Background, Proceedings, and Outlook from the Canada-US Connected Health Workshop

Cross-Border Health Foundation

IN PARTNERSHIP WITH

HIMSS North America

PCHAlliance

About the authors

Dani Peters is the Co-Founder of Cross-Border Health and serves as an advisor. She has worked in health policy and government relations in Canada and the United States for over a decade. Prior to founding Magnet Strategy Group, Dani served in senior roles with two government relations consulting firms, one in Washington, D.C., and the other in Ottawa, Ontario. She serves on the business advisory board at Bloom Burton & Co., a healthcare investment advisory firm in Toronto, and a Health Scholar in Residence at the World Health Innovation Network, within the Odette School of Business at the University of Windsor.

Oliver Kim is the Co-Founder of Cross-Border Health. He has over fifteen years of health policy experience at the federal and state level. During his decade as a senior advisor to two U.S. Senators and the legislative director for one of the nation's largest safety-net providers, he worked on several critical initiatives such as the Affordable Care Act, the Medicare Modernization Act, and the American Revitalization and Recovery Act. He has spoken at international health conferences and was selected for the Woodrow Wilson foreign policy fellowship and an AcademyHealth health policy award.

Melanie Selvadurai is a Masters of Business Administration candidate at the DeGroote School of Business at McMaster University and is a senior intern at Healthcare Information and Management Systems and Society (HIMSS) Foundation's Institute for e-Health Policy, supporting Government Relations.

About Cross-Border Health

Cross-Border Health brings together government and stakeholders from Canada and the United States to discuss and act upon common priorities in health. Cross-Border Health promotes dialogue between health leaders in Canada and the United States, through targeted policy initiatives, informational exchanges and publications. Cross-Border Health is a 501(c)(3) non-profit organized under US law and based in the Washington, DC area.

About HIMSS North America

Healthcare Information Management Systems and Society (HIMSS) North America, a business unit within HIMSS, positively transforms health and healthcare through the best use of information technology in the United States and Canada. As a cause-based non-profit, HIMSS North America provides thought leadership, community building, professional development, public policy, and events. HIMSS North America represents 64,000 individual members, 640 corporate members, and over 450 non-profit organizations. Thousands of volunteers work with HIMSS to improve the quality, cost-effectiveness, access, and value of healthcare through IT.

About PCHAlliance

The Personal Connected Health Alliance (PCHAlliance) aims to make health and wellness an effortless part of daily life. The PCHAlliance, a non-profit organization formed by HIMSS, believes that health is personal and extends beyond healthcare. PCHAlliance mobilizes a coalition of stakeholders to realize the full potential of personal connected health. Members are a vibrant ecosystem of technology and life sciences industry icons and innovative, early stage companies, governments, academic institutions, and associations from around the world.

Acknowledgements

A special thanks to sponsors and partners of the Canada-US Connected Health Workshop:

Executive Summary

The Canada-US Connected Health Workshop, organized in conjunction with the Connected Health Conference in the Washington, DC metro area on December 14, 2016, assembled more than eighty participants from multiple disciplines and sectors in both countries to discuss regulatory and policy coordination in connected health. The term "connected health" is associated with a number of definitions, for the purposes of our event and paper, we define connected health as patient healthcare services enabled through digital health technologies delivered where the patient is located, when they need it, and in a manner that is conveniently available.[1]

This report summarizes the workshop discussions, while providing rationale and recommendations for greater cross-border cooperation in the regulation of digital health technology.

The workshop identified common interests and challenges surrounding the implementation of connected health technologies in both Canada and the United States.

	Regulatory systems must keep pace with rapid growth in connected health technologies.
	Telehealth is transforming traditional care delivery yet administrative barriers remain.
	The health supply chain provides an opportunity to connect Canada and the United States in ways that can improve patient safety and system efficiency.
	For issues such as privacy, there are regulatory and policy challenges due to intersections between federal and sub-national authorities and statutes.
	Achieving consistency in privacy rules across jurisdictions could accelerate innovation in digital healthcare.
	Interoperability remains a challenge for providers and policymakers and is a necessary goal to make health data useful.
	Using health information and data analytics can help achieve public health goals and improve chronic care management.

Recommendations from the Canada-US Connected Health Workshop are focused on Canada-US regulatory and policy coordination in connected health. The report's recommendations are based on the workshop's discussions and subsequent consultation with speakers, audience members, and other subject matter experts.

SUMMARY OF WORKSHOP RECOMMENDATIONS

Topic	Recommendation	Rationale
Canada-US alignment on health data privacy protection	Establish a Canada-US Health Privacy and Security Forum	Promote knowledge exchange, regulatory consistency and help establish a common front on health privacy protection in a digital age
Regulatory harmonization in health information technology/digital health	Add health information technology topics to future work plans under the Regulatory Cooperation Council	Ensure Canada and the US work collaboratively to harness the potential of new technology, while also striking a balance with safety and security concerns
Governance in storage, handling, and sharing health records for research purposes	Pursue Canada-US Memorandum of Understanding to govern the storage, handling, and sharing of data for the purposes of research	Great potential for Canada and the US to collaborate and combine datasets while establishing a common understanding of the use of digital health records for research

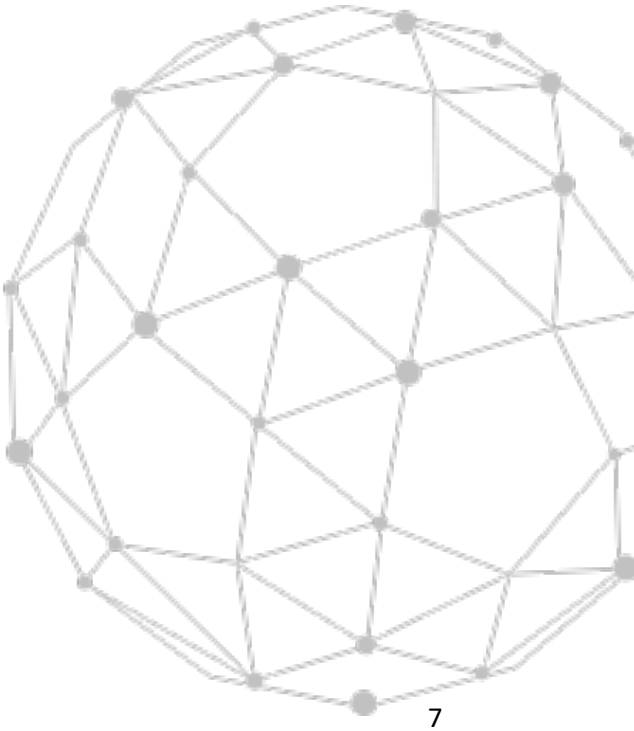
Introduction

The Canada-US relationship is one that is unique in the world, based on deep economic and cultural ties, common values, and a peaceful border. Our close bilateral ties contribute to information sharing and policy coordination between federal, state, and provincial officials on a daily basis. Although Canada and the US have a long history of working collaboratively on a wide range of policy issues, health is often neglected because the two countries' systems are perceived to be entirely different from one another. While our systems may seem dissimilar on the surface, many of the challenges associated with delivering better health are the same. Cross-border health priorities—ranging from health privacy and data utilization discussed in this paper but also areas outside the scope of this paper such as food safety, public health preparedness, and counterfeit medicines—are significant given the permeable Canada-US border.

What is Connected Health?

We define connected health as patient healthcare services enabled through digital health technologies delivered where the patient is located, when they need it, and in a manner that is conveniently available.[2] In the ideal connected health system, the delivery of healthcare services is not limited by time or distance between a provider and the patient. But to achieve this ideal, connected health requires novel privacy and security solutions to address barriers to adoption and patient scepticism about how their information will be handled.[3] The 2016 Canada-US Connected Health Workshop was both timely and pertinent to the rapid evolution of connected health systems in both Canada and United States. The continued evolution expected in these systems will require a better policy and regulatory coordination to enable secure data sharing among interoperable partners within and across borders.

While our systems may seem dissimilar on the surface, many of the challenges associated with delivering better health are the same.



I. An Overview of Current Policies and Laws in Canada and the United States

American Health Privacy Laws and Regulation

In the United States, federal law provides the foundation for the privacy and handling of health information. States may impose their own health privacy and confidentiality laws beyond federal law, and these laws vary from state to state.

The security and privacy of health data is governed mainly by two federal laws. Under the Health Insurance Portability and Accountability Act (HIPAA),[4] the Department of Health and Human Services (HHS) promulgated two major rules on the privacy and security of health data: the Privacy Rule regulates when "covered entities"[5] and "business associates"[6] can disclose "personal health information" (PHI),[7] and the Security Rule regulates how covered entities secure such data.[8] Covered entities include health plans, healthcare clearinghouses, and healthcare providers that transmit health information in electronic form.[9] HIPAA also applies to a covered entity's business associates, individuals, or businesses that help the covered entity perform certain functions or activities that require the use or disclosure of PHI.[10] PHI can include names, medical record numbers, social security numbers, and medical record information.[11]

The second major federal law, the Health Information Technology for Clinical and Economic Health Act (HITECH), subsequently modified federal privacy rules, while simultaneously encouraging greater data sharing through an investment in Electronic Health Records (EHRs).[12] Through meaningful-use requirements, the federal government encourages health providers eligible for incentives to share health data not only among other eligible providers but also public health agencies and other providers that are ineligible for incentives.[13] Such data sharing should improve public health, clinical research, and payment and delivery reforms.[14]

To balance individual privacy with this explicit encouragement to share health data, HITECH authorized HHS to enact several new privacy protections. First, HITECH expands the definition of a business associate[15] and clarifies that business associates must comply with both HIPAA regulations on data security[16] and the new HITECH privacy protections.[17] Further, business associates can be held liable for their failure to comply with the Privacy Rule.[18] Second, HITECH requires individuals to be notified of breaches, or the impermissible disclosure or use of protected health information, by a covered entity or its

business associates.[19] Third, HITECH also gives individuals more control over their health information by improving their right to see who has obtained copies of their records, as well as requiring them to be notified in the event of a data breach.[20] In addition, the HIPAA Omnibus Rule implemented a number of provisions of the HITECH Act and permits updates to HIPAA privacy, security and breach notification rules.[21]

The federal Privacy Rule sets a national floor for healthcare privacy and pre-empts state laws that are less protective, meaning states can only mirror or enact more stringent protections than federal law.[22] State laws generally touch on types of health information, the source of the data, and restrictions of the disclosure and use of data.[23]

Canadian Health Privacy Laws and Regulations

In Canada, health information protection laws primarily fall under provincial jurisdiction. Health information protection laws in the provinces of Ontario, New Brunswick, Newfoundland and Labrador, Nova Scotia, Alberta, Saskatchewan, and Manitoba cover the collection, use, and disclosure of personal health information by health care providers, known as data custodians or trustees. Data storage and system management providers can also be subject to health information protection laws.

Under provincial statutes, patients are granted access to their personal health information, while disclosure without a patient's consent is prohibited.[24] Provincial health privacy laws limit data custodians' use of health information within their organizations and prohibit disclosure of health information for purposes without patient consent.

At the federal level, the Personal Information Protection and Electronic Documents Act (PIPEDA) regulates the use of information for commercial activities by private sector organizations in Canada, and provides a "floor" for privacy expectations.[25] Certain provinces (Ontario, New Brunswick, Newfoundland and Labrador) have issued exemptions to PIPEDA for personal health custodians, where provincial health privacy legislation has been deemed "substantially similar" to PIPEDA.[26] Other provinces and territories have passed health privacy laws that have not been deemed substantially similar to PIPEDA. Thus, PIPEDA still applies in certain cases, including the transmission of personal health information across borders or to destinations outside Canada.[27]

With respect to privacy breach reporting, at the provincial level, Alberta amended its privacy legislation to mandate data breach reporting for private sector organizations, including private organizations in the health sector.[28] Other provincial health privacy laws in Ontario, New Brunswick, and Newfoundland and Labrador contain reporting requirements for the health sector.[29,30, 31] Under amendments to PIPEDA by the Digital Privacy Act in 2015, Canadians must be notified in circumstances in which their personal information has been lost or stolen and there is a risk of resulting harm. In addition, organizations must report data breaches to the Privacy Commissioner of Canada.

The Privacy Commissioner of Canada has engaged in a public consultation about new data breach requirements, pursuant to the legislation. Recently, the Office of the Privacy Commissioner of Canada made a submission to the National Security Policy Directorate of Public Safety Canada, along with its provincial and territorial counterparts, as part of a national consultation on key elements of Canada's national security laws. The submission made reference to Canada-US privacy principles under the "Beyond the Border Action Plan." Canada's privacy commissioners suggested the government consider importing some Canada-US privacy principles into law, to ensure there is a level of consistency between domestic and international information sharing agreements.[32]

Why the Canada-US relationship presents opportunity for better adoption of connected health technologies

Canada and the United States not only share the friendliest border in the world but also have a uniquely close partnership in regulatory harmonization. For example, the US-Canada Regulatory Cooperation Council (RCC),[33] an effort dedicated to harmonizing regulations across different sectors, was established in 2011 at the highest levels of government. Within the context of public safety and security, Canada and the US benefit from extensive cooperation and bilateral initiatives, most notably in the "Beyond the Border" Action Plan, the Canada-US Cyber Security Action Plan, and the Canada-US Privacy Principles. The trusted partnership between Canada and the US provides an opportunity to build upon a track record in regulatory and policy coordination so priorities for harmonizing critical requirements for mobile health technologies and related issues can be set. Ultimately, greater regulatory cooperation can advance the economic competitiveness of the mobile health sector in both countries, while maintaining high levels of protection for health, safety, and security.

Health privacy and security

Advances in today's Canadian and American health systems are highly dependent on leveraging data to produce value-based results from secure datasets. At the same time, the growth and adoption of connected health technologies could be threatened by the lack of coordination and information sharing between different nations. Such coordination between nations can be a complex— especially where there may be a language barrier, geographic distances, or cultural differences on privacy. A key question is what are existing policies—as well as legal and ethical considerations— to address privacy and security, and it is possible to create a level of consistency across borders?

Canada and the US are poised to establish more formal cooperation around common health data security interests, based on current coordination in related areas:

- In 2011, the "Beyond the Border" Canada-US collaboration enhanced data transfer security with an aim to accelerate the legitimate flow of services.[34] In 2012, the initiative introduced a set of joint privacy principles to fortify data sharing procedures across borders.[35] Although the Beyond the Borders Action Plan does not cover health services, the initiative is the cornerstone for common cross-border security initiatives and emphasizes the mutual commitment by both countries to individual privacy.[36]
- The "Beyond the Border" Health Security Working Group is a joint effort by Canadian and US experts to better communicate and share information before and during an emergency response such as H1N1, Ebola, Zika virus.
- The Canada-US Cybersecurity Action Plan[37] (2010-2015) established an arrangement for analytic exchange between the US National Cybersecurity and Communication Integration Center and the Canadian Cyber Incident Response Centre. Under the plan, both organizations benefit from a compilation of lessons learned using automated indicator sharing and coordinated joint alerts, which enables rapid information exchange across borders.
- The 2010 Canada-United States Action Plan on Critical Infrastructure[38] promotes a more integrated Canada-US approach to critical infrastructure resilience through activities that coordinate the movement of people and goods across the border during and following an emergency.

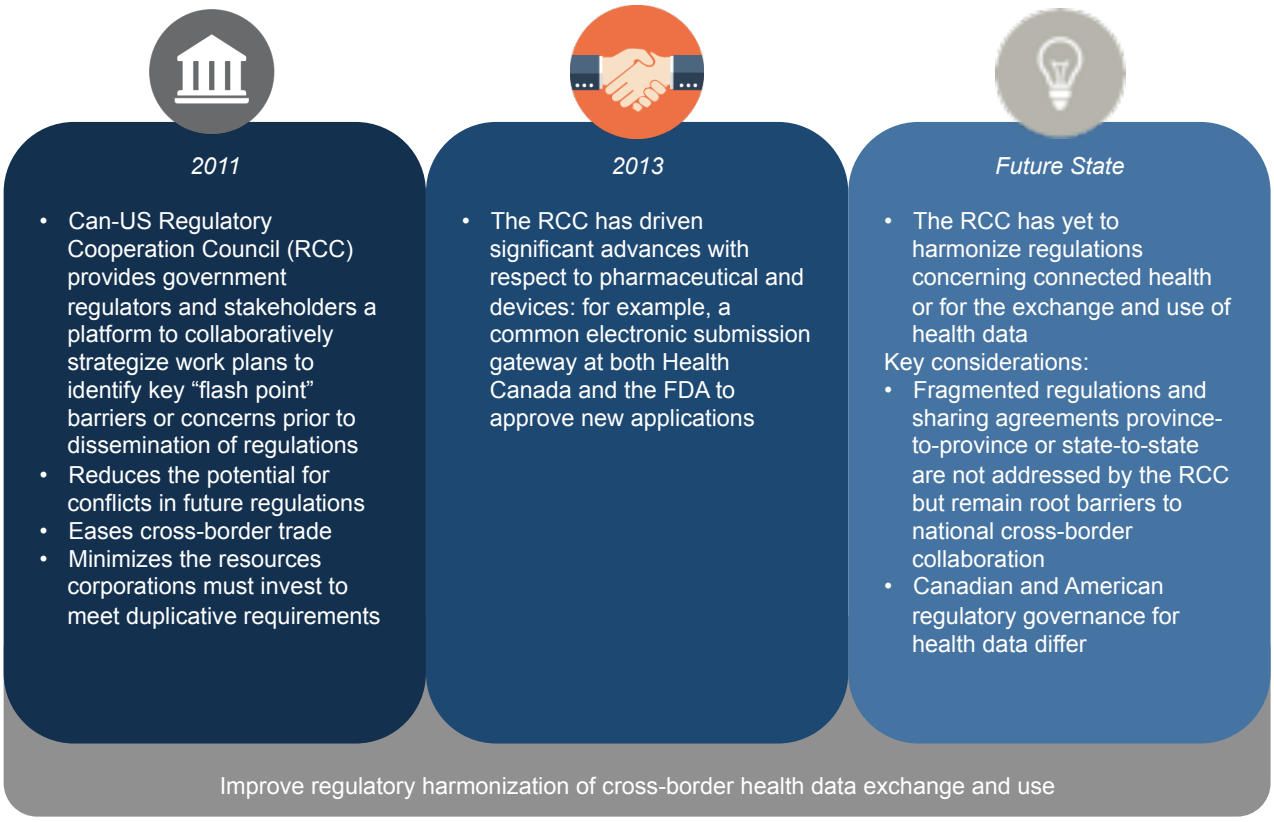
- Hosted by Public Safety Canada, Justice Canada, and the US Departments of Justice and of Homeland Security, the Canada-United States Cross-Border Crime Forum[39] (CBCF) addresses transnational crime issues such as organized crime, counter-terrorism, smuggling, economic crime, and other emerging cross-border threats. In addition, the CBCF concentrates on resolving obstacles to cross-border cooperation in law enforcement, primarily with regard to policy, regulations, and legislation.

Areas of Regulatory Harmonization between Health Canada and Food and Drug Administration

The RCC provides government regulators and stakeholders a platform to collaboratively strategize work plans to identify key "flash point" barriers or concerns prior to promulgation of regulations.[40]

The RCC reduces the potential for conflicts in future regulations, eases cross-border trade, and minimizes the resources corporations must invest to meet duplicative requirements. Simplifying the regulatory process has the potential to reduce the price of consumer goods and free capital for reinvestment.

The RCC has driven significant advances with respect to pharmaceuticals and medical devices: for example, a common electronic submission gateway at both Health Canada and the Food and Drug Administration (FDA) to approve new applications. But the RCC has yet to harmonize regulations concerning connected health or the exchange and use of health data.[41]



Steps to Regulatory Harmonization of Cross-Border Health Exchange and Use

While the RCC could serve as a vehicle to harmonize regulations in connected health, certain limitations should be considered. First, the RCC efforts are aimed at federal regulatory concerns.[42] Fragmented regulations and sharing agreements province-to-province or state-to-state are not addressed by the RCC but remain root barriers to national cross-border collaboration. Second, Canadian and American regulatory governance for health data differ. Canada Health Infoway, an independent, non-profit government funded organization tasked with accelerating the adoption of digital health solutions, is not a regulatory authority. Therefore, there is no direct Canadian equivalent to the American Office of the National Coordinator (ONC).[43]

In addition to the RCC, there are other forums that both Health Canada and the FDA participate in such as the International Medical Devices Regulators Forum (IMDRF), a voluntary group comprised of nine regulatory authorities: Australia, Brazil, Canada, China, the European Union, Japan, Russia, Singapore, and the United States. Health Canada is chair of the IMDRF in 2017 and will be hosting IMDRF's Management Committee (MC)

meetings in March and September 2017. Under the IMDRF, one item currently under consultation relates to regulation of software as a medical device (sAMD).[44]

In both countries, under the direction or in partnership with regulatory authorities, processes are being established to mitigate cybersecurity-related health risks:

- Health Canada's 2016-17 priorities and plans emphasize the urgent need to modernize frameworks to keep with the rapid pace of technology.[45,46,47,48]
- Organizations such as the Canadian Cyber Threat Exchange (CCTX) are sharing cybersecurity threat analysis and risk mitigation recommendations cross-sectors nationally.[49]
- In late 2016, the FDA issued guidance on procedures for managing post-market cybersecurity concerns specific to connected medical devices. The FDA guidance recommends that device makers should have a cybersecurity risk management program and establishes criteria for reporting based on the probable risk to patients.[50] Additionally, in late 2016, the FDA initiated a Memorandum of Understanding with the National Health Information Sharing and Analysis Center (NH-ISAC) and the Medical Device Innovation, Safety and Security Consortium (MDISS) to encourage information-sharing on cybersecurity threats for medical devices.

Data storage

Health data can be transferred outside one's own country jurisdiction for a variety of purposes – patient treatment, a commercial transaction, processing or long term storage. The cross-border collection, processing and storage of health data can produce efficiency gains and accessibility for organizations in both countries. At the same time, the movement to outsource data processing and storage on a cross-border basis demands greater Canada-US cooperation over proper governance and guidelines for cross-border data flows.[51]

In Canada, cross-border flow and storage of health records in the United States has been limited by concerns involving the US PATRIOT Act. While privacy legislation in Canada protects personal health information stored in Canada, any data transferred out of Canada will be subject to laws in the country where the data has been transferred.

British Columbia and Nova Scotia	• Enacted data blocking measures that prohibit public sector bodies (which include utilities, hospitals and Crown corporations in those provinces) from permitting out-of-country access or disclosure. • The data-blocking restrictions place rigorous restrictions on the storing, accessing and disclosing of B.C. and Nova Scotia public sector data by service providers from or to locations outside Canada.
Alberta	• Amended public sector privacy laws to require notice to and consent from individuals for disclosure of personal information to law enforcement bodies outside Canada.
Quebec	• Privacy legislation does not require notice, but notice of out-of-country data transfers is recommended as a best practice.

Canadian legislation for data transfers outside Canada differs by province. Certain provinces have enacted legislation that places restrictions on storage of records outside Canadian jurisdictions, including health records.

The US PATRIOT Act has been controversial both in the United States and abroad. Section 215 of the PATRIOT Act expanded the power of American law enforcement officials to obtain personal information records stored within the United States. In Canada, the law provoked controversy about the security and privacy of data pertaining to Canadian citizens held in the United States. Despite an opinion from the Canadian Attorney General determining that the PATRIOT Act posed "minimal" risk, this contentious political issue resulted in four provinces enacting legislation that restricted data exchange, including health data, between these provinces and the United States.[52]

There are cases where the presence of Canadians' health data in the US has been permitted once the provincial privacy commissioner determined that appropriate controls were in place to restrict access to personal health information.[53] A Canada-US framework relating to the collection, processing, and storage of health data could aim to establish a uniform set of controls that strike a necessary balance between security, privacy, and accessibility.

Research

Health data can be used for medical research, population health, and healthcare delivery systems improvement.[54] Researchers are pursuing initiatives with data mining[55] and big data analytics[56] that may contribute to improving the quality of health services and lead to advances in population health by identifying key trends.[57] When available, electronic health records (EHRs) provide "longitudinal, comprehensive, and interoperable" data and serve as a "repository of electronically maintained information about an individual's lifetime health status and health care."[58] In turn, data analysts and researchers can use such data to improve the delivery of care by looking at the effectiveness and cost of specific interventions and treatments.[59] Using data, efforts to refine payment and delivery systems are possible regardless of payer source because both the United States and Canada share an interest in reducing costs while ensuring access to care and quality services.[60]

Efforts to refine payment and delivery systems should be possible regardless of payer source

As a starting point, policymakers must balance access to data for research with the privacy of trial participants, especially when trials are publicly funded.[61] Failing to do so may make some patients wary of participating but could also affect innovation.[62] For example, security issues and privacy restrictions stand as key barriers to widespread adoption of precision medicine, a highly promising field that has attracted significant government support in the United States.[63] The 21st Century Cures Act ("Cures"), enacted in December 2016, attempts to balance the demand for access to high quality data with stronger privacy protection.[64] The 21st Century Cures Act allows the National Institutes of Health (NIH) to mandate the sharing of data generated from NIH-supported research.[65] Scientists could then benefit from these publicly-funded data more quickly for the advancement of biomedical research.[66] The law requires NIH to provide NIH-funded scientists with a certificate of confidentiality, which requires them to protect identifiable patient information but also provides them with legal protections from being compelled to reveal such information

outside of certain situations.[67] To further protect individual privacy, the law allows NIH to refuse to release information in response to a Freedom of Information Act request if providing such information would allow the requestor to identify individual patients.

Additionally, policymakers should continue to work with industry stakeholders, patient advocates, and researchers to improve data sharing across borders in a secure manner to improve the drug development and approval process.[68] Data exchanges could reduce costs and improve the efficiency of clinical trials occurring in different countries.[69] If different countries harmonized the commercialization process and streamlined how the resulting data must be submitted, pharmaceutical companies may be able to reduce duplicative trials and could simplify data submission to multiple regulators, thus reducing the approval time for new drugs to come to market and into the hands of patients.[70] The reported costs of running clinical trials has increased so much that many pharmaceutical companies and foundational sponsors are looking outside the United States and Europe to run these trials.[71] Assembling clinical trial data from different countries can be complex. Each country's rules for conducting a trial, securing patients' data, and the sophistication of IT infrastructure may exhaust resources and budgets on redundant processes.[72]

Greater use and exchange of health data can enhance these harmonization efforts and the drug development process. Data derived from EHRs can be another means of collecting information to help supplement clinical trials:

> If the researchers aim to show whether a specific treatment achieves the desired benefits, they may reasonably choose to conduct a randomized clinical trial to ensure that uncontrolled variables that influence outcomes, such as age or drug interactions, do not confound the study. However, observational studies may be needed to determine whether the results of randomized clinical trials that involved only a few thousand patients can be generalized to the patient population at large and to realistic treatment situations rather than carefully controlled ones. Furthermore, observational research based on medical records will often be sufficient to determine a treatment's adverse effects.[73]

II. A Summary of the 2016 Connected Health Workshop

Cross-Border Health's one-day workshop consisted of two panels to cover the current policy, legal, and business environments in each country, followed by a facilitated dialogue with representatives from the relevant Canadian and US regulatory and policy-setting agencies.

Our first panel provided a broad overview of each country's health system and how each country conceptualizes mobile health, health IT, and other technologies to foster connected health.

Our second panel focused on the business and operational side of mobile health and the challenges facing providers, developers, and other stakeholders, by examining questions such as:

- How is information managed, and how could it be used for research and public health purposes?
- Who owns the data contained in mobile records, and what is the role of consumers in data utilization?
- What are existing policies, laws, and ethical considerations to address privacy and security, and is it possible to harmonize them across borders?

The second panel also addressed the importance of international regulatory coordination with respect to the growth and adoption of connected health technologies.

Finally, the workshop concluded with a facilitated dialogue between Canada and US federal and provincial bodies aimed at identifying topics worthy of ongoing Canada-US regulatory coordination in connected health.

To solicit input from the audience, key framing questions included:

- To what extent are Canada and the United States currently aligned with respect to regulatory oversight of mobile health and big data?
- Is it desirable to work toward regulatory coordination in mobile health? If so, what should be the key objectives? Key concerns?

- Are there “low hanging fruit” opportunities in regulatory cooperation that could be targeted first to build momentum for future efforts?
- As mobile health and big data capabilities around health IT continue to evolve, regulatory considerations will continue to be challenged. Are there forward-looking topics that Canada and the United States could begin to address now before regulations are promulgated?

Key Points from Panel Sessions

Panel 1: Mobile Health and Regulation in Canada and the United States: Policy and Legal Landscape

Panel Speakers

- Edward Brown, MD, CEO, Ontario Telemedicine Network
- Tim Squire, Partner, Fasken Martineau LLP
- Ashley Ridlon, Senior Manager, Bipartisan Policy Center
- Nicolas Terry, Indiana University Robert H. McKinney School of Law and Executive Director of the William S. and Christine S. Hall Center for Law and Health

Panel moderator

- Dale Van Demark, Partner, McDermott Will & Emery LLP

Key Points

(1) Canada and US health systems share important similarities and challenges:
   - Lack of accountability in system over patient journey
   - Complex and expensive systems, but both are moving away from fee-for-service models
   - Powerful role of sub-national government (states and provinces) in delivering care
   - Following privacy rules is essential for vendors, but confusion and compliance is costly and can create barriers for smaller vendors in both countries
   - Regulatory oversight in areas such as mobile health and cybersecurity is evolving, with new ground that need to be covered; for example, US federal

health data protection (HIPAA) are limited when non-covered entities such as most mobile app developers and data brokers acquire health data

- Notable differences include:
    - Canada does not have one national health system, but rather 13 health systems given the 10 provinces and 3 territories.
    - In the US, most insurance is private and half of Americans receive health insurance from their employer

(2) Canada-US regulatory cooperation can promote better trade and security

- Connected health could be overly-regulated in some areas and under-regulated in others
- Great opportunity for better Canada-US cooperation on regulatory matters, making it easier for companies to sell into each other's country
- FDA and Health Canada share similar definitions for low risk medical devices
- FDA provided additional guidance to stakeholders to help navigate regulatory approval process for medical devices and digital and mobile health applications. One panelist noted that FDA has taken a "light touch" in respect to regulation of such health applications.
- It is important for Health Canada to provide guidance, address risks associated with technology, providing clarity to industry on what to expect
- The 21st Century Cures Act established new policies dealing with device regulation that could be the subject of future regulatory harmonization discussions with Health Canada. For example, 21st Century Cures exempted five categories of software functions from the definition of "device" under the Food, Drug and Cosmetics Act, effectively limiting FDA regulation of low-risk medical devices. However, if the FDA determines that a type of software would reasonably be likely to have serious adverse health impact, then the FDA could regulate that software as a device.

(3) Both countries should find ways to collaborate, as they look to confront similar demands:

- Establishing an effective payment model for telemedicine
- Struggling with interoperability to the frustration of payers, patients, and policymakers

- Achieving oversight of the wearable technology market
- Determining ownership and control over patient data
- Integrating privacy and security laws, determining who holds and owns data
- Ensuring privacy for mobile health applications
- Using mobile technology applications to address aging populations with multiple chronic diseases

Panel 2: Cross-Border Opportunities for Commerce, Public Health, and Research in Mobile Health and Connected Care

Panel Speakers

- Adam Darkins, MD, Vice President of Medical Affairs and Enterprise Technology Development, Medtronic
- Carrie Stover, Senior Director, Ascension
- Mike Popovich, CEO, Science Technologies Corporation (STC)
- Alicia Duval, Senior Vice President, Industry Relations, GS1 Canada

Moderator

- Jodi Daniel, Partner, Crowell and Moring, LLP

Key Points

(1) Consumers are central to realizing the potential of connected health

- Data can empower patients to mitigate public health risks, promote patient self-management and prevent hospital admissions and readmissions
- Portability of patient records and patient rights to access data remain a challenge
- Office of National Coordinator for Health IT (ONC) has proposed rules for direct-to-consumer help to engage providers and support patients' ability to download records
- The Blue Button program,[74] initiated by the US Department of Veterans Affairs and now available for over 450 organizations, serves as a model for patient electronic access to records

(2) Telehealth is challenging traditional care delivery, but public policy has not caught up with the technology so administrative barriers remain.

- In a telehealth system, the care question goes beyond what needs to be done and asks where, when, and who should perform the task at hand. Chronic diseases such as diabetes do not need to be cared for in the hospital. Remote patient monitoring allows health providers to better handle chronic disease and conditions, which is an increasing demand on their resources
- Legislation and regulations should enhance the widespread utilization of telehealth. Currently, some laws and policies prevent virtual care from being available in some areas
- Ongoing uncertainty around billing and reimbursement for telehealth stalls its deployment. Providers are willing to take risks to encourage utilization, but the legal process complicates efforts for providers to assume risk in reimbursement

(3) The health supply chain is an untapped opportunity

- Adoption of identification standards in health sector could provide tools to strengthen patient safety, global trade, and counterfeit seizures
- Canada and the United States share a highly integrated in supply chain in other sectors such as transportation, which could inspire similar integration in the health sector
- Identification standards require cross-border working groups that are committed to implementation. In Great Britain, the National Health Service established a process dedicated to implementation, which contributed to the success of its health supply chain programs

(4) Interoperability is necessary to make health data useful

- Health organizations have volumes of patient data but need to have systems that can talk to one another, so as to empower physicians and patients with data

(5) Better consistency in privacy rules between jurisdictions can accelerate innovation in digital healthcare

- Breach notification rules provide a challenge, as more breaches create fear and security risks stifle innovation
- There is tremendous complexity and unevenness between federal and state/ provincial authority in privacy. Striving for simplicity and consistency can promote innovation and better data security

(6) Targeting Disease: Canada-US Collaboration on public health issues and chronic conditions

- Cases of H1N1, Ebola, and Zika as well as the opioid crisis demonstrate the importance of cross-border cooperation in public health.
- Canada and United States both are grappling with rising healthcare costs associated with chronic diseases, and information sharing on patient populations and trends can be useful
- Choosing to focus on one area for Canada-US data sharing and interoperability, such as immunization records, can lay the groundwork for other areas, such as opioid data, diabetes, etc.

Panel 3: Facilitated Dialogue: US and Canada Regulatory Agencies

Panel Speakers

- Bakul Patel, Associate Center Director for Digital Health, Food and Drug Administration
- Vikesh Srivastava, Associate Director, Business Informatics Division, Resource and Operations Directorate, Health Products and Food Branch, Health Canada
- Cora Tung Han, Senior Attorney, Division of Privacy and Identity Protection, Federal Trade Commission
- Deven McGraw, Deputy Director for Health Information Privacy, Office of Civil Rights, US Department of Health and Human Services
- Jill Clayton, Privacy Commissioner, Province of Alberta
- Michael Green, CEO, Canada Health Infoway
- Steven Posnack, Director, Office of Standards and Technology, Office of National Coordinator for Health Information Technology

Moderator

- Diane Johnson, Senior Director, North America Regulatory Affairs, Policy and Intelligence Medical Devices, Johnson & Johnson

Key Points

(1) Regulatory systems must keep pace with rapid growth in connected health technologies

- In certain areas, software is evolving to be classified as medical devices.
- Common definitions and vocabulary in connected health can serve as an initial step toward harmonization between different jurisdictions. Regulators can benefit from establishing a common set of principles for the clinical evaluation of software.
- Adapting to changes is a challenge and underscores the importance of building capacity within regulatory agencies. Workforce, tools, and systems are being updated to adjust to technological advancements in the field
- Regulators fulfill an important role in protecting the consumer from deceptive or misleading mobile health apps and consumer data security risks
- Regulators in Canada and other countries can look to FDA's Sentinel Initiative as a model for building effective partnerships between regulators and data partners, to ensure rapid and secure access to information from a variety electronic healthcare data sources

(2) Overlapping regulatory authorities demand effective multi-agency cooperation, and there are good examples in both countries:

- American example: Joint guidance between the Federal Trade Commission and HHS's Office of Civil Rights, FDA, and ONC for mobile health apps[75]
- Canadian example: Canada Health Infoway and Health Canada on Prescribe-IT™, which allows prescribers to electronically transmit a prescription to a patient's pharmacy of choice[76]

(3) Big data provides opportunities for regulators, along with a demand for governance rules

- Increasing availability and a variety of data sources is a positive development. Important questions remain about how to leverage data to improve safety and health outcomes

- The use of big data and analytics is multi-dimensional and requires cooperation across different sectors
- Regulatory authorities are developing the capacity to leverage big data to inform regulatory decision-making and exploring applications of big data, such as in pharmacovigilance
- Regulators are looking to support areas like secure messaging, big data, and video conferencing
- Inappropriate handling and sharing of data are legitimate concerns about big data, heightening demands for regulations and standards. 21st Century Cures created new statutes governing how data can be legally stored and shared

(4) Interoperability has come a long way, but significant goals remain unmet

- After considerable investment, it is important for EHRs to talk to one another. In Canada, interoperability still has a long way to go, but activities such as a pan-Canadian system for e-prescribing signals a positive development

(5) There is a critical inter-relationship between federal and sub-national authorities and statutes regarding privacy

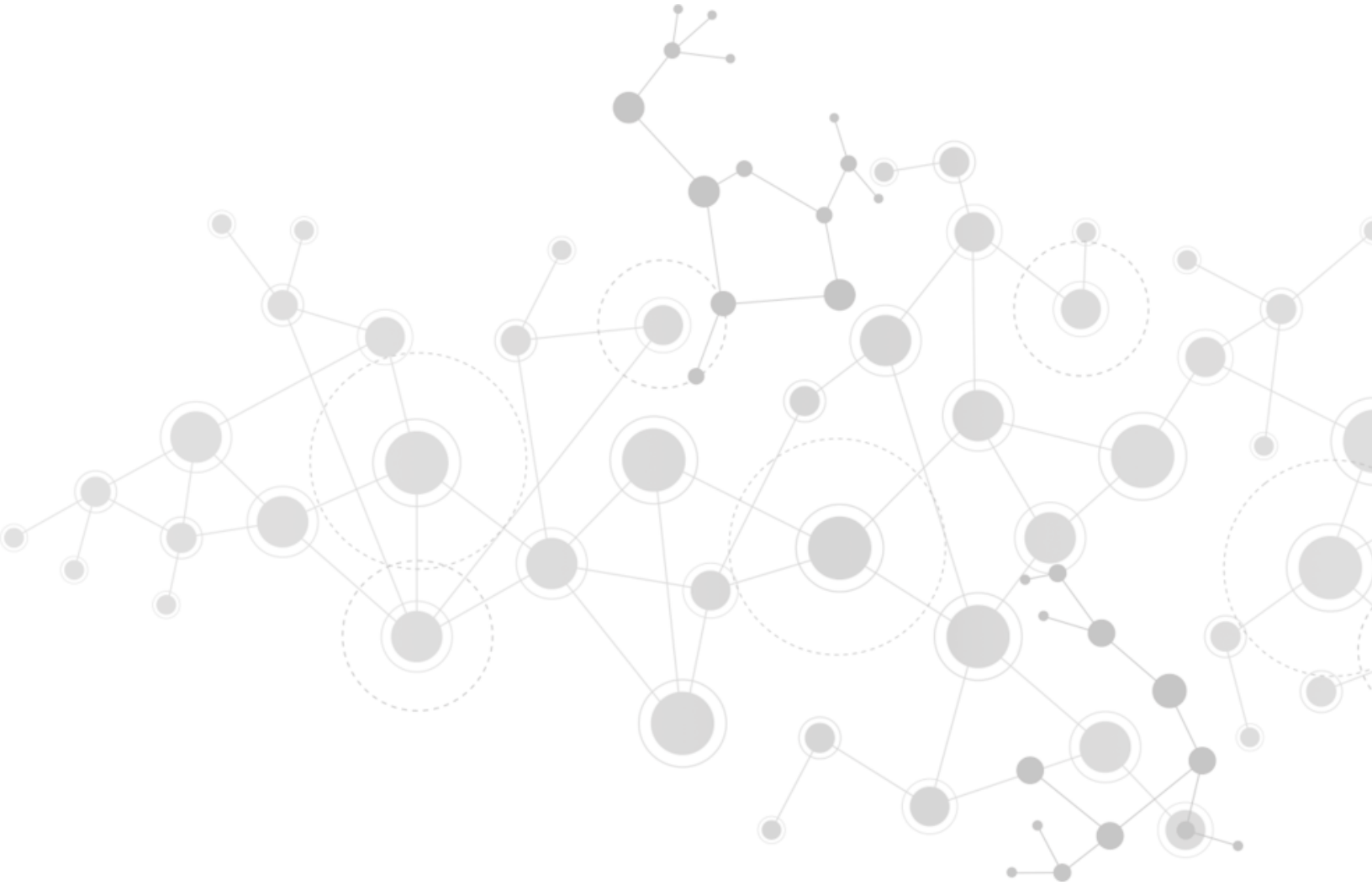
- In the US, not all items fall under HIPAA's jurisdiction at the federal level. For example, there are state and federal privacy breach notification rules that are different from one another
- In Canada, each of the thirteen provinces has its own health privacy legislation
- For example, Alberta requires privacy impact assessments (PIAs) for new technologies being sold in the province, but not all provinces have the same PIA requirements

(6) Issues around patient records and data include:

- Individual patients want to access their patient records digitally. Systems need to address the fact that the more we are connected, the more vulnerable we are to losing patient data
- Real world data provide opportunities in regulatory evaluations. There are opportunities for a harmonized set of real-world data, encouraging open methods in development to mine observational data, and considering adaptive approval pathways using patient data

(7) Possible areas for Canada-US collaboration could include:

- Information sharing, common certification for health apps
- Enhancing surveillance, information sharing to confront the opioid epidemic
- Cross-border internet sales of medicine
- Learnings about privacy impact assessments, privacy risk for devices, EHRs, or health exchanges

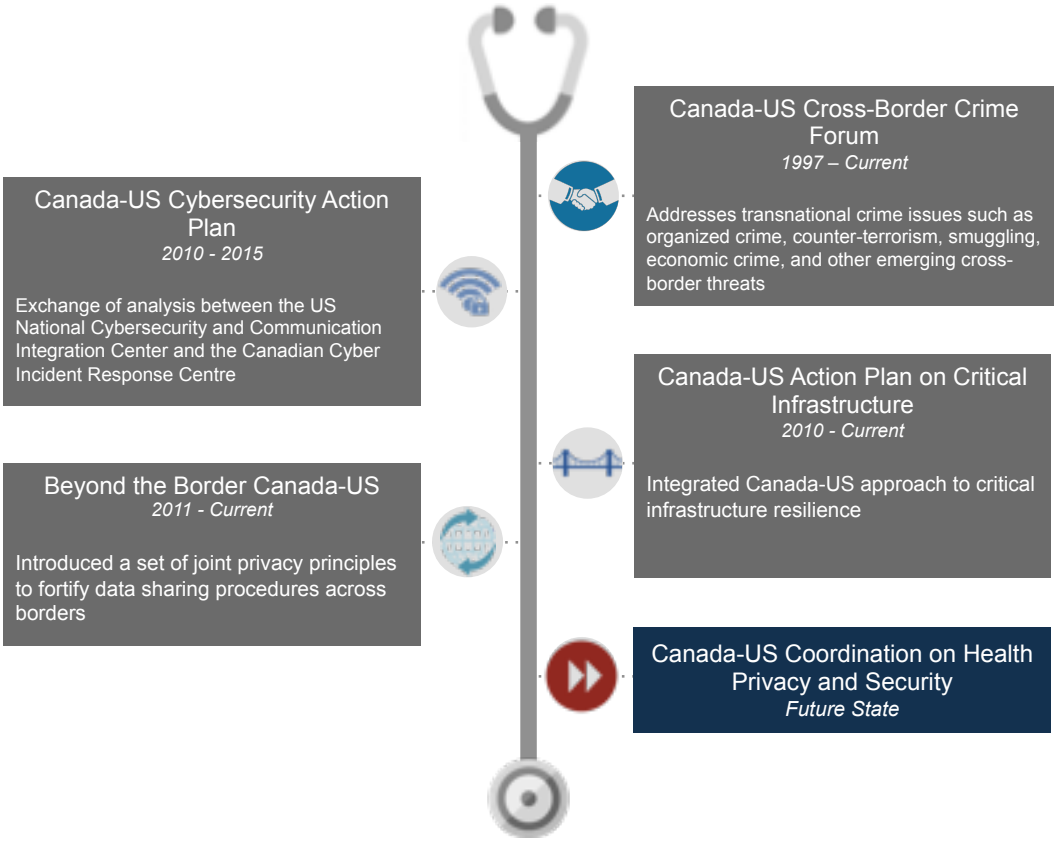


III. Recommendations Based on the Workshop Proceedings and Input

A central objective of our Canada-US Connected Health Workshop was to develop recommendations for future Canada-US regulatory and policy coordination in connected health. The recommendations below are based on the workshop's discussions and subsequent consultation with speakers, audience members, and other subject matter experts.

1. Canada-US Alignment on Health Data Privacy Protection

Currently, a coordinated Canada-US dialogue on health privacy protection does not exist, but it would serve as a natural extension to the Canada-US "Beyond the Border" Action Plan's Joint Statement on Privacy Principles. In addition, any mutual understanding in health privacy and keeping patient information secure could build upon existing Canada-US agreements that align our federal, state, and provincial authorities around common goals in security, public health preparedness, cyberterrorism, and critical infrastructure.



In both countries, health privacy laws and regulations fall under federal and subnational jurisdictions, while health providers—the predominant holders of EHRs—are heavily dispersed. The multiplicity of actors, laws, and regulations can complicate national and bilateral cooperation over health privacy protection while hindering the process of scaling up technology adoption across jurisdictions. And, when health information is breached, clarifying rules for cross-border breach notification may help ensure that patients will be notified in the case of a serious breach of their information because providers, insurers, and other stakeholders will know their responsibilities. The patchwork nature of privacy laws and regulations make it more difficult to keep patient privacy secure.

For such reasons, there is value in establishing a Canada-US dialogue between health privacy administrators from federal and sub-regional levels and law enforcement and a broader group of stakeholders in the health sector. A dedicated forum could enable cross-border knowledge exchange and help establish a common front on health privacy protection between regulatory and enforcement bodies. Reaching an alignment on policy, regulations, and standards could provide a level of consistency that is important for strengthening security while providing greater economic opportunities for digital health technologies.

Recommendation: Establish a Canada-US Health Privacy and Security Forum to assemble privacy regulators, enforcement officers, and health stakeholders more formally. The Forum would meet continually to share information about common risks, develop a work plan with common goals, and identify areas where coordination may be beneficial to security and economic interests such as breach notification and voluntary standards development.

Anticipated Outcome: Improved coordination on health privacy matters, while fostering greater economic and trade opportunities for Canada-US technology providers.

2. Regulatory Harmonization in Health Information Technology

Through the RCC, Canada and the United States have established a track record in regulatory harmonization, including a common electronic submission gateway at both Health Canada and the FDA to approve new drug applications. As described above, the

RCC prevents conflicting future regulations, eases cross-border trade, and minimizes the resources corporations must spend to meet requirements.

Similar to RCC efforts concerning pharmaceuticals and medical devices, the RCC could be utilized to harmonize policies for the exchange and use of health data. The FDA's recent guidance document on Post-Market Management of Cybersecurity in Medical Devices[77] provides an example of the forward-looking topics that would benefit from Canada-US alignment, especially given Canada-US coordination in cybersecurity in other sectors. A consistent approach to regulating connected health technologies could ensure Canada and the United States are working collaboratively to harness the potential of new technology, while also striking a balance with safety and security concerns.

Recommendation: Explore the potential to add health information technology topics to future work plans under RCC. As a first step, conduct stakeholder-government meetings to identify topics that could serve as early deliverables. Some topics may require bringing in new government agencies that may not fit squarely into the RCC dialogue, such as ONC and Canada Health Infoway.

Anticipated outcome: Drive economic opportunities in connected health technologies while strengthening security through better cooperation

3. Governance of Storage, Handling, and Sharing Health Records for Research Purposes

The growing practice of data mining and big data analytics has the potential to improve health quality and lead to advances in population health by identifying key trends. There is a great capacity for Canada and the US to collaborate and combine datasets, but a common understanding of the use of digital health records for research is required.

Canada and the United States share a similar patient pool, renowned research institutions, and repositories of patient data. For example, in recent years there has been a trend of increased interest in combining Canada-US data registries for specific diagnostic categories (e.g., oncology).[78] Such tools could support a coordinated strategy focused on harnessing health data for medical breakthroughs. In addition to exploring health trends, an aligned strategy for the use of health data for research could help attract investment in a Canada-US data "bloc" as a destination for research. At the same time, to promote collaboration, we need to have a mutual understanding about maintaining the privacy of

records used in research. The recently passed 21st Century Cures legislation set forth a new law in the United States governing the use of data for research. Areas like precision medicine are being pursued in both countries and carry tremendous potential for collaboration.

Recommendation: Pursue a Canada-US Memorandum of Understanding to govern the storage, handling, and sharing data for the purposes of research.

Anticipated outcome: Accelerated Canada-US collaboration in health research, looking at common trends in patient populations, which would serve as economic driver for research investment.

SUMMARY OF RECOMMENDATIONS

Topic	Recommendation	Rationale
Canada-US alignment on health data privacy protection	Establish a Canada-US Health Privacy and Security Forum	Promote knowledge exchange, regulatory consistency and help establish a common front on health privacy protection in a digital age
Regulatory harmonization in health information technology/digital health	Add health information technology topics to future work plans under the Regulatory Cooperation Council	Ensure Canada and the US are working collaboratively to harness the potential of new technology, while also striking a balance with safety and security concerns
Governance of storage, handling, and sharing health records for research purposes	Pursue a Canada-US Memorandum of Understanding to govern the storage, handling, and sharing data for the purposes of research	Great potential for Canada and the US to collaborate and combine datasets while establishing a common understanding over the use of digital health records for research

Portions of the background section were derived from Oliver Kim's "Ebbs and Flows: Issues in Cross-Border Exchange and Regulation of Health Information," in Annals of Health Law (2017), available at http://www.annalsofhealthlaw.com/annalsofhealthlaw/vol__26_issue_1?pg=46#pg46.

[1] The Road Ahead in Connected Health: Technology-Driven Healthcare Has Arrived (Rep. No. 1). (2015, Fall). Retrieved April 30, 2017, from HIMSS Media website: https://validic.com/wp-content/uploads/2015/04/HIMSS-white-paper-connected-health.pdf.
Portions of the background section were derived from Oliver Kim's "Ebbs and Flows: Issues in Cross-Border Exchange and Regulation of Health Information," in Annals of Health Law (2017), available at http://www.annalsofhealthlaw.com/annalsofhealthlaw/vol__26_issue_1?pg=46#pg46.

[2] The Road Ahead in Connected Health: Technology-Driven Healthcare Has Arrived (Rep. No. 1). (2015, Fall). Retrieved April 30, 2017, from HIMSS Media website: https://validic.com/wp-content/uploads/2015/04/HIMSS-white-paper-connected-health.pdf.

[3] Terry, N. Protecting Privacy in the Age of Big Data. 81 UMKC Law Review 1 (2012).

[4] Health Insurance Portability and Accountability (HIPAA) Act, Pub. L. No. 104–191, 110 Stat. 1936 (1996).

[5] 45 C.F.R. § 164.104 (2013).

[6] 45 C.F.R. § 160.103 (2014).

[7] Id. Under the Privacy Rule, covered entities may use and disclose Public Health Information (PHI) without an authorization for uses such as "treatment, payment, or health care operations," certain public health activities, and when the individual health information has been "de-identified." For a covered entity to disclose PHI for other purposes, the covered entity may need to seek the patient's authorization or offer him an opportunity to agree or object.

[8] 45 C.F.R. § 164.306 (2013). Under HIPAA's Security Rule, covered entities and business associates must follow standards to "ensure the confidentiality, integrity, and availability of all electronic" PHI and "protect against any reasonably anticipated threats or hazards" or unpermitted disclosures. Further, covered entities and business associates must "implement policies and procedures to prevent, detect, contain, and correct security violations."

[9] 45 C.F.R. § 164.104 (2013); Centers for Medicare and Medicaid Services, "Are you a covered entity?," available at https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html.

[10] Summary of HIPAA Privacy Rule (Rep.). (n.d.). Retrieved April 30, 2017, from U.S. Department of Health and Human Services website: http://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/.

[11] Id.

[12] Kara, J. (2002). HITECH 101. American Bar Association Young Lawyers Division. Retrieved April 30, 2017, from American Bar website: http://www.americanbar.org/groups/young_lawyers/publications/the_101_201_practice_series/hitech_101.html.

[13]The Medicare and Medicaid Electronic Health Record Incentive Programs: Stage 2 Toolkit, (2013), Retrieved April 30, 2017, from Centers for Medicare and Medicaid Services website: https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Downloads/Stage2_Toolkit_EHR_0313.pdf.

[14] Joachim, R. (2014). Creating Value in Health Care through Big Data: Opportunities and Policy Implications. Health Affairs, 1115-1116.

[15] American Recovery and Reinvestment Act of 2009 § 13408, 42 U.S.C.A. § 17938 (including patient safety organizations, state health information organizations, and subcontractors); 45 C.F.R. § 160.103 (2014).

[16] American Recovery and Reinvestment Act of 2009 § 13401, 42 U.S.C.A. § 17931.

[17] American Recovery and Reinvestment Act of 2009 § 13401, 42 U.S.C.A. § 17934.

[18] American Recovery and Reinvestment Act of 2009 § 13401, 42 U.S.C.A. § 17931.

[19] HITECH Breach Notification Interim Final Rule (Rep. No. 1). (2009, Fall). Retrieved April 30, 2017, from U.S Department of Health and Human Services website: http://www.hhs.gov/hipaa/for-professionals/breach-notification/laws-regulations/final-rule-update/HITECH/index.html.

[20] 42 U.S.C.A. §§ 17932, 17935, & 17937.

[21] HHS Final Rule Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules (January 25, 2013). Retrieved September 05, 2017 from U.S. Department of Health and Human Services website: https://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf

[22] Pritts, J. L. (2002). Altered States: State Health Privacy Laws and the Impact of the Federal Health Privacy Rule. The Yale Journal of Health Policy, Law, and Ethics. Retrieved April 30, 2017, from Yale Digital Common Law website: http://digitalcommons.law.yale.edu/yjhple/vol2/iss2/6.

[23] Habte, L. M. (2014, December 5). Federal and State Privacy Laws: Strategies for Analysis of Big Data in Healthcare (Rep. No. 1). Retrieved April 30, 2017, from Healthcare Informatics website: https://www.healthcare-informatics.com/article/federal-and-state-privacy-laws-strategies-analysis-big-data-healthcare?page=2.

[24] Id.

[25] Id.

[26] Id.

[27] Id.

[28] Alberta's Personal Information Protection Act (Rep.). (n.d.). Retrieved April 30, 2017, from http://www.qp.alberta.ca/1266.cfm?page=P06P5.cfm&leg_type=Acts&isbncln=9780779762507.

[29] Ontario's Personal Health Information Protection Act (Rep.). (2016). Retrieved April 30, 2017, from http://www.ontario.ca/laws/statute/04p03.

[30] Personal Health Information Privacy and Access Act (Rep.). (2009). Retrieved April 30, 2017, from http://laws.gnb.ca/en/showfulldoc/cs/P-7.05/20121030.

[31] Personal Health Information Act (Rep.). (2008). Retrieved April 30, 2017, from http://assembly.nl.ca/Legislation/sr/statutes/p07-01.htm.
[32] Consultation on Canada's National Security Framework (Rep.). (2016). Ottawa, ON: National Security Policy Directorate. Retrieved April 30, 2017, from https://www.priv.gc.ca/en/opc-actions-and-decisions/submissions-to-consultations/sub_psc_161205/.
[33] United States and Canada Announce the 2016 Annual Work Plans (Rep.). (2016). ON: U.S.-Canada Regulatory Cooperation Council. Retrieved April 30, 2017, from http://trade.gov/rcc/.
[34] Beyond the Border: A Shared Vision for Perimeter Security and Economic Competitiveness (Rep.). (2016). Public Safety Canada. Retrieved April 30, 2017, from https://www.publicsafety.gc.ca/cnt/brdr-strtgs/bynd-th-brdr/index-en.aspx.
[35] Beyond the Border Action Plan Joint Statement of Privacy Principles (Rep.). (2015). Public Safety Canada. Retrieved April 30, 2017, from https://www.publicsafety.gc.ca/cnt/nws/nws-rlss/2012/20120628-2-en.aspx.
[36] Beyond the Border U.S. Fact Sheet (Rep.). (2017). Retrieved April 30, 2017, from https://www.dhs.gov/sites/default/files/publications/2017%201%2019%20BTB%20Fact%20Sheet.pdf.
[37] Cybersecurity Action Plan Between Public Safety Canada and the Department of Homeland Security (Rep.). (2015). Retrieved April 30, 2017, from https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cybrscrt-ctn-plan/index-en.aspx.
[38] Canada-United States Action Plan for Critical Infrastructure (Rep.). (2010). U.S Department of Homeland Security and Public Safety Canada. Retrieved April 30, 2017, from https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cnd-ntdstts-ctnpln/cnd-ntdstts-ctnpln-eng.pdf.
[39] Canada-United States Cross-Border Crime Forum (Rep.). (2015). Public Safety Canada. Retrieved April 30, 2017, from https://www.publicsafety.gc.ca/cnt/brdr-strtgs/crss-brdr-crm-frm-en.aspx.
[40] Canada-US Law Institute, "Welcoming Remarks," 37 Can.-US L.J. 289, 295 (2012).
[41] Canada-United States Regulatory Cooperation Council Joint Forward Plan August 2014 (Rep.). (2016). Government of Canada. Retrieved April 30, 2017, from https://www.canada.ca/en/treasury-board-secretariat/corporate/transparency/acts-regulations/canada-us-regulatory-cooperation-council/joint-forward-plan-august-2014.html.
[42] Id.
[43] Office of the National Coordinator for Health Information Technology (Rep.). (n.d.). Retrieved April 30, 2017, from https://www.healthit.gov/newsroom/about-onc.
[44] Software as a Medical Device (SaMD): Clinical Evaluation (Rep.). (2016). Retrieved April 30, 2017, from International Medical Device Regulators Forum website: http://www.imdrf.org/consultations/cons-samd-ce.asp.
[45] Health Canada 2016-17 Report on Plans and Priorities (Rep.). (n.d.). Retrieved April 30, 2017, from https://www.canada.ca/en/health-canada/corporate/transparency/corporate-management-reporting/report-plans-priorities/2016-2017-report-plans-priorities.html.
[46] Ontario's Personal Health Information Protection Act (Rep.). (2016). Retrieved April 30, 2017, from http://www.ontario.ca/laws/statute/04p03.
[47] Personal Health Information Privacy and Access Act (Rep.). (2009). Retrieved April 30, 2017, from http://laws.gnb.ca/en/showfulldoc/cs/P-7.05/20121030.
[48] Personal Health Information Act (Rep.). (2008). Retrieved April 30, 2017, from http://assembly.nl.ca/Legislation/sr/statutes/p07-01.htm.
[49] Mission of the Canadian Cyber Threat Exchange (Rep.). (n.d.). Canadian Cyber Threat Exchange. Retrieved April 30, 2017, from https://cctx.ca/mission/.
[50] Postmarket Management of Cybersecurity in Medical Devices (Rep.). (2016). Retrieved April 30, 2017, from Food and Drug Administration website: https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf.
[51] Collins, A., & Teitlebaum, C. (n.d.). Canadian Privacy Legislation and the Cross-Border Transfer of Personal Health Information; Part One: Personal Health Information (Rep.). Retrieved April 30, 2017, from http://www.airdberlis.com/Templates/Articles/articleFiles/454/Article%20-%20Cross%20Border%20Transfer%20of%20Personal%20Health%20Information.pdf.
[52] Fred Cate, Provincial Canadian Geographic Restrictions on Personal Data in the Public Sector, 3–8 (2008) (discussing the laws passed in Alberta, British Columbia, Nova Scotia, and Quebec).
[53] Health (Rep.). (n.d.). Information and Privacy Commissioner of Ontario. Retrieved April 30, 2017, from https://www.ipc.on.ca/images/Findings/up-phipa_hi06_45_rpt.pdf.
[54] WHO Consultation on Data Results Sharing During Public Health Emergencies. Background and Briefing. (Rep.). (2015). World Health Organization Centre for Evidence Based Medicine. Retrieved April 30, 2017, from http://www.who.int/medicines/ebola-treatment/background_briefing_on_data_results_sharing_during_phes.pdf.
[55] Data Mining: What is Data Mining? (Rep.). (n.d.). Retrieved April 30, 2017, from http://www.anderson.ucla.edu/faculty/jason.frand/teacher/technologies/palace/datamining.htm.
[56] Roski, J., Bo-Linn, G. W., & Andrews, T. A. (2014). Creating value in health care through big data: opportunities and policy implications. Health Affairs (Millwood). Retrieved April 30, 2017, from https://www.ncbi.nlm.nih.gov/pubmed/25006136.
[57] A New Era for the Healthcare Industry, Cloud Computing Changes the Game (Rep.). (2016). Retrieved April 30, 2017, from Accenture website: https://www.accenture.com/us-en/~/media/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Technology_2/Accenture-New-Era-Healthcare-Industry-Cloud-Computing-Changes-Game.pdf.
[58] Drabiak-Syed, K. (2013). Granular Control of EHRs to Overcome Fragmented Disclosure Law. Indiana Health L Rev, 10, 39-40.
[59] Sweet, L., & Moulaison, D. (2013). EHR Data and Metadata Challenges. Big Data 245-246.
[60] Cross-Border Health and Wilson Center, Canada-U.S. Health Summit 2015, (2016). Retrieved April 30, 2017, from http://pages.wilsoncenter.org/rs/219-MVU-643/images/Canada-U.S._Health_Summit_Summary_Report.pdf.

[61] Doshi, J. A., Hendrick, F. B., & Graff, J. S. (2016). Data, Data Everywhere, but Access Remains a Big Issue for Researchers: A Review of Access Policies for Publicly-Funded Patient-Level Health Care Data in the United States. EGEMs, 4(2), 1204. Retrieved April 30, 2017, from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4827788/
[62] Terry, N. Regulatory Disruption and Arbitrage in Healthcare Data Protection. 17 Yale Journal of Health Policy, Law, and Ethics (forthcoming 2017).
[63] 2016 Global Life Science Outlook (Rep.). (2016). Retrieved April 30, 2017, from Deloitte website: https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Life-Sciences-Health-Care/gx-lshc-2016-life-sciences-outlook.pdf.
[64] Hudson, K. L., & Collins, F. S. (2017). The 21st Century Cures Act — A View from the NIH. New England Journal of Medicine, 376, 111-113. Retrieved April 30, 2017, from http://www.nejm.org/doi/full/10.1056/NEJMp1615745.
[65] Sarata, A. K. (2016). The 21st Century Cures Act (Division A of P.L. 114-255) (Rep.). Congressional Research Services. Retrieved April 30, 2017, from https://fas.org/sgp/crs/misc/R44720.pdf.
[66] Hudson, K. L., & Collins, F. S. (2017). The 21st Century Cures Act — A View from the NIH. New England Journal of Medicine, 376, 111-113. Retrieved April 30, 2017, from http://www.nejm.org/doi/full/10.1056/NEJMp1615745.
[67] Sarata, A. K. (2016). The 21st Century Cures Act (Division A of P.L. 114-255) (Rep.). Congressional Research Services. Retrieved April 30, 2017, from https://fas.org/sgp/crs/misc/R44720.pdf.
[68] Cockburn, I. M., Bollyky, T. J., & Berndt, E. (2010). Bridging the gap: improving clinical development and the regulatory pathways for health products for neglected diseases. Clinical Trials. Retrieved April 30, 2017, from http://journals.sagepub.com/doi/abs/10.1177/1740774510386390.
[69] Hoffman, S., & Podgurski, A. (2013). The Use and Misuse of Biomedical Data: Is Bigger Really Better? (Rep.). Case Western Reserve University. Retrieved April 30, 2017, from http://scholarlycommons.law.case.edu/cgi/viewcontent.cgi?article=1605&context=faculty_publications.
[70] Global Forum (Vol. 3, Ser. 2, Rep.). (2011). ICH. Retrieved April 30, 2017, from http://www.diaglobal.org/Tools/Content.aspx?type=eopdf&file=%2fproductfiles%2f19794%2fgf_14%2Epdf.
[71] Li, R., et al., (2015). Global Clinical Trials: Ethics, Harmonization & Commitments to Transparency. Harvard Pub Health Rev, 1–2.
[72] Hoffman, supra note 69, at 506–07.
[73] Id. at 507.
[74] Your Health Data (Rep.). (n.d.). Health IT. Retrieved April 30, 2017, from https://www.healthit.gov/patients-families/your-health-data.
[75] Tool Created in Conjunction with HHS and FDA Will Help Businesses Determine Applicable Laws and Regulations (Rep.). (2016). Federal Trade Commission. Retrieved April 30, 2017, from https://www.ftc.gov/news-events/press-releases/2016/04/ftc-releases-new-guidance-developers-mobile-health-apps.
[76] PrescribeIT (Rep.). (n.d.). Canada Health Infoway. Retrieved April 30, 2017, from https://www.infoway-inforoute.ca/en/solutions/e-prescribing/prescribeit.
[77] Postmarket Management of Cybersecurity in Medical Devices (Rep.). (2016). Retrieved April 30, 2017, from Food and Drug Administration website: https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf.
[78] Cancer in North American 2004-2008; Volume One: Combined Cancer Incidences for United States and Canada (Rep.). (n.d.). North American Association of Central Cancer Registries, Inc. Retrieved April 30, 2017, from https://www.naaccr.org/wp-content/uploads/2016/11/Contents-of-CINA-2004-2008-V1.pdf.