Information and Privacy
Commissioner of Ontario
Commissaire à l'information et à la
protection de la vie privée de l'Ontario

September 4, 2024 ***VIA EMAIL***

Paul Pirie, Director (Acting), Digital Health Program Branch
Digital and Analytics Strategy Division
222 Jarvis Street, 7th Floor
Toronto ON M7A 0B6
Ministry of Health | Ministry of Long-Term Care
Email: digitalhealthprogrambranch@ontario.ca

Dear Mr. Pirie:

RE: Proposed regulations impacting individual access to electronic health records, establishing a digital identity ecosystem and other new digital health-related tools

INTRODUCTION

As Ontario's Information and Privacy Commissioner, I am mandated to protect individuals' privacy and access to information rights. Among other things, my role involves offering comment on the privacy protection implications of proposed legislative schemes or government programs.

In that capacity, I am writing regarding proposed regulatory amendments (the Proposal or the Proposed Regulations) contained in the July 6, 2024 edition of the Ontario Gazette that would amend the General Regulation O. Reg 329/04 under the *Personal Health Information Protection Act, 2004* (PHIPA).[1] The Proposal seeks to introduce separate but related programs aimed at providing individuals access to various digital health resources, including certain personal health information (PHI) held in the provincial Electronic Health Record (EHR). A central component of this broad initiative is a digital identity ecosystem that depends on the collection and use of Ontarians' PHI within a new database. The Proposal also introduces a new model of health care delivery by digital means. These are discrete but significant amendments.

The premise underlying the Proposal is simple and something IPC strongly supports: enabling easy, secure and meaningful access to one's own health records. Empowering Ontarians' right of access to their PHI is one of the core purposes of PHIPA.[2] It allows individuals to better manage their health and, in turn, helps create efficiencies in the system. These are laudable policy goals. Unfortunately, the Proposal, as currently conceived, will not achieve these goals, and may run directly counter to them for the following reasons:

---

[1] Amendment of Regulation O. Reg. 329/04 (General) under the *Personal Health Information Protection Act, 2004* (PHIPA) to provide validation, verification and authentication services and support access to personal health information held in the electronic health record (EHR) 24-HLTC020.

2 See s. 1(b) of PHIPA: "The purposes of this Act are…to provide individuals with a right of access to personal health information about themselves, subject to limited and specific exceptions…."

1. **The Proposed Regulations contain several obstacles to easy and meaningful access, including being exclusionary by design and practical effect.** The Proposal appears to be driven by technology limitations and other operational constraints that impede the right of access, instead of the "privacy by design" principles we strongly recommend should guide and enable access. The result is likely to amplify inequities among Ontarians by creating two-tiered access to PHI in the EHR: one for those who can use the proposed digital access, and another yet unknown method of access for those who cannot.

2. **The Proposed Regulations depend on creating a "digital identity ecosystem" without the requisite up front planning and design.** The ecosystem being suggested here does not meet the conditions set out by the Federal, Provincial and Territorial Privacy Commissioners in their 2022 Resolution on Ensuring the Right to Privacy and Transparency in the Digital Identity Ecosystem in Canada (FPT Resolution).[3] Instead, it relies on the persistent collection, use and disclosure of one's health card number (among other sensitive identifying information) between a multitude of private and public sector actors, without clear lines of accountability, and without any access or correction rights. This model requires more careful consideration, development and transparency than exists within the Proposal.

3. **The Proposed Regulations assign the operation *and* oversight of this ecosystem to Ontario Health without the commensurate level of accountability and oversight for the agency.** As the province's centralized health care agency, Ontario Health will be conferred a whole new function, separate from its many other existing mandates. The Proposal also converges the distinct mandates of Ontario Health in a way that muddles what it (and others) will be doing with people's PHI and for what purposes. As a result, it lacks the necessary clarity to ensure proper accountability and does not provide for independent oversight.

4. **The Proposed Regulation introduces a new model of health care delivery through new digital tools** (i.e. "Approved Digital Health Resources"). This significant shift in how individuals receive health care and interact with the health care system requires much more careful consideration to ensure the necessary level of accountability, transparency and independent oversight.

5. **The Proposed Regulations lack consistency and coherence with PHIPA**. They seem unduly rushed and awkwardly tacked onto the PHIPA framework without the necessary reflection and careful analyses needed to ensure consistency and coherence. The result is a complex and confusing set of rules that will be difficult to implement in practice, let alone provide appropriate oversight and accountability.

---

[3] See Ensuring the Right to Privacy and Transparency in the Digital Identity Ecosystem in Canada: Resolution of the Federal, Provincial and Territorial Privacy Commissioners and Ombuds with responsibility for privacy oversight (September 20-21, 2022) (accessed August 8, 2024)(FPT Resolution). The Resolution defines "Digital identity ecosystems" as interconnected systems involving public and private sector organizations that agree to follow common rules for managing the exchange and verification of digital identity information.

In addition to these broad policy concerns, there are key operational pieces that remain to be completed *before* such a scheme can be codified in regulation. These include Privacy Impact Assessments (PIAs) and Threat and Risk Assessments (TRAs) for the many moving parts underlying the Proposal. These are essential assessments that should serve to identify and address any potential risks to any new data-driven program—and they need to be done before, not after, drafting regulation. The IPC recommends that the Ministry of Health (Ministry) reconsider its Proposal once these assessments have been completed to consider their findings and recommendations, as well as our feedback below. At that point, we would be pleased to re-engage with the Ministry in a proper and timely consultation to help ensure the next set of regulations are drafted in a manner that enables, rather than undermines, the desired policy objectives.

BACKGROUND

A. The Electronic Health Record (EHR) and the Right to Access

The EHR was established as a distinct record set to enable custodians (i.e. health care providers) to collect, use and disclose PHI for the purposes of providing care.[4] The EHR currently comprises several repositories including those for lab tests, drug records, diagnostic imaging, and clinical notes.[5] As the Prescribed Organization (PO) under PHIPA, Ontario Health has the power and responsibility to develop and maintain the EHR.[6]

Part V of PHIPA governs individuals' rights of access and correction of their PHI.[7] It applies to the PHI contained in the EHR, and includes several categories of activity logs Ontario Health is required to maintain in respect of the EHR.[8] The Ministry previously proposed regulations setting out the rules and restrictions for giving effect to these rights in 2022.[9] However, those regulations never came into force. The current Proposal would strike them and replace them with the EHR Access part of the Proposed Regulations.

B. Overview of the EHR Access Regulations

The EHR Access part of the Proposal aims to operationalize PHIPA's EHR access provisions by enabling a "digital means of access" (DMoA) that relies on a new digital identity ecosystem referenced in the VVAS Regulation part of the Proposal.[10] That is, a person must *successfully*

---

[4] See ss. 55.1(1) of PHIPA. Part V.1 and its corresponding regulations came into force on October 1, 2020. See O. Reg 329/04, ss. 18.1-18.11.

[5] Referring to the Ontario Laboratories Information System (OLIS), Digital Health Drug Repository (DHDR), Diagnostic Imaging Common Service (DI CS), Acute and Community Clinical Data Repository (acCDR) which are repositories that compose Ontario's EHR. It unclear if/when information from EHR's fifth repository, the Provincial Client Registry which supports patient identification and linking of digital health records, would be made available to individuals.

[6] See ss. 55.2(1) of PHIPA.

[7] See ss. 51-55 of PHIPA.

[8] See ss. 55.3, PHIPA, paragraphs 4, 5 and 6.

[9] See Ontario Gazette Vol. 155-06, pages 377-382 (accessed August 8, 2024). See PHIPA Regulations at ss. 18.1.1 and ss. 18.1.2.

[10] See supra note 6. The "digital means of access" is a key reference in the Proposed Regulations but it is undefined. We understand this to refer to a Provincial Patient Viewer (PPV). See VVAS Regulations, s. 7, ss. 25.1(3)(d).

employ the digital identity ecosystem, which confirms their identity, in order to access their records in the EHR. To do this, a person must first meet certain eligibility requirements.[11] Then, a person must successfully confirm their identity through a two-step process of validating their health card information and digitally comparing a "selfie" with the photo on their health card.[12] This process, if successful, would lead to creating an "Ontario Health Account" – a persistent digital health identity that would be used like a key for subsequent authentication by the DMoA.[13] Initially, this access will be limited to a small "user-testing" group. Further regulatory action will be required to enable the largest number of Ontarians to access the DMoA.

C. Overview of the VVAS Regulations

The VVAS part of the Proposal sets out a multi-actor system that will deliver digital identity confirmation services—i.e. validation, verification, authentication, and Ontario Health Account Management Services (VVAS)—between digital assets so that the providers of those tools (i.e. Ontario Health and certain approved custodians, including the Ministry) can be sure that a person is who they say they are before allowing them to access health care resources and services, including the DMoA. The component parts are complex and technical but viewed altogether, they create a "digital identity ecosystem" with Ontario Health at the center.

Part I: IPC Comments on the EHR Access Regulations

A. The Proposal does not create equitable means of access for all Ontarians

Our overarching concern about this proposed model is its exclusionary nature. By design, the DMoA model will only be available for some, not all Ontarians.[14] As examples, Ontarians will be excluded from this DMoA if they are under 16; if they lack access to technological devices; if they do not have a health card with a picture ID; and if they lack the capacity to consent to the collection, use or disclosure of their PHI. None of these individuals could create an Ontario Health Account and therefore access their EHR-based PHI using the digital identity ecosystem.

The EHR Access Regulation allows for an "alternative process" for all those who cannot (or are unwilling to) access their records through the DMoA/Digital Identity Ecosystem[15], but we are unclear what that alternative process will be other than that it will be developed at some point in the future.[16] This appears to create two levels of access, at least initially: one for those who meet

---

[11] See VVAS Regulations, s. 7, ss. 25.1(4).
[12] See VVAS Regulations, s. 3 and s. 4, which create authorities for the collection and disclosure of health numbers.
[13] See VVAS Regulations, s. 7, ss. 25.1(3)(b) and (e).
[14] The Ministry has indicated it will expand eligibility in the future but the EHR Access Regulation contains no suggestion to this effect while simultaneously being "forward-looking" in other areas. As such, we assume no plans are forthcoming.
[15] See the EHR Access Regulation, s. 1(1) - Application of s. 51(5) of the Act, para. 2, records. ss. 18.1.2(4)(b), ss. (5)(b), (6), (8)(b) and s. 1(2) amending the new ss. 18.1.1(3)(b).
[16] Compare EHR Regulations, s. 1(1) - Application of s. 51(5) of the Act, para. 1, records. ss. 18.1.1(4) to EHR Regulations, s. 1(2) amending the new ss. 18.1.1(3)(b) and revoking ss. 18.1.1(4). Read together, this amendment within the same regulations is, we are told, intended to facilitate a "user-testing phase" to help test functionality of the Proposal. See reference in s. 1(1) to only "individuals specified by Ontario Health" have access to the EHR

eligibility and have the means to have an OHA to gain access to the DMoA, and another for people who will only be afforded an as-yet determined, potentially cumbersome means of access—many of whom will likely be among our most vulnerable and marginalized. All Ontarians have a right to access records of their PHI contained in the EHR. While we recognize the utility of digital solutions to enable this access, technological opportunities or limitations should not overshadow this fundamental principle. Equal priority should be given to ensuring an equivalent access by analog means for those who want or need it.

B. The Proposal removes the right to severability and terminates overall access

PHIPA provides that where a custodian refuses an individual access to their PHI based on an applicable exception, the individual retains the right to access any remaining portion of the record that can reasonably be severed from the part of the record to which the exception applies.[17]

The EHR Access Regulation would remove this right of access to one's non-restricted PHI in the EHR through the DMoA. If an exception applies to a single record in the EHR, a person's access to the EHR would be restricted in full. As we understand it, this is because the underlying technology cannot support more granular options at this time. Instead, individuals would be forced to pursue their access rights through the "alternate process" (whatever it may be) or by contacting the custodian(s) directly through the current (often paper-based) course of submitting a request, outside the EHR.

In other words, in the event one record in the EHR is restricted, the individual would have no digital access to any of their PHI in the EHR and would have to pursue a much slower non-digital means of access (insofar as they would be redirected towards other processes). As we have noted in previous comments to the Minister of Health, to block everything or block nothing is not a meaningful choice.

C. The Proposal diminishes and delays the right to access

PHIPA requires that Ontario Health, as the Prescribed Organization that operates the EHR, keep activity logs regarding the EHR.[18] Once the relevant provisions of PHIPA come into force, Ontario Health will be required to provide individuals access to these logs.[19] Under the Proposal, this requirement would be scaled back from providing access to the logs themselves to providing only "summaries" of the logs. The rationale is that the logs are technical, disparate, and not easily understood by lay readers. While this may be true for some logs, a better solution, in our view, would be to provide summaries to individuals in addition to the original logs, upon request, rather than removing access to the logs altogether. Access to the actual logs might be particularly

---

records through the DMoA. This first phase under s.1(1) does not contemplate an alternative process; instead, Ontario Health is to redirect individuals to the relevant custodian for access to their records.

[17] See ss. 52(2) of PHIPA.

[18] See ss. 55.3 paragraphs 4, 5 and 6 of PHIPA.

[19] See ss.51(5) paragraph 2 of PHIPA (not yet in force; these sections are intended to be called into force alongside the Proposed Regulations).

important for individuals who have signed a consent directive, for example, and want a more detailed account of who accessed their EHR, when and for what purposes.

Furthermore, the EHR Access Regulation provides Ontario Health up to 90 days, with the possibility of an extension, to provide a log's summary upon request. This is three times longer than PHIPA provides for custodians who must respond to an access request within 30 days. The Proposed Regulation does not impose a deadline for responding to an access request so that a deemed refusal may be triggered if the deadline is not met, such as exists for custodians when they fail to respond within their prescribed time limit. Also, the Proposal would only require Ontario Health to provide log summaries dating back 12 months prior to the request. The result of all of these regulatory choices, collectively, amounts to serious incursions into an individual's right of access to their PHI contained within the EHR, and reduces overall transparency of the system.

D. The Proposal limits eventual access to all clinical data in the EHR and undermines the opportunity for meaningful access to one's health records

As mentioned above, there are currently four clinical data repositories within the EHR: labs, drugs, diagnostic imaging, and clinical reports. However, only the labs and drugs repositories are captured by the Proposal. This approach deviates from the *phased-in* approach to the four repositories that exists in the current as-yet-proclaimed regulations.[20] This narrowing of future access is especially striking when one considers several other phased-in and future-state oriented pieces of the Proposed Regulations.[21] We see no rationale for not maintaining the same extended timelines for *eventual* access to all clinical repositories as already exists, albeit not in force.

Absent access to one's full clinical, the opportunity for empowering individuals to manage their health care (with corresponding health system benefits) is not likely to be meaningful. This is especially true when accounting for the fact that the planned access to labs and drugs may only provide a marginal improvement to what Ontarians can already access through existing digital channels.[22]

Part II: IPC Comments on the VVAS Regulations

A. A digital identity ecosystem should adhere to certain foundational conditions

Digital identity ecosystems can be tools to modernize public services—such as being proposed here—but they also pose significant privacy, security, transparency and accountability concerns given their role of transmitting someone's identity between services and relying on that identity to access them. Recognizing these risks, in 2022, the IPC, together with its Federal, Provincial and Territorial counterparts, adopted a Resolution (Ensuring the Right to Privacy and

[20] See ss. 18.1.1(3) of O. Reg 329/04.
[21] See e.g. footnote 16. Also, under the VVAS Regulations, the Approved Digital Health Resource "digital front door" regime is introduced though not intended to be operational at the outset. See s. 25.3.
[22] For example, many Ontarians can already access lab results using online portals offered by community laboratories, such as LifeLabs or Dynacare.

Transparency in the Digital Identity Ecosystem in Canada)[23]. As part of the Resolution, regulators from across Canada recognized the potential benefits of a secure, privacy-protective, digital identity. However, we emphasized that to be trusted and widely adopted, digital identities and the ecosystem in which they are used must meet high standards that honour the rights implicated; without which, the benefits cannot be realized.

We then set out a non-exhaustive list of conditions and properties every digital identity ecosystem should possess including, as examples, being the subject of a completed privacy impact assessment that has been provided to the oversight body in the *early design* phase; offering alternative forms of identification which are convenient and accessible as well as offering options and alternatives that ensure fair and equitable access to services for all; only collecting, using, retaining or sharing the minimum amount of personal health information needed to confirm an individual's identity; and, not using the information to create any central databases. These systems must be secured from identity theft, fraud and other harms and must not allow tracking or tracing of credential use for other purposes. Most importantly, governments and organizations must be held accountable for their use and subject to independent oversight.

It is not clear whether and how the current Proposal that purports to create a new digital health identity ecosystem can meet these and other foundational conditions the FPT Resolution calls for, and which are critically important to ensure public trust.

B. A new, centralized, data repository raises security, privacy and access concerns

The VVAS Regulations create a central database that holds individuals' Ontario Health Accounts (OHAs) and the PHI used to substantiate them. The OHA holds PHI including people's health card numbers and dates of birth because, we are told, this PHI is necessary to enable an individual's access to the universe of digital health services that exist behind it. This raises several concerns. First, as a matter of privacy, it is not clear that the health card number *must* be used or retained in this way to connect individuals to their records. The IPC believes other means may be able to achieve the same purposes without the associated privacy risks. Also, the IPC understands offshore actors will be engaged to resolve individuals' failures to verify, validate and/or authenticate their credentials. It is not clear how privacy and security will be assured to mitigate the risks of involving third parties, particularly in other jurisdictions.

Second, on the issue of access, the VVAS provisions do not incorporate Part V of PHIPA. As a result, there is no individual right to access their records of PHI held in the VVAS database, including who is viewing/ handling/dealing with their PHI, circumventing their ability to submit complaints, where appropriate, to my office.

C. Ontario Health's new function is improperly converged with its other roles

The VVAS Regulations give Ontario Health a new function to operate (through others) and oversee the digital identity ecosystem without the commensurate level of accountability and transparency and independent oversight we believe are required. Nor does the Proposal consider

[23] See footnote 3.

Ontario Health a custodian for purposes of this new function—though there are several references to it functioning as if it were one, and maintaining custody or control of PHI, albeit inconsistently[24]. The opacity creates confusion about under which function, and for what purpose(s), PHI will be collected, used and disclosed.

Further, the VVAS Regulations recognize Ontario Health *simultaneously* serving different functions – as operator/overseer of the digital identity ecosystem; as Prescribed Organization developing and maintaining the EHR; and as Prescribed Person for purposes of certain data registries – while blending the authorities with which it operates them. This adds to the conflation, complexity and confusion of its roles and functions. For instance, the Proposed Regulations permit Ontario Health to "use" the OHA and other PHI in the new data repository as a Prescribed Person under of 39(1)(c) of PHIPA, for the purposes of providing certain digital correspondence to Ontarians (e.g. cancer screening letters).[25]

The Proposed Regulations should clearly articulate the authority under which Ontario Health operates, its various functions, and an oversight model that is commensurate with this potentially complex meshing of functions and the quantity of sensitive PHI involved. No organization, including Ontario Health, should be enabled to handle such large quantities of sensitive information without these core components.

D. A new model for provision of health care should not be introduced by PHIPA regulation

The VVAS Regulations go far beyond facilitating access to one's electronic health records. They introduce a wholly separate concept—digital tools referred to as "Approved Digital Health Resources" (ADHRs)—to facilitate the provision of health care digitally.[26] The VVAS Regulations set out an approval scheme for ADHRs whereby Ontario Health together with the Ministry of Health would set eligibility requirements, which impose contracting requirements and other obligations,[27] but provides no clear model of oversight and accountability for these new tools and the actors who operate them. Furthermore, our understanding is that the Ministry will be the first such approved custodian to operate an ADHR, setting up a self-approval scheme that raises further concerns about transparency, accountability and independence.

ADHRs would represent a significant shift in how individuals receive health care and interact with the health care system. It also invites different levels of access depending on who can and cannot access these tools considering exclusionary design choices identified above. ADHRs as vehicles for health care delivery are being through mere subsection reference in a regulation attached to a

---

[24] See VVAS Regulations, s. 4, which amends s. 12 of O. Reg 329/04 (governing the disclosure of health number by prescribed parties) to state: "The Agency or its agents may disclose a health number that it has custody or control of for the purpose of providing validation and verification services or authentication services in accordance with this Regulation..." (emphasis added). See also the reporting obligation on Ontario Health in the event of theft, loss or unauthorized use or disclosure including when there is a pattern of such behavior related to PHI "in the custody or control of the Agency," para. 4 of ss. 25(4). Compare with the provisions in the main authorizing section of the VVAS Regulation, ss. 25.1(1), (2) and (3) (which contain no references to custody or control).

[25] See VVAS Regulations, ss. 25.1(3)(e).

[26] See VVAS Regulations, s. 1, "Digital Health Resource."

[27] See VVAS Regulations, ss. 25.3.

privacy law.[28] This fundamental shift in health care delivery deserves much fuller consideration and transparency.

Part III: General Lack of Consistency and Coherence with PHIPA

Read altogether, the Proposed Regulations seem as though they were unduly rushed and awkwardly tacked onto the PHIPA framework without the necessary reflection and careful analyses needed to ensure consistency and coherence. The result is a complex and confusing sets of rules that will be difficult to implement in practice, let alone provide oversight and accountability. For example, the Proposed Regulations:

- Import several but not all requirements from the service provider provisions under the existing regulations,[29] and applies them to the "Approved Health Information Custodian" who will provide the ADHRs. In addition, conceptually, custodians and service providers hold very different authorities under PHIPA;
- Incorporate some but not all PHIPA provisions setting out authorities and restrictions of persons acting on behalf of others (i.e. agents and service providers);[30]
- Exclude two out of the four scenarios set out in PHIPA's regulations for reporting data breaches to the IPC;[31]
- Confuse the different definitions of collection/use/disclosure under PHIPA generally and the purpose-built definitions for the EHR under Part V.1;
- Blur the application of the reasons health care providers may refuse access under PHIPA by creating a hazy and confusing back-and-forth between custodians and Ontario Health about when and how that part of the access regime applies and,
- Incorporate and exclude different Parts and provisions of PHIPA, when in fact, they are all ultimately meant to dovetail.

CONCLUSION

In closing, the full picture of the Proposed Regulations reveals a proposal that is rushed, problematic and incomplete. While the underlying objectives are noble and important, we recommend that the Ministry not proceed with its current Proposal until it has completed its PIAs/TRAs and appropriately addressed the findings and recommendations arising therefrom. More time and careful thought is needed to reconcile many of the concerns we raise above and simplify the Proposal in a manner that protects Ontarians' privacy, facilitates easy and meaningful

---

[28] See VVAS Regulations, s. 1, "Digital Health Resource," which is a provincially-funded health resource that …
"(a) is provided by a health information custodian for use by individuals, and
(b) enables a health information custodian to:
(i) use electronic means to collect, use, modify, disclose, transmit, maintain, or dispose of personal health information for the purpose of providing health care or assisting in the provision of care, or
(ii) allow individuals to access, use, disclose, maintain, or otherwise manage their records of personal health information (emphasis added)."

[29] See s. 6 of O. Reg 329/04.

[30] See s. 25.4 of the VVAS Regulations, which imports s. 17 of PHIPA but with "necessary modifications," making it unclear what responsibilities do and do not apply. It also excludes ss. 10(4) and 37(2) (where a service provider or agent is permitted to use PHI on behalf of custodian).

[31] See s. 6.3 of O. Reg. 329/04.

access to their EHR, and enhances transparency and accountability of the digital ecosystem being proposed.

For the IPC's part, we stand ready to continue consultation with the Ministry of Health and Ontario Health to advance this ambitious proposal.

In the spirit of openness and transparency, I am providing a copy of this letter to the Ministry of Health, as well as the Chief Executive Officer of Ontario Health. I will also post this letter publicly on my office's website.

Sincerely,

Patricia Kosseim
Commissioner

c. Michael Hillmer, Assistant Deputy Minister, Digital and Analytics Strategy Division
Christine Sham, Director, Information Management Strategy and Policy Branch
Matthew Anderson, Chief Executive Officer, Ontario Health
Sylvie Gaskin, Chief Privacy Officer, Ontario Health
Michael Maddock, Assistant Commissioner, Strategic Initiatives and External Relations Division, Information and Privacy Commissioner of Ontario
Andrew Drummond, Director of Health Policy, Information and Privacy Commissioner of Ontario