where the data are kept? The site of the CSP's corporate headquarters? Any place where the CSP keeps significant assets? In Canada, accountability requires that custodians determine if privacy protection *provided by the laws of a foreign jurisdiction* is comparable to that of Canada.[107] But should these determinations really be left to custodians, rather than government or individuals?

In Europe, it is either the national data protection authority or the data subject who typically decides whether an international transfer is acceptable. The EU data protection framework restricts international transfers to processors in jurisdictions outside the EU whose laws the European Commission has not deemed "adequate." Transfer may also proceed with the unambiguous consent of the data subject. In stark contrast to the European approach, Canada's *PIPEDA* does not explicitly distinguish between transfer to local CSPs and those in foreign jurisdictions. The OPC has offered interpretive guidance that, "at the very least, a company in Canada that outsources information processing to the United States should notify its customers that the information may be available to the U.S. government or its agencies under a lawful order made in that country".[108] This minimalist right to notification (and opt-out) falls short of the European requirement of unambiguous consent of the "data subject". Quebec's private sector privacy law is unique in specifically requiring individuals be notified of the *place* where their PHI is sent if outside Quebec.[109]

---

[106] A "real and substantial connection" test is applied. See, e.g., Office of the Privacy Commissioner of Canada, "PIPEDA Report of Findings @2015-002: Website that Generates Revenue by Republishing Canadian Court Decisions and Allowing them to be Indexed by Search Engines Contravened PIPEDA" (OPC, 15 June 2015), online: <https://www.priv.gc.ca/cf-dc/2015/2015_002_0605_e.asp>.

[107] Office of the Privacy Commissioner of Canada, "PIPEDA Case Summary #2008-394: Outsourcing of Canada.com E-mail Services to U.S.-based Firm Raises Questions for Subscribers" (OPC, 19 September 2008), online: <https://www.priv.gc.ca/cf-dc/2008/394_20080807_e.asp>.

[108] Office of the Privacy Commissioner of Canada, "PIPEDA Case Summary #2005-313: Bank's Notification to Customers Triggers *Patriot Act* Concerns" (OPC, 19 October 2005), online: <https://www.priv.gc.ca/cf-dc/2005/313_20051019_e.asp>.

In some provinces, governments do have a say whether extra-jurisdictional transfer is acceptable. This is limited to PHI held by public bodies in British Columbia, Nova Scotia, and Alberta. In British Columbia and Nova Scotia, PHI held by public bodies cannot be transferred across borders without the individual's consent or ministerial approval.[110] Alberta's *FIPPA* and *HIA* do not directly restrict transfers, but do make it an offence to answer to compelled disclosures not authorized by Alberta law.[111] Under the accountability principle, would this not effectively prohibit extra-territorial PHI transfer by public bodies or health custodians altogether?

With the Edward Snowden revelations[112] and the European Court of Justice's decision invalidating the EU-U.S. Safe Harbour Agreement due to mass government surveillance with limited judicial remedy,[113] the spotlight is currently on international data transfer. Despite being in a similar position to Europe, as Canada is "a leading consumer but laggard in service provision",[114] Canadian policy debate is surprisingly silent on cross-border issues. Once again, rules and guidance for when custodians can transfer PHI abroad are needed, and contractual requirements can also help mitigate unjustified intrusions of Canadians' privacy under foreign law.

(c) Meeting Transparency Obligations through Specific Contractual Requirements

How does the cloud impact the realization the Fair Information Practice principle of openness? This principle is an important reference for custodians assessing whether a cloud contract offers comparable protection. The custodian's duty of openness, in particular, is threatened in the cloud.

---

[109] Quebec's *PPIPS*, *supra* note 36, s. 8(3).

[110] *Personal Information International Disclosure Protection Act*, S.N.S. 2006, c. 3, s. 5(1); *Freedom of Information and Protection of Privacy Act*, R.S.B.C. 1996, c. 165, s. 33.2 (in 2014, however, the Information & Privacy Commissioner of British Columbia issued updated guidance allowing public bodies to store data outside the jurisdiction when a technique called tokenization is appropriately employed, the implication being that this approach complies with the law because tokenization pseudonymizes the portion of personal data that is stored outside of the province. See Office of the Information & Privacy Commissioner for British Columbia, "Updated Guidance on the Storage of Information Outside of Canada by Public Bodies" (Victoria: OIPCBC, 16 June 2014), online: < oipc.bc.ca/public-comments/1649 > .

[111] *Freedom of Information and Protection of Privacy Act*, R.S.A. 2000, c. F-25, s. 92(3); Alberta's *HIA*, *supra* note 5, s. 107(5.1); see also Power, *supra* note 4 at 7.22—7.23.

[112] See generally Edward J. Snowden, "The World Says No to Surveillance," Editorial, *The New York Times* (4 June 2015), online: < www.nytimes.com > .

[113] *Schrems*, *supra* note 3.

[114] EC, European Data Protection Supervisor, *Opinion 4/2015: Towards a New Digital Ethics: Data, Dignity and Technology* (Brussels: EDPS, 2015), online: < https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-09-11_Data_Ethics_EN.pdf > .

Custodians are required to make specific information about PHI management policies and practices "readily available" to individuals in an understandable form.[115] How should this duty extend to the CSP? Custodians cannot be open with individuals about data handling practices unless information about the CSP's privacy and security practices is readily available to the custodian. Indeed, custodians should be able to "confirm what happens to [PHI] after it is provided to a third-party service provider".[116] But CSPs may believe that openness comes at the cost of security, as it gives insight into security mechanisms to potential attackers. Information security experts insist that to achieve "security through obscurity" in this way is undesirable and ineffective.[117] Custodians also need to know about subcontracting practices and ensure subcontractors adhere to the conditions in the cloud contract. Ideally, the custodian should be asked to consent to subcontracting or should at least be notified in a timely fashion.[118] Specific information about subcontractors could include the names, locations, and accountability measures in place.[119] If public disclosure of subcontracting practices creates a security risk, disclosure could be made to the custodian in a general manner or under a non-disclosure agreement.

Breach notification requirements were raised under the 2013 OECD Data Protection Guidelines, and recently incorporated into *PIPEDA*.[120] They typically require custodians to notify individuals or privacy authorities (or service providers to notify custodians) of a breach that may adversely affect individuals.[121] The purposes of these requirements are to increase openness of an organization's information handling practices, support individuals' right to informational self-determination, strengthen best practices, and improve the general public's awareness of the gravity and scale of breaches.[122] Breach notification is currently required in four Canadian jurisdictions.[123]

---

[115] See e.g., *PIPEDA*, *supra* note 36, Schedule 1, 4.8, 4.8.2.

[116] Office of the Privacy Commissioner of Canada, "Legal Information Related to PIPEDA: Interpretation Bulletin" (OPC, 2012), online: < https://www.priv.gc.ca/leg_c/interpretations_02_acc_e.asp > .

[117] See e.g., Peter P. Swire, "A Model for When Disclosure Helps Security: What Is Different about Computer and Network Security?" (2004) 3:1 J. Telecommunications & High Technology L. 163 at 183.

[118] International Organization for Standardization, "ISO/IEC 27018:2014: Information Technology—Security Techniques—Code of Practice for Protection of Personally Identifiable Information (PII) in Public Clouds Acting as PII Processors" (ISO, 2014) at A7, online: < www.iso.org/iso/catalogue_detail.htm?csnumber = 61498 > [ISO, "IEC 27018"]; EC, *Opinion 05/2012*, *supra* note 51 at 3.4.1.1.

[119] EC, *Opinion 05/2012*, *supra* note 51 at 3.4.1.1.

[120] OECD, *2013 Guidelines*, *supra* note 92 at 26; see also requirements established under the *Digital Privacy Act*, S.C. 2015, c. 32, s. 10, which has received royal assent, and will come into force with regulations, online < https://openparliament.ca/bills/41-2/S-4/ > .

[121] OECD, *2013 Guidelines*, *supra* note 92 at 27.

[122] Kenneth A. Bamberger & Deirdre K. Mulligan, "Privacy on the Books and on the Ground" (2011) 63:2 Stan. L. Rev. 247 at 275—276.

- Ontario's *PHIPA* requires that a custodian notify an individual at the first reasonable opportunity if PHI is stolen, lost, or accessed without authorization.[124] In addition, an agent must notify a custodian of a breach.[125]
- Alberta's *PIPA* requires that a custodian notify the Alberta Privacy Commissioner where there is a real risk of significant harm, without unreasonable delay.[126]
- Newfoundland's *PHIA* requires reporting of a "material" breach to privacy authorities.[127]
- In British Columbia, breach notification of authorities is not required, but is encouraged.[128]

Attention also needs to be given to who will determine if a breach is "material." Where custodians have breach notification obligations, accountability dictates that these obligations and the specific conditions which trigger them are clearly articulated in cloud contracts.

V. GAPS IN PRIVACY PROTECTION IN CLOUD CONTRACTS

To support our legislative analysis, we also reviewed the current contractual practices of six CSPs of various sizes based in the U.S., Canada and the EU. Because some of these contracts were acquired during confidential negotiations, we have omitted the names of the CSPs.

We have identified a number of gaps in the privacy protection provided by their Terms of Service. Our review addressed five questions:

1. What restrictions exist on international data transfer?
2. Which law(s) apply to PHI in clouds?
3. Who is responsible for PHI in clouds?
4. What is regulated as PHI in clouds?
5. What privacy protection is currently provided?

We have made recommendations elsewhere about how these gaps can be addressed by the contracting parties.[129] However, given the imbalance of

---

[123] Ontario's *PHIPA*, *supra* note 5, s. 12; Alberta's *PIPA*, *supra* note 49, s. 37.1; Newfoundland's *PHIA*, *supra* note 5, s. 15; New Brunswick's *PHIPA*, *supra* note 5, s. 49.

[124] Ontario's *PHIPA*, *supra* note 5, s. 12.

[125] *Ibid*, s. 17(3).

[126] Alberta's *PIPA*, *supra* note 49, s. 34.1.

[127] Newfoundland's *PHIA*, *supra* note 5, s. 15(4).

[128] Power, *supra* note 4 at 6.25.

[129] For a comprehensive list of policy and contractual recommendations see Adrian Thorogood et al, "Policy Brief: Protecting Privacy in Cloud-Based Genomic Research" (Centre of Genomics and Policy, 2015), online: <www.genomicsandpolicy.org/Ressources/20150729_PolicyBrief.pdf>.

bargaining power in favour of large CSPs with respect to all but the largest of their clients, and CSPs' preference for standard form contracts, at least some of these gaps can only be addressed top-down through regulation.

(a) What Privacy Protection is Currently Provided?

Multiple providers cited secure sockets layer (SSL) encryption as their protection mechanism of choice, but this bears only on data in transit, not data at rest, and is thus generally insufficient. While several organizations have promoted the establishment of cloud privacy standards,[130] these were not referenced by the Terms of Service we reviewed. Other than the legislatively driven U.S. HIPAA Business Associate Agreement requirements, the vast majority of protections referenced in the various CSP Terms of Service are industry driven, and none are Canadian per se.[131] No CSPs made contractual commitments to meet or maintain these standards.

(b) What is Regulated as PHI in Clouds?

Four of six providers did not include custodian's data in their definition of personal information. In effect, these CSPs do not acknowledge that they are processors of personal information on behalf of the custodian. Would these contracts meet the minimum contractual requirement for service contracts to limit use to authorized purposes? One might infer that the decision not to include custodian content in the definition of personal information may be tied to the type of service being provided. For example, access to researcher content differs between CSPs providing SaaS and IaaS, the latter of which is more often used by researchers and largely the focus of the cloud implementations addressed in this article. In the former, the CSP would necessarily be actively involved in the data management, whereas in the latter, the provider may have no role whatsoever. An analogy for IaaS may be that of a storage locker. The entity renting out the locker does not maintain control over the content of the locker. Similarly, in IaaS, the CSP, in effect, provides a virtual box in which custodians may store their content. The CSP would not actively engage with such contents (at least not by design) and would therefore not be able to, for example, encrypt the contents. This may be the logic behind why providers do not include obligations to protect PHI.

---

[130] See e.g., EC, Cloud Select Industry Group on Service Level Agreements, online: < https://ec.europa.eu/digital-agenda/en/cloud-select-industry-group-service-level-agreements > ; ISO, "IEC 27018", *supra* note 118.

[131] BSA Software Alliance, "2013 BSA Global Cloud Computing Scorecard: Country: Canada" (2013) at 2, online: < cloudscorecard.bsa.org/2013/assets/PDFs/country_reports/Country_Report_Canada.pdf > : "Canada has not yet issued any formal guidelines, standards, or regulations regarding cloud computing security. However, Canadian organizations may be influenced by relevant standards being developed by the National Institute of Standards and Technology (NIST) in the United States."

However, just as the entity renting out the storage locker may prevent the owner from accessing it, or may maintain a master key to access its contents, so too does the CSP have a super user account enabling the CSP to stop and start access, and possibly to read or modify the data. Some CSP personnel may also have such access even where it is relegated to those on a "need-to-know" basis. This weakens the argument that the CSP is not processing PHI. For health custodians, the primary concern is individuals' PHI placed in the cloud. Indeed, in research, the efficient analysis of vast datasets of individual data is the main driver behind seeking a cloud-based solution. For this reason, a definition of PHI that does not include custodian data presents a significant gap in the approach to its regulation and, ultimately, its protection.

(c) Who is Responsible for PHI in Clouds?

All the CSPs reviewed limit their privacy obligations to PHI they collect about their clients, excluding PHI contained within client data. This leaves the custodian solely responsible for PHI in the cloud. Again, this presents a pronounced risk to privacy, especially where the custodian stores large genomic datasets. Researchers, as custodians, are accountable for participant PHI throughout the data lifecycle. Custodian obligations ought to extend to CSPs—both obligations to safeguard PHI and obligations arising where such safeguards fail, including breach notification, indemnification, and acceptance of liability for damages caused by the CSP's negligence or misconduct. Again, the role of the CSP will differ depending on the service model. However, absent appropriate contractual provisions requiring specific safeguards, addressing breach notification, and recognizing CSP liability, it is unclear whether custodians can ensure that participant privacy is adequately protected in the cloud.

(d) Which Law(s) Apply to PHI in Clouds?

Extraterritoriality and enforceability have always been challenges in the online world. Some of the earliest cases coincided with the growth of the modern Internet dating back to the mid-'90s.[132] But while the early days saw an Internet that connected two points with a largely passive network in between such points, cloud computing enables processing in multiple locations. In such cases there may be several legal systems with potential relevance to the contract. Today, it is much easier to argue that any law may apply, provided it is connected to the activity of interest.[133] In the cloud, potentially any node found along the path of a given computation or transmission may also provide enough of a connection to

---

[132] See e.g., *Inset Systems Inc. v. Instruction Set, Inc.*, 937 F.Supp. 161 (D. Conn., 1996); *Bensusan Restaurant Corp. v. King*, 937 F.Supp. 295 (S.D. N.Y. ,1996), and perhaps most notably, *Zippo Manufacturing Co. v. Zippo Dot Com, Inc.*, 952 F.Supp. 1119 (U.S. W.D. Pa., 1997).

[133] See *Society of Composers, Authors Music Publishers of Canada v. Canadian Assn. of Internet Providers*, 2004 CSC 45, 2004 SCC 45, 2004 CarswellNat 1919, 2004

assert jurisdiction. While there is good reason for the parties to contractually submit to the jurisdiction of the CSP, good argument can also be made that the law of the custodian's or individuals' jurisdiction should apply. Where this cannot be done, accountability requires that the custodian consider if additional duties derived from local laws need to be imposed through contract.

(e) What Restrictions Exist on International Data Transfer?

The issues raised by international data transfer are not dissimilar to those of application of law. The problem with international data transfer is that, as mentioned earlier, where a site has a connection to the data, the application of that site's law may follow. In other words, if the researcher's data is moved from a data centre in Canada to one in the U.S., U.S. law may apply. In addition to lack of certainty around the applicable law, data might be subject to law enforcement requests from agencies in other jurisdictions. These issues are exacerbated further where there is no notice requirement by the CSP either in advance of an international transfer, or in advance of a request by law enforcement for access to the data.

Elsewhere we have provided best practice recommendations for contracting in the cloud, and have created a checklist for cloud contracting for genomic researchers.[134] These resources can help healthcare providers, researchers, and CSPs alike ensure the privacy of Canadians is protected in the cloud. Legal reform also will be necessary to promote privacy in the cloud, and, as we argue in the next section, must be carried out in a harmonized manner.

VI. DISCREPANCIES ACROSS PROVINCES AFFECTING INTEROPERABILITY OF CLOUD CONTRACTS

This section identifies discrepancies between Canadian laws applying to PHI. Such discrepancies create confusion over already vague standards and raise doubts about the interoperability of cloud contracts across provinces. The cloud business model underlying scalability and cost effectiveness relies on standard service offerings framed by standard form contracts. Even where arguably technical, these discrepancies make it difficult to be sure that a given cloud contract is legally compliant across provinces. Uncertainty over compliance, especially given the small size of some provincial health sectors, may discourage companies from crafting Canadian-specific contracts. They are more likely to espouse a "take it or leave it" approach (such as "HIPAA" compliant services in Canada). Such an approach imposes a heavy burden of compliance assessment on custodians, who remain accountable for PHI transferred to the cloud.

CarswellNat 1920, REJB 2004-66511, (*sub nom. Socan v. Canadian Assn. of Internet Providers*) [2004] 2 S.C.R. 427, [2004] S.C.J. No. 44 (S.C.C.).

[134] Thorogood et al, *supra* note 129; Centre of Genomics and Policy, "Annex 1: Contract Checklist for Cloud-Based Genomic Research" (Centre of Genomics and Policy, 2015), online: < www.genomicsandpolicy.org/Ressources/20150728_Annex1.pdf > .

(a) Definition of "Identifiable"

It is increasingly uncertain when information, particularly health information, is considered "identifiable" and thus governed by privacy laws.[135] This uncertainty is of great concern to the research community, which has traditionally relied heavily on de-identification, thereby avoiding the application of privacy laws. Uncertainty over de-identification is particularly acute in genetics because every individual has a unique genetic make-up. The genome is akin to a bar code, a unique tracing tag for an individual. Researchers have demonstrated that it is technically possible to detect an individual's presence within pooled genotype data, such as the aggregated results of genomic studies.[136] Concerns have centred on the risk of re-identification from de-identified genetic databases or study results. It is feared that an individual will be identified within a dataset, and that potentially sensitive health information about that individual will be revealed. What is "identifiable" is also a moving target:

> 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.[137]

In the cloud, encryption and access controls further complicate the legal determination of whether information is identifiable.[138]

To complicate the matter, the legal definition of "identifiable" varies between Canadian provinces. Some do not define the term or define it in a circular manner (e.g., "[i]nformation about an identifiable individual"). Others consider information to be "identifiable" if it "allows identification," if identity is "readily ascertainable," or if identification is "reasonably foreseeable."[139] Still others

---

[135] Paul M. Schwartz, "Information Privacy in the Cloud" (2013) 161:6 U. Pa. L. Rev. 1623; Paul M. Schwartz & Daniel J Solove, "Reconciling Personal Information in the United States and European Union" (2014) 102:4 Cal. L. Rev. 877; Paul Ohm, "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization" (2010) 57:6 UCLA L. Rev. 1701.

[136] Nils Homer et al, "Resolving Individuals Contributing Trace Amounts of DNA to Highly Complex Mixtures Using HighDensity SNP Genotyping Microarrays," online: (2008) 4:8 PLoS Genetics e1000167 <journals.plos.org/plosgenetics/article?id = 10.1371/journal.pgen.1000167>. See also Anne S.Y. Cheung, "Re-Personalizing Personal Data in the Cloud" in Anne S.Y. Cheung & Rolf H Weber, eds, *Privacy and Legal Issues in Cloud Computing* (Northampton, MA: Edward Elgar, 2015) 69 at 70.

[137] Patricia Kosseim & Megan Brady, "Policy by Procrastination: Secondary Use of Electronic Health Records for Health Research Purposes" (2008) 2:1 McGill J.L. & Health 5 at 28.

[138] W, Kuan Hon, Christopher Millard & Ian Walden, "The Problem of 'Personal Data' in Cloud Computing: What Information Is Regulated?—the Cloud of Unknowing." (2011) 1:4 Intl Data Privacy L. 211.

explicitly include indirect identifiers (those that need to be combined with other information to identify an individual) in the definition. Some statutes define and specifically exempt "de-identified" information from the definition of identifiable, even though by definition it is information that has been rendered non-identifiable.[140] As a particularly confusing example, article 1 of Prince Edward Island's *HIA* defines "identifying" by one legal standard (reasonably foreseeable), and "de-identified" by another (identity cannot be "readily ascertained").

Canadian health researchers must contend with yet more definitions. The Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans (*TCPS*),[141] applies only to research on human subjects. This definition includes research involving personally identifiable information. However, the *TCPS* goes on to discuss privacy risks along a spectrum from identifiable to coded to anonymized to anonymous, and requires researchers to employ safeguards proportionate to the risk of re-identification.[142] The *TCPS* definitions of coded and anonymized (respectively, the reversible/irreversible removal of direct identifiers) differs from the definition of de-identified in Canadian health sector laws (i.e., information rendered non-identifiable). Coding and anonymization are essential technical safeguards for privacy in research, but applying these processes does not necessarily resolve the question of whether the *TCPS* continues to apply.[143] Other questions remain unanswered: does "identifiability" depend on who can (or could foreseeably) access the information? Consider the case where identifiers are removed from genetic information and replaced with a code. The genetic information remains identifiable to the researcher with the code, but may not be identifiable for a researcher with only the coded information.[144]

An emerging approach recognizing the limits of de-identification is to simply prohibit re-identification. This strategy could be adopted by custodians for cloud contracts (or even by Canadian legislators). *HIPAA* requires that researchers accessing information that is de-identified under a Safe Harbour exception commit data custodians to "[n]ot identify the information or contact the individuals".[145] A U.S. Federal Trade Commission Report on consumer privacy

---

[139] See Appendix 1, below.

[140] See Council of Canadian Academies, *supra* note 49; Saskatchewan's *HIPA*, *supra* note 36, s. 3(2); Manitoba's *PHIA*, *supra* note 36, s. 3; New Brunswick's *PHIPA*, *supra* note 5, s. 3(2)(a); Nova Scotia's *PHIA*, *supra* note 36, s. 5(2)(a).

[141] *TCPS*, *supra* note 4.

[142] *Ibid* at 5A.

[143] Bartha M. Knoppers et al, "Questioning the Limits of Genomic Privacy," Letter to the Editor, (2012) 91:3 American J. Human Genetics 577.

[144] This distinction was recognized in Office of the Privacy Commissioner of Canada, "PIPEDA Case Summary #2009-018: Psychologist's Anonymized Peer Review Notes are the Personal Information of the Patient" (OPC, 18 June 2010), online: <https://www.priv.gc.ca/cf-dc/2009/2009_018_0223_e.asp>.

proposes that commercial data be excluded if "the company commits publicly not to re-identify it and, further, ensures through contractual or other mechanisms that downstream users keep the data in a de-identified form."[146] New Zealand is considering explicitly prohibiting re-identifying data.[147] The Global Alliance for Genomics and Health, an international coalition of individuals and institutions implicated in genomic medicine and research, stipulates in its *Responsible Data Sharing Framework* that its members should not attempt to re-identify participants in genomic research with de-identified data.[148]

Court decisions and OPC interpretations offer some guidance as to what is identifiable information.[149] But it is unclear if this guidance applies across all statutes. We concur therefore with the findings of an expert task force that has recommended "a consistent national approach to what kinds of information should be removed from health data to make [it] de-identifiable" under Canadian law.[150]

(b) Duty of Confidentiality

All provinces require that custodians protect the confidentiality of PHI through security measures, but the specificity of these requirements varies. As cloud contracts must ensure comparable protection, it would follow that the CSP is bound to respect such requirements, even detailed ones. These duties should also be passed on by the CSP to subcontractors, agents, and employees, and should survive the termination of contracts.[151] In most provinces, statutes applying to PHI provide a briefly worded standard of confidentiality. Quebec's *PPIPS*, for example, requires that security measures be taken throughout the

---

[145] *HIPAA Privacy Rule*, *supra* note 46, § 164.514(e).

[146] Gehan Gunasekara, "Paddling in Unison or just Paddling? International Trends in Reforming Information Privacy Law" (2014) 22:2 Intl. J.L. & I.T. 141 at 151; US, Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (Federal Trade Commission, 2012) at 22, online: < https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf > .

[147] NZ, New Zealand Data Futures Forum, "Harnessing the Economic and Social Power of Data" at 21—22, online: < https://www.nzdatafutures.org.nz/sites/default/files/NZDFF_harness-the-power.pdf > .

[148] Global Alliance for Genomics and Health, *Framework for Responsible Sharing of Genomic and Health-Related Data* (2014) at 5, online: < https://genomicsandhealth.org/files/public/Framework%20for%20Responsible%20Sharing%20of%20Genomic%20and%20Health-Related%20Data%20-%20Version%2010%20September%202014.pdf > .

[149] See e.g., Office of the Privacy Commissioner of Canada, "Legal Information Related to PIPEDA: Interpretation Bulletin" (OPC, 2015), online: < https://www.priv.gc.ca/leg_c/interpretations_02_e.asp > .

[150] Council of Canadian Academies, *supra* note 49 at 207.

[151] ISO, "IEC 27018," *supra* note 118 at A10.1.

lifecycle of PHI that "are reasonable given the sensitivity of the information, the purposes for which it is to be used, the quantity and distribution of the information and the medium on which it is stored."[152] In Alberta, regulations impose extensive duties of confidentiality on a health sector custodian. The custodian must establish a written record of all administrative, technical, and physical safeguards; designate a security officer; and periodically assess the safeguards.[153] A cloud contract for the Canadian health sector would need to comply with the security requirements of the strictest province.

(c) Definition of Service Provider

Not all Canadian privacy laws explicitly define who or what constitutes a service provider, and different terms are used by those that do. *PIPEDA* does not define the term, but mentions "transfer[s] to . . . third part[ies] for processing" when discussing accountability.[154] All Canadian health information statutes define or refer to "agent[s]"[155] or "affiliate[s]"[156] These terms are defined broadly to capture any third party that acts on behalf of a custodian for the purposes of the custodian,[157] and in most cases includes employees.[158] Agents are expressly permitted to process PHI on behalf of the custodian.[159] Canadian health privacy laws also define service provider. An "information manager"[160] or "information management service provider"[161] is an entity that processes PHI for or provides information management or information technology services to a custodian. Information managers are typically treated as a subset of agent, and are thereby also permitted to receive and process PHI.

A number of health privacy laws distinguish between employees and service providers in order to impose stricter contractual requirements on the latter. Ontario's *PHIPA* regulations refer to "a person who supplies services for the purpose of enabling a health information custodian to use electronic means to collect, use, modify, disclose, retain or dispose of personal health information, and who is not an agent of the custodian."[162] The stricter contractual

---

[152] Quebec's *PPIPS*, *supra* note 36, s. 10; see also Ontario's *PHIPA*, *supra* note 5, s. 12(1).

[153] Alberta's *HIA*, *supra* note 5, *Health Information Regulations*, Alta. Reg. 70/2001, s. 8(1) [Alberta's *HIA Regs*].

[154] *PIPEDA*, *supra* note 36, Schedule 1, 4.1.3.

[155] New Brunswick's *PHIPA*, *supra* note 5, s. 1; Newfoundland's *PHIA*, *supra* note 5, s. 2(1)(a); Ontario's *PHIPA*, *supra* note 5, s. 2; Nova Scotia's *PHIA*, *supra* note 36, s. 3(a); Prince Edward Island's *HIA*, *supra* note 36, s. 1(a).

[156] Alberta's *HIA*, *supra* note 5, s. 1(1)(a); Saskatchewan's *HIPA*, *supra* note 36, s. 2(a).

[157] See e.g., Ontario's *PHIPA*, *supra* note 5, s. 2; Power, *supra* note 4 at 5.15.

[158] *Cf* Manitoba's *PHIA*, *supra* note 36.

[159] Ontario's *PHIPA*, *supra* note 5, s. 17.

[160] Alberta's *HIA*, *supra* note 5, s. 66(1); Manitoba's *PHIA*, *supra* note 36, s. 1(1); New Brunswick's *PHIPA*, *supra* note 5, s. 1; Newfoundland's *PHIA*, *supra* note 5, s. 2(1)(l).

[161] Saskatchewan's *HIPA*, *supra* note 36, s. 2(j).

requirements imposed on service providers are discussed below. Ontario's *PHIPA* also defines an even more specific category: "health information network provider" (HINP). A HINP is:

> a person who provides services to two or more health information custodians where the services are provided primarily to custodians to enable the custodians to use electronic means to disclose personal health information to one another, whether or not the person is an agent of any of the custodians.

HINPs are subject to even more detailed contractual requirements, described below.[163]

In Ontario, CSPs dealing with PHI would attract the stricter contractual requirements of service provider and potentially, depending on the primary purpose of the service, also those of HINPs. The existence of a separate regime for HINPs, distinguished based on the networking service they provide, raises the question of whether CSPs, or CSPs providing certain types of services, could be similarly distinguished.

(d) Required Clauses in Service Provider Contracts

Cloud contracts are key to accountability and compliance. If custodians lack sufficient bargaining power to impose comparable protection through negotiation, however, they will be forced to choose between noncompliance and forgoing the cloud. To relieve custodians of this dilemma, Canadian policy makers should consider strengthening the statutory requirements for cloud contracts. Beyond the basic conditions of limited use and confidentiality required in outsourcing contracts, some Canadian health privacy statutes already require additional contractual clauses. In Ontario and Newfoundland, health privacy laws require that service providers ensure their privacy obligations are passed on to employees or subcontractors.[164] Alberta's law has exceptionally detailed conditions for an outsourcing agreement. An agreement must:

- identify the objective and principles of the agreement;
- identify permitted forms of processing;
- describe how access requests will be handled;
- describe how information will be protected;
- describe how information will be accessed; and
- describe how the agreement can be terminated.[165]

If the PHI leaves Alberta, the contract additionally must allow the custodian to monitor compliance and contain remedies for non-compliance.[166] Other provinces require the outsourcing agreement to comply with regulations, but

---

[162] Ontario's *PHIPA*, *supra* note 5, *General*, O. Reg. 329/04, s. 6(1) [Ontario's *PHIPA Regs*].

[163] *Ibid*, s. 6(2).

[164] *Ibid*, s. 6(1); Newfoundland's *PHIA*, *supra* note 5, s. 22(5).

[165] Alberta's *HIA Regs*, *supra* note 153, s. 7(2).

have failed to issue regulations.[167] These discrepancies seem a product of evolutionary drift as some jurisdictions update their laws more frequently than others, rather than purposeful design.

With the exception of HINPs, requirements for service provider contracts under Canadian health privacy laws are more formal than substantive: the contract must address certain issues, but there is no requirement as to how responsibility should be divided. Formal requirements work to promote transparency about how the parties will jointly address privacy, and in turn promote accountability. Indeed, having the CSP spell out the limits of its responsibility allows the custodian to better assess whether the CSP offers comparable protection. They also allow a flexible division of responsibilities. U.S. and EU laws, by contrast, have more extensive contractual requirements for service providers than Alberta or Ontario. Contracts must address the binding of employees and subcontractors, breach notification, notification of changes to law or compelled disclosure requests, prior consent for subcontracting, and even third party beneficiary clauses for data subjects.[168] Given that contractual requirements are an important means of ensuring accountability in the cloud, it is concerning that Canadian provinces, to varying extents, inadequately address this in their legislation.

Exceptionally, in Ontario, contracts between PHI custodians and HINPs must include a number of substantive obligations. HINPs are required to notify the custodian of unauthorized processing or a breach; make publicly available a plain language description of their services and safeguards appropriate for informing individuals; make publicly available directives, guidelines, or policies that apply to the HINPs (unless commercially sensitive); keep records of all access to PHI from the network and all transfers over the network; provide written privacy and security assessments; and bind subcontractors.[169] This distinct regime, applicable to services that primarily provide networking between two custodians, is unique under Canadian law. Could the HINP regime present a potential model for distinguishing a regime specific to CSPs? This direction is unlikely, considering the diversity of purposes for which CSPs are used. In addition, a cloud specific regime may fail to provide sufficient flexibility. In situations where a lesser degree of control over PHI is ceded to the CSP (e.g.,

---

166 *Ibid*, s. 8(4).

167 Saskatchewan's *HIPA*, *supra* note 36, s. 63(1)(j); Manitoba's *PHIA*, *supra* note 36, s. 25(3); Newfoundland's *PHIA*, *supra* note 5, s. 22(2); New Brunswick's *PHIPA*, *supra* note 5, s. 52(3).

168 *HIPAA Privacy Rule*, *supra* note 46 at § 164.504 (e)(2)(ii); The EU standard contractual clauses—for transfer to a processor in jurisdictions where the law has not explicitly been deemed adequate: EC, Directorate—General Justice, Commission Decision C(2010)593 Standard Contractual Clauses (processors) (EC, 2014), online: < ec.europa.eu/justice/data-protection/international-transfers/files/clauses_for_personal_data_transfer_processors_c2010-593.doc > .

169 Ontario's *PHIPA Regs*, *supra* note 162, s. 6(3).

IaaS), applying extensive substantive requirements on CSPs would be disproportionate and inappropriate.

(e) Accountability Standard

Privacy laws across Canada, "in one form or another, embody the principle that organizations are accountable for the [PHI] in their custody and control."[170] Under *PIPEDA*, the accountability standard for transfers to third parties is providing "a comparable level of protection" through contractual or other means.[171] British Columbia's *PIPA* simply states that "[a]n organization is responsible for personal information under its control, including personal information that is not in the custody of the organization."[172] A written agreement with an information manager under New Brunswick's *PHIPA* or Newfoundland's *PHIA* must simply "provide for" the protection of the PHI.[173] Quebec's *PPIPS* has the most stringent accountability standard, requiring custodians to take "all reasonable steps" to safeguard the privacy of personal information.[174] Is this variation merely terminological, or do custodians in some provinces have a heightened duty to assess the risks of transfers to third parties and foreign jurisdictions?[175]

(f) Transfer = "Use" or "Disclosure"?

Canadian privacy laws typically permit transfers to a service provider, where certain conditions are met, by characterizing such a transfer as a "use" rather than a "disclosure." This is strange, as the common meaning of transfer is more closely related to disclosure than to use. But this counter-intuitive characterization is needed to permit transfer where the custodian already has permission to use PHI for a given purpose. Treating transfer as a "use" also clarifies that the service provider is not a custodian in respect of the PHI: if there is no disclosure, there is no corresponding collection.[176] *PIPEDA* does not explicitly characterize a transfer to a service provider as a use, but this was done by OPC interpretive guidance.[177] Several health privacy laws clarify that a

---

[170] Kosseim, Kardash & Penta, *supra* note 35 at 210.

[171] *PIPEDA*, *supra* note 36, Schedule 1, 4.1.3.

[172] British Columbia's *PIPA*, *supra* note 49, s. 4(2).

[173] New Brunswick's *PHIPA*, *supra* note 5, s. 52.(3); Newfoundland's *PHIA*, *supra* note 5, s. 22(2).

[174] Quebec's *PPIPS*, *supra* note 36, s. 17.

[175] Eloïse Gratton, "Privacy Interviews with Experts" (Nymity, 2014), online: <https://www.nymity.com/~/media/Nymity/Files/Interviews/2014/2014-07-Gratton.pdf>.

[176] See e.g., Alberta's *HIA*, *supra* note 5, s. 66(7); Saskatchewan's *HIPA*, *supra* note 36, s. 18(5); Manitoba's *PHIA*, *supra* note 36, s. 25(5).

[177] Office of the Privacy Commissioner of Canada, "PIPEDA: Processing Personal Data Across Borders: Guidelines" (OPC, 2009), online: <https://www.priv.gc.ca/information/guide/2009/gl_dab_090127_e.pdf>.

transfer to an agent is a "use" not a "disclosure."[178] By contrast, Alberta's HIA does not classify transfer as a use or a disclosure, but rather as a *sui generis* transaction that does not require consent.[179] Counter-intuitive and discrepant classifications of "transfer" across provinces are confusing, and highlight that categories of processing underpinning Canadian privacy laws (collection, use, disclosure) are antiquated.

(g) Access for Health Research

Like service providers, Canadian privacy laws also permit transfers to researchers without individual consent under certain conditions. Several important variations between conditions across Canadian provinces have been canvassed in-depth by an expert panel of the Council of Canadian Academies.[180] Discrepancies include the type of body that must approve the research (e.g., ethics review board or privacy commissioner), situations where consent can be foregone (e.g., impracticable), and the contractual terms to be included in a custodian-researcher agreement. In data-centric sciences, such as genomics, the cloud is an attractive platform for providing access to research data across wide geographies. These discrepancies may concern researchers engaging CSPs to share research data across Canada.

(h) Summary

There are many discrepancies across Canadian privacy laws that apply to PHI. In many cases, these discrepancies are technical or terminological. In some cases, the discrepancies are substantive and indicate that privacy protections are weaker in some provinces. Requirements for custodian-service provider agreements are not detailed, except in Ontario and Alberta. Provincially applicable rulings and interpretations may exacerbate discrepancies in the black letter of provincial regulatory frameworks. Even where discrepancies are technical, they can create confusion. To give but one example, the European Commission's Article 29 Data Protection Working Party assessed *PIPEDA* as "adequate" for the purposes of transferring Europeans' personal data to commercial entities in Canada governed by that statute, but more recently reached a negative finding for Quebec's private sector law, even though it was deemed substantially similar by an Order-in-Council,[181] and arguably offers

---

[178] Nova Scotia's *PHIA*, *supra* note 36, s. 29(2); Ontario's *PHIPA*, *supra* note 5, s. 6(1); Ontario's *PHIPA Regs*, *supra* note 162, s. 6(4) (transfer to non-agent goods, service provider).

[179] Alberta's *HIA*, *supra* note 5, s. 66(3).

[180] Council of Canadian Academies, *supra* note 49.

[181] The Federal government declared Quebec's legislation substantially similar to *PIPEDA* in 2003. See Office of the Privacy Commissioner of Canada, "Legal information related to PIPEDA: Substantially Similar Provincial Legislation" (OPC, 2003), online: < https://www.priv.gc.ca/leg_c/legislation/leg-rp_030611_e.asp#provincial >. For discussion, see Jennifer Stoddart, Benny Chan & Yann Joly, "The European Union's

higher protection than *PIPEDA*.[182] To be cost-effective in the relatively small Canadian healthcare and health research market, CSPs need to develop standard contracts that are legally compliant across jurisdictions.

VII. CONCLUSION

This article has discussed three growing gaps in legal protection where accountability for PHI in the cloud is at risk. First, Canadian privacy and health privacy laws do not clarify how obligations are to be divided between custodians and CSPs. Second, the challenge of assessing the risks of cross-border transfers in Canada is largely left to custodians, who may not be well-equipped for the task. Third, CSP data handling and security practices are obscure, threatening the privacy principle of transparency. Moreover, our review of CSP Terms of Service revealed that these legislative gaps are not rectified by standard form cloud contracts typically on offer. Legislative intervention is therefore recommended to ensure cloud services are available to support genomic research and medicine in a manner that adequately protects the privacy of Canadian participants and patients. This may be achieved through more prescriptive legislation that establishes detailed requirements for contracts between custodians and service providers. In addition, appropriate (but not overly restrictive) conditions for cross-border transfers of PHI could also be considered.

Legislative efforts to protect privacy could also be reinforced by improved cloud contracting practices. We have provided detailed recommendations for custodians and for CSPs on how to improve cloud contracts elsewhere.[183] Briefly, custodians should ensure that cloud contracts include comprehensive technical, administrative, and physical safeguards clauses meeting industry standards and subject to periodic, independent audits.[184] Custodians should ensure that contractual obligations imposed on CSPs extend to their employees and subcontractors. The CSP should be bound to ensure the availability of service and the integrity of data during the full lifecycle of data processing. Adequate notice periods should be provided for suspension of or changes to services, such as the location of data storage. Finally, the CSP should assume liability for damages resulting from its own negligence or misconduct.

We also recommend that efforts to enhance legislative protections for privacy in the cloud be harmonized across jurisdictions. A host of discrepancies already exist between Canadian privacy laws, concerning:

Adequacy Approach to Privacy and International Data Sharing in Health Research" (2016) 44:1 The Journal of Law, Medicine & Ethics 143-155.

[182] Gratton, *supra* note 175: "Q: When is adequacy never adequate? A. When Québec's data protection law is considered 'inadequate' for Europe."

[183] See Thorogood et al, *supra* note 129, and Centre of Genomics and Policy, *supra* note 134.

[184] In the case of IaaS, audit may be largely limited to the physical premises of the CSP.

- When is data transferred to the cloud considered identifiable, and thus governed by privacy law?
- How exactly are CSPs defined?
- When is transfer of PHI to the cloud prohibited?
- What provisions must be included in a cloud contract?
- How can these contracts be monitored and enforced by custodians?
- And how can Canadian patients and research participants enforce their privacy rights in the cloud?

Without a harmonized effort, discrepancies may become more pronounced and privacy protections put more at risk.

It appears that the future of healthcare and health research will involve genomics, big data and, of course, cloud computing. In order to ensure privacy is not compromised, and to enhance transparency and accountability in the cloud, regulators should provide clear rules of engagement for custodians and CSPs.

Appendix 1: Table of Key Privacy Statutes in Canada

Canada (Federal)	*Privacy Act*, R.S.C. 1985, c. P-21. • *Privacy Regulations,* SOR/83-508. • *Privacy Act Extension Order, No. 1*, SOR/83-553. • *Privacy Act Extension Order, No. 2*, SOR/89-206. *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5. • *Regulations Specifying Publicly Available Information*, SOR/2001-7. • *Organizations in the Province of British Columbia Exemption Order*, SOR/2004-220. • *Organizations in the Province of Alberta Exemption Order*, SOR/2004-219. • *Health Information Custodians in the Province of Ontario Exemption Order*, SOR/2005-399. • *Organizations in the Province of Quebec Exemption Order*, SOR/2003-374. • *Personal Health Information Custodians in New Brunswick Exemption Order*, SOR/2011-265. • *Personal Health Information Custodians in Newfoundland and Labrador Exemption Order*, SI/2012-72.
British Columbia	*Personal Information Protection Act*, S.B.C. 2003, c. 63. • *Personal Information Protection Act Regulations*, B.C. Reg. 473/2003. *Freedom of Information and Protection of Privacy Act*, R.S.B.C. 1996, c. 165. • *Freedom of Information and Protection of Privacy*

	Regulation, B.C. Reg. 155/2012. *Privacy Act*, R.S.B.C. 1996, c. 373. *E-Health (Personal Health Information Access and Protection Act of Privacy) Act*, S.B.C. 2008, c. 38. • *Disclosure Directive Regulation*, B.C. Reg. 172/2009. • *E-Health Regulation*, B.C. Reg. 129/2011.
Alberta	*Personal Information Protection Act*, S.A. 2003, c. P-6.5. • *Personal Information Protection Act Regulation*, Alta. Reg. 366/2003. *Freedom of Information and Protection of Privacy Act*, R.S.A. 2000, c. F-25. • *Freedom of Information and Protection of Privacy Regulation*, Alta. Reg. 186/2008. • *Freedom of Information and Protection of Privacy (Ministerial) Regulation*, Alta. Reg. 56/2009. *Health Information Act*, R.S.A. 2000, c. H-5. • *Health Information Regulation*, Alta. Reg. 70/2001. • *Alberta Electronic Health Record Regulation*, Alta. Reg. 118/2010. • *Designation Regulation*, Alta. Reg. 69/2001.
Saskatchewan	*The Freedom of Information and Protection of Privacy Act*, S.S. 1990-91, c. F-22.01. • *The Freedom of Information and Protection of Privacy Regulations*, R.R.S., c. F-22.01, Reg. 1. *The Health Information Protection Act*, S.S. 1999, c. H-0.021. • *Health Information Protection Regulations*, R.R.S., c. H-0.021, Reg. 1. *The Local Authority Freedom of Information and Protection of Privacy Act*, S.S. 1990-91, c. L-27.1. • *Local Authority Freedom of Information and Protection of Privacy Regulations*, R.R.S., c. L-27.1, Reg. 1. *The Privacy Act*, R.S.S. 1978, c. P-24.
Manitoba	*The Freedom of Information and Protection of Privacy Act*, S.M. 2008, c. 40. • *Access and Privacy Regulation*, Man. Reg. 64/98. *The Personal Health Information Act*, S.M. 2013, c. 22. • *Personal Health Information Regulation*, Man. Reg. 245/97. *The Privacy Act*, C.C.S.M., c. P125. *The Personal Information Protection and Identity Theft Prevention Act*, S.M. 2013, c. 17.

Ontario	*Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c. F.31. • *General*, R.R.O. 1990, Reg. 460. • *Disposal of Personal Information*, R.R.O. 1990, Reg. 459. *Municipal Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c. M.56. • *General*, R.R.O. 1990, Reg. 823. *Personal Health Information Protection Act, 2004*, S.O. 2004, c. 3, Schedule A. • *General*, O. Reg. 329/04. *Quality of Care Information Protection Act, 2004*, S.O. 2004, c. 3, Schedule B. • *General*, O. Reg. 330/04. • *Definition of* "*Quality of Care Committee*," O. Reg. 297/04.
Quebec	*An Act respecting access to documents held by public bodies and the protection of personal information*, R.S.Q., c. A-2.1. • *Regulation respecting the distribution of information and the protection of personal information*, C.Q.L.R., c. A-2.1. • *Regulation respecting public bodies that must refuse to release or to confirm the existence of certain information*, C.Q.L.R., c. A-2.1. *An Act respecting the protection of personal information in the private sector*, R.S.Q., c. P-39.1. *An Act respecting health services and social services*, R.S.Q., c. S-4.2 • *Regulation respecting the information that institutions must provide to the Minister of Health and Social Services*, C.Q.L.R., c. S-4.2. *An Act respecting the sharing of certain health information*, R.S.Q., c. P-9.0001. • *Regulation respecting access authorizations and the duration of use of information held in a health information bank in a clinical domain*, C.Q.L.R., c. P-9.0001. *Civil Code of Québec*, S.Q. 1991, c. 64.. *Charter of Human Rights and Freedoms*, R.S.Q., c. C-12.
New Brunswick	*Right to Information and Protection of Privacy Act*, S.N.B. 2009, c. R-10.6. • *General Regulation*, N.B. Reg. 2010-111. *Personal Health Information Privacy and Access Act*, S.N.B. 2009, c. P-7.05. • *General Regulation*, N.B. Reg. 2010-112.

Prince Edward Island	*Freedom of Information and Protection of Privacy Act*, R.S.P.E.I 1988, c. F-15.01. • *General Regulations*, P.E.I. Reg. EC564/02. *Health Information Act*, S.P.E.I. 2014, c. 31 [not yet in force].
Nova Scotia	*Freedom of Information and Protection of Privacy Act*, S.N.S. 1993, c. 5. • *Freedom of Information and Protection of Privacy Regulations*, N.S. Reg. 105/94. *Municipal Government Act*, S.N.S. 1998, c. 18. *Personal Information International Disclosure Protection Act*, S.N.S. 2006, c. 3. • *Personal Information International Disclosure Protection Regulations*, N.S. Reg. 113/2008. *Personal Health Information Act*, S.N.S. 2010, c. 41. • *Personal Health Information Regulations*, N.S. Reg. 217/2012. *Privacy Review Officer Act*, S.N.S. 2008, c. 42.
Newfoundland & Labrador	*Access to Information and Protection of Privacy Act*, S.N.L. 2015, c. A-1.2. • *Access to Information and Protection of Privacy Regulations*, N.L.R. 11/07. *Personal Health Information Act*, S.N.L. 2008, c. P-7.01. • *Personal Health Information Regulations*, N.L.R. 38/11. *Privacy Act*, R.S.N. 1990, c. P-22. *Health Research Ethics Authority Act*, S.N.L. 2006, c. H-1.2. • *Health Research Ethics Authority Regulations*, N.L.R. 57/11.
Yukon	*Access to Information and Protection of Privacy Act*, R.S.Y. 2002, c. 1. • *Access to Information Regulation*, Y.O.I.C. 1996/053. *Health Information Privacy And Management Act*, S.Y. 2013, c. 16.
Northwest Territories	*Access to Information and Protection of Privacy Act*, S.N.W.T. 1994, c. 20. • *Access to Information and Protection of Privacy Regulations*, N.W.T. Reg. 206-96.
Nunavut	*Access to Information and Protection of Privacy Act*, S.Nu. 1994, c. 20. • *Access to Information and Protection of Privacy Regulations*, N.W.T. (Nu.) 206-96.