Electronic Healthcare Law Review

VOLUME 11, NUMBER 1 Cited as (2020-21), 11 Electronic Healthcare Law Review AUGUST 2021

• PRIVACY COMMISSIONERS COMMENT ON VACCINE PASSPORTS[1] •

Daniel G.C. Glover, Partner, Michael Scherman, associate, Dana Siddle, Counsel, Grace Waschuk, associate, and Jennifer Choi, associate, McCarthy Tétrault LLP
©McCarthy Tétrault LLP, Toronto, Vancouver, Calgary


Daniel G.C. Glover


Michael Scherman


Dana Siddle


Grace Waschuk


Jennifer Choi

As the number of Canadians who have received their first dose of one of the COVID-19 vaccines increases and case numbers continue to decline across the country, we are seeing the slow easing of the public health orders and restrictions which, among other things, closed restaurants, limited occupancy, and curtailed travel. As a result, governments and businesses have begun to shift their focus on post-pandemic recovery, as re-opening plans continue to be rolled out.

To help facilitate this re-opening, and to encourage higher vaccination rates, "vaccine passports" are being considered by businesses, industries and various levels of government as a means of confirming a person's COVID-19 vaccination status. In Canada, Quebec has already started to issue downloadable QR codes that individuals can keep on their phones to prove that they have been vaccinated. While vaccine passports may ultimately take a variety of different forms – from physical certificates to smart phone credentials – in essence, they represent a record containing personal health information that individuals may be required to disclose to employers or in exchange for certain goods, services or access.

On May 19, 2021, the Federal, Provincial, and Territorial Privacy Commissioners (the "**Privacy Commissioners**") released a joint statement[2]

• In This Issue •

LexisNexis®

ELECTRONIC HEALTHCARE LAW REVIEW

Electronic Healthcare Law Review is published four times a year by LexisNexis Canada Inc., 111 Gordon Baker Road, Suite 900, Toronto ON M2H 3R1 by subscription only.

All rights reserved. No part of this publication may be reproduced or stored in any material form (including photocopying or storing it in any medium by electronic means and whether or not transiently or incidentally to some other use of this publication) without the written permission of the copyright holder except in accordance with the provisions of the *Copyright Act.* © LexisNexis Canada Inc. 2021

ISBN 0-433-46965-X (print)
ISBN 0-433-46969-2 (PDF)
ISBN 0-433-46967-6 (print & PDF)

Subscription rates: $305.00 per year (print or PDF)
$395.00 per year (print & PDF)

General Editor
Domenic A. Crolla, Gowling WLG (Canada) LLP, Ottawa
Maureen Murphy, Gowling WLG (Canada) LLP, Ottawa
Robert Sheahan, Gowling WLG (Canada) LLP, Ottawa

Please address all editorial inquiries to:

LexisNexis Canada Inc.
Tel. (905) 479-2665
Fax (905) 479-2826
E-mail: ehlr@lexisnexis.ca
Web site: www.lexisnexis.ca

ADVISORY BOARD

Jennifer Chandler, University of Ottawa, Faculty of Law • Giuseppina D'Agostino, Osgoode Hall Law School, Toronto • Paul DeMuro, Nelson Mullins Riley & Scarborough LLP, Fort Lauderdale, Florida • Chantal Léonard, Canadian Nurses Protective Society, Ottawa • Anne MacDonald, Ottawa Hospital • Maureen Murphy, Gowling WLG (Canada) LLP, Ottawa • Jean Nelson, Canadian Medical Association, Ottawa • Martin Lapner, Gowling WLG (Canada) LLP, Ottawa

Note: This review solicits manuscripts for consideration by the Editors, who reserves the right to reject any manuscript or to publish it in revised form. The articles included in the *Electronic Healthcare Law Review* reflect the views of the individual authors and do not necessarily reflect the views of the advisory board members. This review is not intended to provide legal or other professional advice and readers should not act on the information contained in this review without seeking specific independent advice on the particular matters with which they are concerned.

LexisNexis®

relating to certain privacy concerns raised by the development of vaccine passports (the "**Statement**"). Citing a need to incorporate "privacy best practices" in order to achieve protections commensurate with the sensitivity of individuals' personal health information, the Statement serves to remind of the serious privacy issues that should be considered alongside the potentially significant benefits that vaccine passports may ultimately facilitate. However, the Statement leaves open important questions of interpretation, some of which are discussed further in the Commentary section below.

SUMMARY OF THE STATEMENT

In the Statement, the Privacy Commissioners recognize that vaccine passports could offer substantial public benefit, including the promotion of personal liberties, fewer restrictions on social gatherings, and accelerated economic recovery. However, they caution that vaccine passports may also represent an encroachment on civil liberties that should only be pursued after careful consideration. The Statement recommends that any vaccine passport be developed and implemented in compliance with federal and provincial privacy laws, and should incorporate privacy best practices to ensure the highest level of privacy protection, given the sensitivity of the personal health information collected and disclosed.

The Privacy Commissioners propose that when developing and approving vaccine passports, the ***necessity***, ***effectiveness*** and ***proportionality*** of the vaccine passports and the contexts in which they are used must be considered to ensure that they comply with the principles underlying Canadian privacy law.

The Privacy Commissioners further suggest that vaccine passports must be limited in terms of the time and scope of their use, advocating that they should be decommissioned "*if, at any time, it is determined that they are not a necessary, effective or proportionate response to address their public health purposes*."

Recognizing that private businesses will be some of the primary users of vaccine passports, the Privacy Commissioners recommend that private sector

entities requesting that individuals present a vaccine passport in order to receive services or enter premises ensure that they have the legal authority to make such a request. In the view of the Privacy Commissioners, this authority should come from legislation or a public health order that clearly specifies: (1) the existence of the legal authority to request or require a vaccine passport; (2) to whom the authority is being given; and (3) the specific circumstances where the authority is operative.

The Privacy Commissioners also suggest that, absent legislation or a specific public health order, consent may provide sufficient legal authority for the implementation of vaccine passports by private sector entities. However, in such instances the Privacy Commissioners contend that: (1) consent must be voluntary and meaningful; (2) the information must be necessary to achieve the purpose; (3) the purpose must be appropriate in the circumstances; and (4) individuals must have a true choice, i.e., consent must not be required as a condition of service.

In contrast, the Privacy Commissioners suggest that, when it comes to public bodies, consent alone will not be a sufficient basis upon which to proceed and implement vaccine passports. In particular, they interpret public-sector legislation to the effect that consent may not be meaningful where a government or public body has a "monopoly" over a particular service.

COMMENTARY

(a) Balancing of Rights

The Statement appears broadly aimed at a range of audiences, including legislators, government entities and commercial businesses. Unfortunately, the Statement does not always distinguish which group(s) each recommendation is directed towards. For example, the Statement includes the following when discussing the balancing of rights in connection with a vaccine passport:

> *"Above all, and in light of the significant privacy risks involved, the necessity, effectiveness and proportionality of vaccine passports must be established for each specific context in which they will be used.*
>
> - *Necessity: vaccine passports must be necessary to achieve each intended public health purpose. Their necessity must be evidence-based and there must be no other less privacy-intrusive measures available and equally effective in achieving the specified purposes.*
> - *Effectiveness: vaccine passports must be likely to be effective at achieving each of their defined purposes at the outset and must continue to be effective throughout their lifecycle.*
> - *Proportionality: the privacy risks associated with vaccine passports must be proportionate to each of the public health purposes they are intended to address. Data minimization should be applied so that the least amount of personal health information is collected, used or disclosed."*

These principles are presented as being generally applicable to both government and business, but as they relate to businesses, they fail to consider *bona fide* business interests. Taking the *Personal Information Protection and Electronic Documents Act* ("**PIPEDA**") as the example, Section 5(3) states that "*An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances"*, which is read in light of PIPEDA's purpose (set out in Section 3) of balancing the right of privacy of individuals with the legitimate needs of businesses. As noted by the OPC in its guidance document on Section 5(3)[3] (quoting *A.T. v. Globe24h.com*)[4], *"the courts have generally taken into consideration "1) the collection, use or disclosure of personal information is directed to a bona fide business interest, and 2) whether the loss of privacy is proportional to any benefit gained.*"

The balancing of *bona fide* business interests with the privacy rights of individuals is fundamental to Canada's current private sector privacy laws. By comparison, the Statement focuses on necessity, effectiveness and proportionality to achieve a public health purpose and does not include any consideration of legitimate business needs. As such,

the considerations set out in the Statement would not be entirely accurate if they were applied to businesses.

(b) Legal Authority

In the Statement there is a suggestion that, for businesses and other entities that are subject to private sector privacy laws, the clearest authority under which to proceed with adopting some form of vaccine passport program would be a newly enacted public health order or law requiring the presentation of a vaccine passport to enter a premises or receive a service. This approach could help prevent a patchwork of policies and systems throughout the private sector, and leave the burden of analysis regarding the legal basis for such programs and how they should be regulated, with policy-makers.

At least in the context of the travel industry, Health Minister Patty Hajdu has indicated[5] that the federal government embraces the concept of vaccine passports and is considering possibilities for a standardized approach to certification forms for vaccinated Canadians that wish to travel internationally.

A consideration of any existing legal authorities that may be relied upon by businesses in other industries wishing to introduce a requirement for vaccine passports may also be worthwhile. For example, individual provinces in Canada already have laws that require students to show proof of immunization against certain diseases. Also, various provincial occupational health and safety laws impose general duties on employers to ensure the health and safety of workers, but the use of such laws to require vaccines has not been broadly tested in Canada.

(c) Consent

With respect to the issue of consent as a legal basis for vaccine passports, the Statement sets out the following:

> *"...consent may provide sufficient authority if it meets all of the following conditions, which must be applied contextually given the specifics of the vaccine passport and its implementation:*
>
> - *Consent must be voluntary and meaningful, based on clear and plain language describing the specific purpose to be achieved;*
> - *The information must be necessary to achieve the purpose;*
> - *The purpose must be one that a reasonable person would consider appropriate in the circumstances;*
> - *Individuals must have a true choice: consent must not be required as a condition of service."*

The first three bullets above are broadly aligned with the requirements of private sector privacy laws (to use PIPEDA as the example, see Section 5(3) and PIPEDA Principles 2 (Identifying Purposes) and 3 (Consent)). The fourth bullet, however, is a notable departure from private sector privacy laws, which recognize that an individual's consent may be required as a condition of service in various circumstances. For example:

- the Model Code to PIPEDA explains in clause 4.3.3 that *"An organization shall not, as a condition of the supply of a product or service, require an individual to consent to the collection, use or disclosure of Personal Information beyond that required to fulfil the explicitly specified and legitimate purposes" (PIPEDA Principles clause 4.3.3)*[6]*; and*
- the Guidelines for Obtaining Meaningful Consent[7] state the following: *"Individuals cannot be required to consent to the collection, use or disclosure of personal information beyond what is necessary to provide the product or service… For a collection, use, or disclosure to be a valid condition of service, it must be integral to the provision of that product or service such that it is required to fulfill its explicitly specified and legitimate purpose."*

The above examples make clear that consent may be required as a condition for service in various circumstances. This is a commonly accepted practice in our daily lives (for example, providing a driver's license to rent a car or to enter a pub). There does not appear to be any reason why the use of vaccine passports (or other verifications of vaccines) by private businesses should be treated any differently, especially where doing so negates a business's reasonable interest (especially in contexts of heightened risk or occupational health and safety concerns) in implementing a mandatory proof of vaccine requirement.

(d) Consent in Quebec

Interestingly, the Statement indicates that "*[i]n Quebec, consent cannot form the legal basis for vaccine passports*". The Statement suggests that requesting the presentation of vaccine passports in Quebec would require that the information is necessary to achieve a specific purpose, one that is serious and legitimate.

This interpretation appears to stem from the requirements for valid consent under Section 14 of Quebec's *Act Respecting the Protection of Personal Information in the Private Sector*,[8] which states:

> *"14. Consent to the collection, communication or use of personal information must be manifest, free, and enlightened, and must be given for specific purposes. Such consent is valid only for the length of time needed to achieve the purposes for which it was requested.*
>
> *Consent given otherwise than in accordance with the first paragraph is without effect."*

However, if it is possible for an individual to know the purposes for which they are presenting their vaccine passport and the uses that will be made of their personal information (for example, to permit the individual to travel or enter an event venue), it seems to be a stretch to conclude absolutely that consent cannot form the legal basis for vaccine passports in Quebec. While consent may not be valid in respect of uses unknown to the individual, that complication would not be unique to Quebec.

(e) Evidence of Vaccine Effectiveness

In connection with the discussion of necessity, effectiveness, and proportionality, and the legal authority for the introduction of vaccine passports, the Statement includes the following:

> *"So far we have not been presented with evidence of vaccine effectiveness to prevent transmission, although members of the scientific community have indicated that this may be forthcoming."*

The effectiveness of vaccines is a relevant consideration for justifying the collection and use of the personal information contained in a vaccine passport for such purposes as currently contemplated by governments and businesses.

However, the determination of vaccine effectiveness based on scientific evidence is a matter for Health Canada and public health officials, rather than the Privacy Commissioners, who have no expertise in the field (or jurisdiction to make such determinations). Before authorizing a vaccine, Health Canada must assess the scientific and clinical evidence to determine (among other things) if a vaccine is effective, with difficult decisions to be made in the midst of a global health crisis. It is not clear why the Statement suggests that there is any role of a privacy regulator to make a potentially conflicting determination as an adjunct to a privacy evaluation. Comity between regulators would suggest deference generally, and especially during a health crisis.

Further evidence of vaccine effectiveness based on real life use may be forthcoming, but, in the meantime, government and public health officials in Canada claim that all COVID-19 vaccines in Canada are "effective", "saving lives", and that they provide protection for the vaccinated person and the community around them. In the context of a public health emergency, public health orders and recommendations to protect the public are often based on evolving evidence. As such, any suggestion that it is necessary to wait for further evidence of vaccine effectiveness in order to solidify the privacy law analysis around the necessity of vaccine passports, particularly in the face of the current evidence of vaccine effectiveness espoused by the relevant authorities, could have an unintended detrimental impact on the timing of pandemic recovery efforts.

(f) Trust

The Statement references "trust" as a requirement for vaccine passport programs under consideration. The Statement suggests that for vaccine passports introduced by and for the use of public bodies, consent alone is not a sufficient basis upon which to proceed under existing public sector privacy laws.

While the basis for trust as a requirement is not anchored in the text of current Canadian privacy law, it has been considered in the broader policy context of privacy laws as relating to the relationship between individuals and government. In its reference document published in 2010 titled "*A Matter of Trust: Integrating Privacy and Public Safety in the 21st Century*"[9], the OPC stated:

> "*Without privacy, without protective boundaries between government and citizens, trust begins to erode. Good governance requires mutual trust between state and citizen. Otherwise, alienation and a sense of inequality begin to spread, circumstances under which no program for public security can be tenable or effective in the long term. Where citizen trust hits a low point, in fact, such security measures may be undermined, ignored, circumvented — or in the most egregious cases — passively or actively resisted*."

Nevertheless, the Privacy Commissioners' emphasis on trust alongside consent, as a privacy concept, is noteworthy.

[***Daniel G.C. Glover*** *is a Partner at McCarthy Tetrault in Toronto. He is national co-lead of the Cyber/Data Group and a member of the Intellectual Property, Privacy, Technology, Consumer Products & Retail Group, Franchise & Distribution, and Appellate Groups. Daniel has significant experience in all aspects of information law. He can be reached at dglover@mccarthy.ca.*

Michael Scherman *is an associate at McCarthy Tetrault in Toronto in the Technology Law and Cyber/Data Group. Michael has deep experience in providing practical legal solutions across a broad range of technology-related transactions, including in relation to privacy, technology outsourcing, cloud services, licensing, joint development arrangements, e-commerce, data sharing, distribution agreements and competitive/public technology procurements. He can be reached at mscherman@mccarthy.ca.*

Dana Siddle *is counsel at McCarthy Tetrault in Vancouver in the Business Law and Technology Law groups. Dana advises on complex commercial transactions and projects involving technology and intellectual property. Dana also supports clients with practical, solutions-oriented advice on challenges and strategies relating to e-commerce, data security, privacy, anti-spam, advertising and emerging technologies. She can be reached at dsiddle@mccarthy.ca.*

Grace Waschuk *is an associate at McCarthy Tetrault in Calgary in the Litigation Group. She maintains a broad corporate commercial litigation practice, focusing on areas including financial services, privacy and commercial leasing litigation. Grace also regularly provides strategic advice to clients including retail, consumer product and technology companies on issues relating to privacy and regulatory compliance. She can be reached at gwaschuk@mccarthy.ca.*

Jennifer Choi *is an associate at McCarthy Tetrault in Vancouver in the Litigation Group. Her practice focuses on commercial dispute resolution and arbitration, including contractual disputes, life sciences and other intellectual property disputes, construction disputes, consumer class actions, environmental prosecutions, and information and privacy law. She can be reached at jchoi@mccarthy.ca.*]

---

1 This article previously appeared as a blog post on mccarthy.ca on May 27, 2021 at: https://www.mccarthy.ca.

2 Office of the Privacy Commissioner of Canada, "Joint Statement by Federal, Provincial and Territorial Privacy Commissioners", *Privacy and COVID-19 Vaccine Passports* (May 19, 2021), online: https://www.priv.gc.ca/en/opc-news/speeches/2021/s-d_20210519/.

3 Office of the Privacy Commissioner of Canada, "Guidance on inappropriate data practices: Interpretation and application of subsection 5(3)" (May 2018), online: https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gd_53_201805/

4 *AT v Globe24h.com*, [2017] 4 F.C.R. 310, 2017 F.C.114.

5 Peter Zimonjic and Chris Hall, "Hajdu says Canada will come up with 'certification' to allow COVID-clear Canadians to travel again", *CBC News* (May 1, 2021), online: https://www.cbc.ca/news/politics/covid-passports-vaccination-international-travel-1.6009840

6 *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5, Schedule 1.

[7] Office of the Privacy Commissioner of Canada, "Guidelines for obtaining meaningful consent" (May 2018), online: https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/,

[8] *An Act respecting the protection of personal information in the private sector*, C.Q.L.R., c. P-39.1.

[9] Office of the Privacy Commissioner, "A Reference Document from the Officer of the Privacy Commissioner of Canada", *A Matter of Trust: Integrating Privacy and Public Safety in the 21st Century* (November 2010), online: https://www.priv.gc.ca/en/privacy-topics/surveillance/police-and-public-safety/gd_sec_201011/.

• VIRTUAL HEALTH CARE: NEW PRIVACY GUIDELINES AND TELEHEALTH VENDOR VERIFICATION PROCESS[1] •

Daniel Fabiano, Partner, and Heather Whiteside, Associate, Fasken Martineau DuMoulin LLP
© Fasken Martineau DuMoulin LLP, Toronto

Daniel Fabiano

Heather Whiteside

Virtual care is integral to Ontario's health system, particularly now amid efforts to slow the spread of COVID-19. To support the safe and secure use of virtual care, the Information and Privacy Commissioner of Ontario has released new guidelines for the health care sector: Privacy and Security Considerations for Virtual Health Care Visits (the "**Guidelines**"). Relatedly, Ontario Health, the province's super-agency for health, has developed a provincial standard for virtual visit solutions (the "**Standard**") and a verification process for telehealth platform vendors that meet the privacy and security criteria laid out in the Standard.

Both health care providers and telehealth platform vendors should consider how the new Guidelines and the province's verification process will impact the way they provide virtual care services in Ontario.

GUIDELINES FROM THE INFORMATION AND PRIVACY COMMISSIONER OF ONTARIO

The Guidelines provide practical advice for health care providers to mitigate the unique privacy and cybersecurity risks posed by virtual care and to meet their obligations under Ontario's *Personal Health Information Protection Act* ("**PHIPA**")[2]. PHIPA applies to all health information custodians, whether they provide care in-person or virtually. The Guidelines also remind custodians that other statutory rules or professional duties may apply to them with respect to virtual health care delivery, in addition to PHIPA.

Enhancing Privacy and Security Accountability

The Privacy Commissioner expects custodians to take the following steps to enhance privacy and security when providing virtual health care:

- conduct **privacy impact assessments** to identify and manage specific privacy and information

ELECTRONIC VERSION AVAILABLE

A PDF version of your print subscription is available for an additional charge.

A PDF file of each issue will be e-mailed directly to you 4 times per year, for internal distribution only.

security risks associated with providing virtual care;
- develop and implement **virtual health care policies** to address how virtual health care may be provided virtually (e.g., when, how, and the purposes for which health care may be provided virtually, any conditions or restrictions in doing so, including access to personal health information restricted to need-to-know access);
- **notify patients** about those virtual care policies;
- ensure employees and agents participate in ongoing **privacy and security training** to reduce the risk of unauthorized collection, use and disclosure of personal health information (including guidance specific to working from home);
- develop an **information security management framework** to monitor, assess, and mitigate any security risks associated with virtual platforms – which would set out all of the required administrative, technical, and physical safeguards expected of employees, other agents, and any electronic service providers (e.g., access controls, maintain audit logs, regularly monitor for and apply software updates, and conduct regular audits and threat risk assessments); and
- have a **privacy breach management protocol** in place for responding to actual and suspected privacy breaches related to the virtual care solution (or otherwise).

Safeguards to Protect Personal Health information

The Guidelines require that custodians put in place appropriate safeguards to protect personal health information when health care is provided virtually, which may include:

- **technical safeguards**, such as using firewalls or protections against software threats and encrypting data on all portable storage devices;
- **physical safeguards**, such as keeping technology that contains personal health information in a secure location; and
- **administrative safeguards**, such as explicit provisions in confidentiality agreements with employees and other agents which address their obligations when delivering virtual health care.

Custodians should consider further platform-specific safeguards when communicating personal health information by email, videoconference, or through patient portals.

Additional safeguards for email communication may include providing notice in the email that the information received is confidential, communicating from professional rather than personal email accounts, and providing instructions to follow if an email is received in error. Custodians should use encryption for emails to and from patients and when emailing personal health information to other custodians.

When engaging in virtual care via videoconference, custodians and patients should join the videoconference from private locations using a secure internet connection. The custodian should confirm that the meeting is secure from unauthorized participants and verify the identity of the patient. If others are present with the patient or if the visit will be recorded, the custodian should have the patient's consent.

With respect to patient portals, custodians must ensure that the privacy safeguards in place are relevant to the functionality or type of platform. This includes developing a procedure for the patient's initial access and subsequent logins and implementing access controls if the patient would like to share information with a substitute decision-maker, employer, or insurance company through the portal. Custodians should clearly explain to patients the type of information that is available in the portal, to whom it is accessible, when information provided by the patient will be reviewed by the custodian, and how long information will remain in the portal.

Selecting Virtual Platform Vendors

The Guidelines encourage custodians to consult Ontario Health's new provincial Standard when procuring a virtual visit solution to ensure it complies with privacy, security, interoperability, and technical

specifications. The Standard and its associated verification process are discussed below.

If custodians engage third-party service providers, it is important to ensure that written contracts containing appropriate privacy and data security clauses are in place. This will ensure that the custodian is itself meeting its own obligations under PHIPA by ensuring that its service provider is taking suitable steps to address PHIPA's requirements.

The Privacy Commissioner has also cautioned against engaging a virtual care solution that requires, as a condition of service, that individuals register with the service provider or accept terms of service and privacy policies that require the handling of personal health information for purposes unrelated to the provision of health care. If a solution does require that the individual have such a direct relationship with the service provider, we recommend that this be assessed in light of the circumstances of the solution, including the patient user's expectations and options for receiving care.

Engaging in Virtual Care

Before engaging in virtual care, custodians should determine whether virtual care is appropriate in the circumstances. This determination involves considering the patient's needs and the purpose of their visit, regulatory guidance, ease of access for the patient, technological requirements, and the custodian's ability to protect the privacy and security of the patient's personal health information in the virtual setting.

In circumstances where virtual care is appropriate and proper safeguards are in place, custodians should still inform their patients of the limitations and risks of virtual care visits. Custodians must have the patient's consent to collect, use, and disclose personal health information through virtual care technologies. Custodians should record virtual patient interactions in the same manner as in-person interactions.

After engaging in virtual care, custodians are encouraged to seek feedback from patients to confirm that they feel comfortable using the digital platforms.

ONTARIO HEALTH'S VIRTUAL VISIT SOLUTION STANDARD AND VERIFICATION PROCESS

Ontario Health's provincial Standard, developed in collaboration with the Ministry of Health and OntarioMD, outlines functional and non-functional requirements for virtual visit solutions used by health care providers. Vendors whose virtual visit solutions meet the criteria set out in the Standard may apply for verification by Ontario Health.

Using a verified solution gives health care providers additional privacy, security, interoperability, and technical assurances and also offers opportunities for provincial program funding.

The Virtual Visit Solution Standard

The Standard provides a comprehensive list of general requirements, privacy and security requirements, and data requirements that apply to all virtual visit solutions. For example, all virtual visit solutions must enable identity verification of the provider and user, provide for the automated verification of patient OHIP numbers, and seamlessly integrate with health care providers' existing point-of-sale (POS) systems.

In terms of privacy and security, virtual visit solutions must publish a notice of their relevant information practices, provide an electronic audit trail of all visits, and ensure virtual visit data is held by systems located in Canada, among other requirements. The minimum data requirement for all virtual visit solutions is an event summary that provides information about the organization, solution, modality of each unique virtual visit, and the day and time it occurred.

The Standard also provides requirements that are specific to either videoconferencing or secure messaging platforms. For example, video solutions are expected to enable scheduled and unscheduled visits, allow users to share files, and provide an audio-only option. Secure messaging solutions must support bidirectional communication between patients and one or more clinicians, ensure secure messaging services are only accessible by authenticated users,

and separate clinical and administrative messages, among other requirements.

The Vendor Verification Process

A virtual visit solution vendor must satisfy all mandatory requirements set out in the Standard in order to be designated as a verified solution by Ontario Health.

Vendors who wish to become verified must complete an application process which includes the following:

1. self-attestation that the solution meets all mandatory virtual visit solution standard requirements for video, secure messaging, or both;
2. summary of the vendor's Privacy Impact Assessment and Threat Risk Assessment, completed within the last two years, showing no significant outstanding risks;
3. completion of the legal terms and conditions associated with becoming a verified solution; and
4. agreement to participate in additional risk-based verification testing within one year of engaging in the verification process.

Ontario Health publishes a list[3] of verified solutions online to assist health care providers in selecting vendors. To date, four vendor solutions have been verified for the provision of video and secure messaging services and two vendor solutions have been verified for only video services.

Ontario Health verification is not a legal requirement to offer telemedicine solutions in Ontario. Ontario Health notes that verification should not be taken as an endorsement of any virtual care platform or service model. Health care providers are still advised to conduct their own due diligence in determining which solution meets their needs.

LOOKING AHEAD

Health care providers engaged in virtual care should assess their current practices to confirm that they align with the Privacy Commissioner's Guidelines. They may also wish to explore whether their current or prospective virtual care platform vendor is verified by Ontario Health.

Platform vendors should consider applying to become verified through Ontario Health's voluntary verification process.

[***Daniel Fabiano*** *is a Partner at Fasken in Toronto. A leading lawyer in the firm's Health Group, Daniel advises health sector organizations on privacy, freedom of information, technology and procurement matters. He can be reached at dfabiano@fasken.com.*

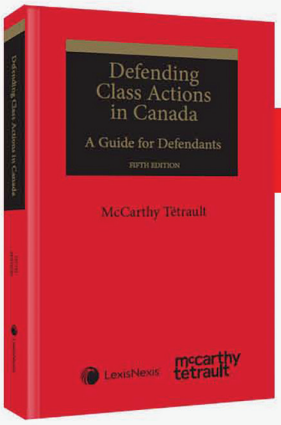
Heather Whiteside *was called to the Bar in June 2021 after completing her articles at Fasken. She will be returning to the Firm as an associate in the fall. Heather can be reached at hwhiteside@fasken.com.*]

---

1 This article was first published in Fasken's Privacy and Cybersecurity Law Bulletin (April 12, 2021).

2 *Personal Health Information Protection Act*, S.O. 2004, c. 3, Sch. A.

3 Ontario Telemedicine Network, "Verified Virtual Visit Solutions for Providers", *Virtual Care for Providers*, online: https://www-origin.otn.ca/providers/verified-solutions.



NEW EDITION

AVAILABLE DECEMBER 2019

$205 | 384 pages | Softcover

ISBN: 9780433503422

Defending Class Actions in Canada: A Guide for Defendants, 5th Edition

McCarthy Tétrault & Jill Yates

This publication is Canada's top resource for enterprises exposed to potential or actual class actions and for the lawyers who represent them.

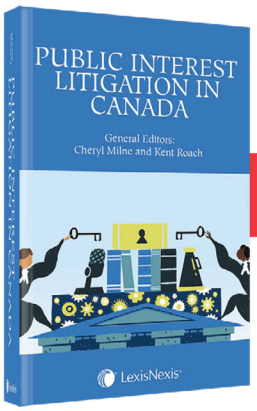
What's New In This Edition

- Commentary on forthcoming legislative changes based on the Law Commission of Ontario's July 2019 report
- Updated discussion on Financial Services Related Claims including revised commentary on Fee Disclosure Cases as well as a new subsection on Duty to Inform
- Significantly revised discussion on Competition Claims and "umbrella purchasers" with reference to *Godfrey v. Sony Corp.*
- Commentary about mass tort claims for torts occurring outside of Canada with reference to *Das v. George Weston Limited*
- New subsection on class actions based on Misclassification of Employees as Independent Contractors and Workplace Harassment and Discrimination
- Significantly revised discussion on Data Breach related class actions and new section on comprehensive risk-management strategy for businesses
- Significantly revised discussion on Global Classes and Absent Foreign Claimants including commentary on the Airia Brands test as well as *Forum Non Conveniens*
- Detailed discussion on the evolution of Third-Party Funding including considerations for Defendants and comparisons of the Certification Analysis in the US and Canada

LexisNexis.ca/ORStore

LexisNexis®

LexisNexis®



NEW PUBLICATION

PUBLIC INTEREST LITIGATION IN CANADA

This new text edited by **Cheryl Milne** and **Kent Roach** presents an overview of theories and strategies for public interest litigation and the various avenues and methodologies that have been used in Canadian history. It also examines its development since the introduction of the *Charter*, challenges and successes, procedural issues, the role of intervenors and its social impact.

The volume is broken down into four parts, with each part comprising long analytical essays and a few case comments.

The Collection of Papers

- Part I: Overarching Themes and Strategies in Public Interest Litigation in Canada
- Part II: Procedural and Technical Issues
- Part III: Interventions
- Part IV: Case Studies

AVAILABLE APRIL 2019

$120 | 464 pages | Softcover | ISBN: 9780433499008

advancing what's possible

LEXISNEXIS.CA/ORSTORE