ONTARIO NURSES' ASSOCIATION

October 21, 2026

Dafna Carr,
Associate Deputy Minister and Chief Digital Health Officer
10th Flr, 56 Wellesley St. W
Toronto, Ontario. M5S 2S3

Dear Associate Deputy Minister Carr,

Re: Amendment to Regulation O. Reg. 329/04 (General) made under the *Personal Health Information Act, 2004* (PHIPA) to Allow Additional Patient-Facing Services to Utilize the Digital Health Identifier

I am writing to you on behalf of the Ontario Nurses' Association (ONA). ONA is Canada's largest nurses' union and represents more than 68,000 registered nurses, nurse practitioners, and health-care professionals, and over 18,000 nursing student affiliates. ONA members provide care in hospitals, long-term care facilities, public health units, the community, clinics, and industry, and are dedicated to advocating for improvements in timely access to health care for all.

The Ministry of Health is consulting on proposed amendments to Ontario Regulation 329/04 (General) under the *Personal Health Information Protection Act, 2004* (PHIPA). The proposed changes would establish a framework that will enable Ontario Health to provide authentication services for approved, provincially funded digital health resources. The amendments would also define digital health resources and their providers, establish an approval process for eligible resources, and permit Ontario Health and its agents, with an individual's express consent, to disclose personal health information (PHI) to approved digital health resource providers for authentication purposes.

The proposed framework would require digital health resource providers to complete privacy and security assessments as part of the approval process. Providers would enter into agreements with Ontario Health outlining the authentication services, the PHI to be collected, and the administrative, technical, and physical safeguards in place to protect it. The amendments would also restrict how PHI obtained through authentication services can be used and disclosed. They would allow PHI to continue to be used for incident and breach management, including after an individual withdraws consent.

The proposed amendments establish a regulatory framework that enables Ontario Health to provide authentication services for approved, provincially funded digital health resources. Improved and secure access to digital health information can support continuity of care, patient engagement, and health-system integration (Ebo et al., 2025). However, the proposed amendments raise several privacy

Provincial Office
85 Grenville Street
Toronto, Ontario M5S 3A2
ona.org

Phone: 1-800-387-5580
Fax: 1-866-964-8864

concerns and implementation considerations that we urge the Ministry of Health to consider.

Consent, Transparency, and Access

PHIPA requires express consent for Ontario Health to collect or use PHI for digital health identifier activities and limits PHI to what is necessary for that purpose. For patients to provide or withhold informed consent, they must be adequately informed of the nature and extent of any ongoing or future disclosure of their information to third parties. The individual seeking consent is responsible for providing sufficient, accessible information so patients can make an informed decision. This includes ensuring that patients understand their right to provide or withhold consent.

Consent may subsequently be withdrawn; however, the proposed amendments permit previously collected PHI to continue to be used or disclosed for specified purposes, including retention, maintenance, disposal, and incident or breach management. This further reinforces our recommendation for greater transparency in communicating how patient information will be collected, disclosed and shared.

Ontarians should have the power to choose not to provide consent. Without express consent, they cannot access digital health resources through the PHI-based authentication process. Individuals should therefore clearly understand the implications of withholding consent, including how it may affect their ability to use the digital authentication process.

Privacy, Security, and Accountability

The proposed approval process includes privacy and security assessments and requires safeguards to protect PHI. These requirements are important given the sensitivity and scale of PHI accessed through provincially connected digital systems.

However, the effectiveness of these safeguards will depend on consistent implementation, ongoing oversight, and clear accountability when privacy or security incidents occur. While specific safeguards may vary by digital health resource and the PHI involved, Ontario Health should establish and consistently apply clear baseline privacy and security standards across approved resources. Ontario Health, its agents, and digital health resource providers must also clearly establish responsibilities for identifying, reporting, investigating, and responding to breaches.

Because Ontario Health approves digital health resources and reviews required assessments, it should maintain clear oversight and accountability to ensure approved providers continue to meet required privacy and security standards.

The amendments also introduce a new record-keeping requirement, directing Ontario Health to log the date an individual uses their digital health identifier to

access an approved digital health resource. This access-log data is itself PHI and should be subject to the same privacy and security safeguards, retention limits and access controls as other information collected under the digital health identifier framework.

Equity and Accessibility

Digital access can improve patients' ability to access and manage their health information; however, reliance on digital authentication may also create barriers (Charalambous, 2026; Ebo et al., 2025). Currently, individuals must have a valid Ontario photo health card and access to a mobile device and the internet to use My Ontario Account for Health (Ontario Health, 2026). Individuals with limited digital literacy, limited access to technology or reliable internet, disabilities, or other accessibility needs may experience disproportionate barriers to this delivery model (Charalambous, 2026). Alternative ways to access health information should remain available to ensure digital authentication does not unintentionally widen existing health inequities.

Outstanding Questions Requiring Additional Information

1. Who can become a digital health resource provider under these proposed amendments?

A digital health resource provider may include Ontario Health, an agent acting on behalf of Ontario Health, or a health information custodian that provides a provincially funded digital health resource. Resources not provided directly by Ontario Health or its agents must undergo Ontario Health's approval process before receiving authentication services (Government of Ontario, 2026). We need more information on what the process entails for an entity that is not Ontario Health or an agent of Ontario Health to become a digital health resource provider or a health information custodian before we can provide an informed position.

2. What PHI may be shared through the authentication process?

The proposed amendments do not prescribe a standardized set of PHI that will be shared with every digital health resource provider. Instead, the agreement between Ontario Health and the provider must identify the PHI that will be collected in respect of the digital health resource. Express consent is required before Ontario Health, or its agents may disclose PHI for authentication (Government of Ontario, 2026).

3. Does withdrawing consent require previously collected PHI to be deleted?

No. The proposed amendments permit Ontario Health, its agents, and digital health resource providers to continue to collect, use, or disclose previously obtained PHI for specified incident and breach management activities even after consent is withdrawn. The amendments also permit Ontario Health to retain, maintain, and dispose of PHI associated with digital health identifier activities

following withdrawal of consent (Government of Ontario, 2026). Patients should always retain control over their consent, including the right to withdraw consent and request the deletion of previously collected PHI.

4. Who determines whether a digital health resource is approved?

Ontario Health, in consultation with the Minister, is responsible for establishing and publishing the eligibility criteria and approval process. Providers seeking approval must submit privacy and security assessments and enter into an agreement with Ontario Health describing the resource, PHI collected, authentication services, and applicable safeguards (Government of Ontario, 2026).

5. Are approved digital health resources subject to ongoing review?

Once approved, digital health resource providers remain subject to requirements governing the collection, use, and disclosure of PHI (Government of Ontario, 2026). However, the consultation draft does not specify a process or schedule for periodically reassessing an approved resource's privacy and security safeguards. Further clarification may be beneficial as digital technologies, and cybersecurity risks continue to evolve.

Overall Assessment

The proposed amendments provide an important framework to expand secure authentication across provincially funded digital health resources. Implementation should be supported by meaningful, transparent consent; strong, consistently applied privacy and security safeguards; clearly defined oversight and accountability; and equitable access for individuals who cannot or choose not to use digital authentication. From ONA's perspective, expanding the use of digital health resources should improve access to health information and services without compromising privacy, patient autonomy, or equity. However, serious gaps exist in protecting patients PHI, particularly their ability to withdraw consent and request the deletion of previously collected information.

Thank you for the opportunity to provide feedback.

Sincerely,



Erin Ariss, RN
Provincial President
Ontario Nurses' Association

References

Charalambous, A. (2026). Assessing and ensuring accessibility of digital tools for underserved populations: A comprehensive examination of global digital equity barriers and solutions. *Measurement and Evaluations in Cancer Care, 4*, Article 100034. https://doi.org/10.1016/j.ymecc.2026.100034

Ebo, T. O., David-Olawade, A. C., Ebo, D. M., Egbon, E., & Olawade, D. B. (2025). Transforming healthcare delivery: A comprehensive review of digital integration, challenges, and best practices in integrated care systems. *Digital Engineering, 6*, *Article* 100056. https://doi.org/10.1016/j.dte.2025.100056

Government of Ontario. (2026). *Consultation draft: Ontario Regulation to be made under the Personal Health Information Protection Act, 2004, amending O. Reg. 329/04 (General).* Amendment to Regulation O. Reg. 329/04 (General) made under the Personal Health Information Protection Act, 2004 (PHIPA) to Allow Additional Patient-Facing Services to Utilize the Digital Health Identifier | regulatoryregistry.gov.on.ca

Ontario Health. (2026, June 4). *Digital health identifier: Description of activities.* Digital Health Identifier: Description of Activities | Ontario Health

Personal Health Information Protection Act, 2004, S.O. 2004, c. 3, Sched. A. Personal Health Information Protection Act, 2004, S.O. 2004, c. 3, Sched. A | ontario.ca