

Ministry of the Solicitor General

Public Safety Division
Public Safety Training Division

25 Grosvenor St.
12th Floor
Toronto ON M7A 2H3

Telephone: (416) 314-3377
Facsimile: (416) 314-4037

Ministère du Solliciteur général

Division de la sécurité publique
Division de la formation en matière
de sécurité publique

25 rue Grosvenor
12^e étage
Toronto ON M7A 2H3

Téléphone: (416) 314-3377
Télécopieur: (416) 314-4037



MEMORANDUM TO: All Chiefs of Police and
Commissioner Thomas Carrique
Chairs, Police Services Boards

FROM: Richard Stubbings
Assistant Deputy Minister
Public Safety Division and Public Safety Training Division

SUBJECT: **First Responders COVID-19 Risk Look-Up Tool Web
Portal: Protection of Personal Health Information and
Appropriate Use**

DATE OF ISSUE:	April 27, 2020
CLASSIFICATION:	For Action
RETENTION:	Indefinite
INDEX NO.:	20-0064
PRIORITY:	High

Further to All Chiefs Memos 20-0041, 20-0044, and 20-0048, I would like to provide you with important information on the contents of the First Responders COVID-19 Risk Look-Up Tool Web Portal (the portal), its appropriate use, and the urgent need to protect personal health information.

Contents of the Portal

The portal now contains confirmed positive test results (beginning on April 1, 2020) for individuals who qualified for and have undergone a COVID-19 test. An individual who is included in the portal is never removed, even if they have subsequently recovered. Policing personnel should continue to conduct point of interaction risk assessments and take other appropriate precautions when interacting with members of the public.

Please note the following considerations regarding the information contained within the portal:

- It may take up to four days for test results to become available;
- The information in the portal is only updated once a day and does not reflect real-time testing information;

- Individuals who have tested positive may no longer have COVID-19;
- An individual who is included in the portal is never removed;
- Individuals' addresses may be recorded inconsistently;
- An address for a multi-unit building may have a positive case but not at the relevant unit; and
- There may be individuals at an address who do not reside there.

The ministry continues to work to improve the portal including the quality of data available and will share further updates as available.

Use and Disclosure of Information

Over the course of the past few days, it has come to the attention of the ministry that some policing personnel have used or disclosed information in the portal in a manner that is not consistent with *Emergency Management and Civil Protection Act* (EMCPA) or the ministry's instructions. The EMCPA requires that information shared pursuant to [O. Reg. 120/20](#) *only* be used to prevent, respond to, or alleviate the effects of the emergency. The EMCPA also requires that any information-sharing authorized under the emergency order occur in a manner that limits its intrusiveness.

The portal should not be used to obtain information about employees in the police service for the purpose of managing the workforce (e.g., identifying whether an employee should remain at home or other employees who were in close contact should self-isolate). Information about employees' COVID-19 status should be obtained directly from employees where appropriate. Given the limitations of the portal, including those described above, the portal is likely a less reliable tool for identifying individuals who are COVID-19 positive than the information employees themselves can provide.

The portal is *only* intended to be used to look up the COVID-19 status of individuals that members of the police service will encounter or have encountered during the declared emergency *as a result of responding to calls for service*, for the sole purpose of supporting frontline policing personnel in making informed decisions about whether they need to take additional precautions to prevent the spread of COVID-19.

The portal must not be used to advise any individual about its contents for unauthorized purposes (e.g., *disclosures to heads of council or public health units for informational purposes*). For greater certainty, searches of the portal should not be conducted to ascertain the number of individuals in a municipality or region that appear on the portal and such information, if already obtained, should not be shared. In the ministry's view, such use of the portal is not consistent with the requirements of the EMCPA. It is imperative that police services boards and chiefs of police protect the sensitive personal health information in the portal.

Audit Logging and Accountability

The ministry has instituted an audit logging function that will track all user activity on the portal and may flag any queries that are deemed to be an inappropriate use of the portal (e.g., broad municipal-based searches). Where such inappropriate use of the portal is confirmed, the ministry may revoke access to the portal for the user who violated the terms of service or the entire group of users affiliated with the police service.

Furthermore, the ministry may report suspected unauthorized portal access or use/disclosure of information from the portal to the Information and Privacy Commissioner of Ontario. Police services board and chiefs of police should commence their own internal investigation and, where appropriate, undertake disciplinary measures for all unauthorized access, or use or disclosure of information from the portal. The ministry will, on request of a chief of police or police services board, provide a copy of an authorized user's audit logs for the purpose of investigating unauthorized access, or use or disclosure of information, for the purpose of pursuing discipline.

Please note that if a police officer misuses the portal or information from the portal, it could amount to misconduct under the *Police Services Act*. Other members of a police service could also face discipline. It is also a provincial offence for any person to willfully disclose personal information in contravention of the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA) or *Freedom of Information and Protection of Privacy Act* (FIPPA).

Retention and Record-Keeping of Information in Portal

The ministry continues to advise police service boards and chiefs of police to set default expiry dates for any alerts/flag in your computer-aided dispatch (CAD). The expiry dates should coincide with the day the declared provincial emergency ceases to be in effect. Where your police service chooses to enter "remarks" into your CAD, please ensure that personal health information is only included if necessary, and only the minimum amount of personal health information is included.

The ministry recognizes that some functionalities of CAD may automatically transfer information into your Record Management System (RMS). This information continues to be subject to applicable law during and after the declared emergency, including the MFIPPA or FIPPA.

Please note the COVID-19 status information should not be entered into the Canadian Police Information Centre (CPIC) and intelligence databases.

Police services should consult with their legal counsel to determine whether specific uses of information from the portal are permitted. The ministry encourages masking and restricting access to such personal health information as soon as practicable and no later than the conclusion of the provincial emergency.

Please be advised that policing personnel should continue to take appropriate notes in memo books in accordance with local policies and procedures, which may include information about the COVID-19 status of an individual. Furthermore, COVID-19 status information may be broadcast over your dispatch centre's encrypted radio communications system to the appropriate policing personnel to the extent necessary. The ministry recognizes that such radio transmissions will be recorded permanently and maintained for evidentiary purposes, where applicable, and in accordance with provincial legislation. Please avoid relaying any personal health information over unencrypted electronic or radio communication systems.

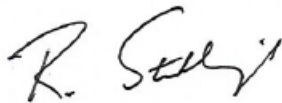
Please note, the EMCPA provides that personal information subject to an emergency order is subject to any law with respect to the privacy and confidentiality of personal information when the declared emergency is terminated.

Please refer to subsection 7.0.2(7) of the EMCPA with respect to the rules that apply to the information subject to this emergency order. Also attached is a Question & Answer document with more information on the portal, for your reference.

If you have any other questions, please contact the COVID-19 Enforcement Support Line at 1-866-389-7638.

Thank you for your continued assistance.

Sincerely,

A handwritten signature in black ink, appearing to read "R. Stubbings".

Richard Stubbings
Assistant Deputy Minister
Public Safety Division and Public Safety Training Division

Attachment