

Privacy Impact Assessment for Ministries

Contents

Before you start **Error! Bookmark not defined.**

PART 1: GENERAL INFORMATION..... 3

- 1. Describe the initiative 4
- 2. Scope of the initiative 4
- 3. Describe the information or data 4
- 4. Risk assessment for initiatives with no personal information..... 5

PART 2: PROTECTION OF PERSONAL INFORMATION..... 5

- 5. Does your initiative involve a cloud-based solution? 5
- 6. Storing personal information 5
- 7. Collection, use and disclosure 6
- 8. Collection Notice..... 8

PART 3: SECURITY OF PERSONAL INFORMATION 8

- 9. Digital tools, databases or information systems 8
- 10. Physical security 8
- 11. Technical security 9
- 12. Controlling and tracking access..... 9

PART 4: ACCURACY, CORRECTION AND RETENTION 9

- 13. Requests for correction..... 9
- 14. Decisions affecting individuals 10

PART 5: AGREEMENTS AND INFORMATION BANKS 11

15.	Does your initiative involve or will it part of a regular and systematic exchange of personal information with partners in or outside government?.....	11
16.	Does your initiative involve sharing personal information with a third party for research or statistical purposes?	11
17.	Will your initiative result in a personal information bank?	11
PART 6: ADDITIONAL RISKS.....		11
18.	Risk response.....	11
PART 7: SIGNATURES.....		14
PCT Summary		14
PCT Signatures.....		14
Ministry Signatures		15

Privacy Impact Assessment for Ministries

PART 1: GENERAL INFORMATION

PCT intake number / PIA file number: HLTH21101, MOH 2021-76

Initiative title:	BC Vaccine Card Verifier App
Ministry:	Ministry of Health
Branch or unit:	Digital Health Strategic Initiatives Branch
Your name:	Nino Samson
Your work phone:	778-974-2712
Your email:	Nino.samson@gov.bc.ca
Initiative Lead name:	Pam Smith
Initiative Lead phone:	(778) 974-2682
Initiative Lead email:	Pam.K.Smith@gov.bc.ca
Ministry Privacy Officer:	Quinn Fletcher
MPO phone:	778 698-5849
MPO email:	Quinn.Fletcher@gov.bc.ca

FOR MPO USE ONLY
Type of PIA (PI or non-PI):
PI
Is this a data-linking initiative under FOIPPA?
No
Is this a common or integrated program or activity?
No
Related PIAs, if any:
HLTH21100 - 2019-45K Health Gateway Update – Vaccine Card
Would you describe this as a high-risk or complex initiative? If yes, why?

Yes – sensitive COVID-19 related file
Briefly summarize the initiative to be published in the Personal Information Directory. This summary may be similar to the answer to question 1 below.
A BC Vaccine Card Verifier App will be available for businesses to download off the Google Play and Apple App Stores which will provide the capability to scan the citizen's vaccine card QR and validate their COVID vaccination status as "Vaccinated", "Partially Vaccinated", or "No records found".

1. Describe the initiative

To support citizens in providing proof of vaccination for non-essential services as mandated by the province of BC starting September 13, 2021, Health Gateway will provide a vaccine card which displays the citizen's COVID-19 vaccination status and a QR which can be scanned by businesses to validate the status presented.

A BC Vaccine Card Verifier App will be available for businesses to download off the Google Play and Apple App Stores which will provide the capability to scan the citizen's vaccine card QR and validate their COVID vaccination status as "Vaccinated", "Partially Vaccinated", or "No records found".

This app will be available widely for business on September 13, 2021.

2. Scope of the PIA

The scope of this PIA is limited to the use of the BC Vaccine Card Verifier App for provincial use however, the app may be able to scan QR codes from other Canadian jurisdictions that follow the [SMART Health Card specification](#).

3. Describe the information or data

The QR code presented contains the following data elements:

- Name
- Date of Birth
- Date of Vaccine

- Vaccine type
- Lot # of vaccine
- Clinic where the vaccine was received

This information has been included to align with the federal standard and to enable the use of this service for other use cases such as travel.

The BC Vaccine Checker App will allow the business to scan the QR and will only display for the business the following:

- Name
- Vaccination Status (Vaccinated, Partially Vaccinated, No records found)

3.1 Did you list personal information in question 3?

Yes.

4. Risk assessment for initiatives with no personal information

N/A

PART 2: PROTECTION OF PERSONAL INFORMATION

Part 2 asks you to think through how you will protect personal information that you collect, use, store, access or disclose.

5. Does your initiative involve a cloud-based solution?

No.

- If you answered yes, go to question 5.1.
- If you answered no, go to question 6.

6. Storing personal information

In most cases, FOIPPA requires that personal information is stored and accessed only in Canada. FOIPPA requirements are designed to reduce the likelihood that British Columbian's personal information is subject to the laws of another country.

If your initiative meets [one of three conditions](#), you may be authorized under FOIPPA to store or access personal information outside Canada.

6.1 Is all personal information stored and accessed in Canada?

No personal information will be stored.

7. Collection, use and disclosure

This section will help make sure you have the authority to collect, use and disclose personal information and that you limit your collection where possible.

Use this column to describe the way personal information moves through your initiative step by step as if you were explaining it to someone who does not know about your initiative.	MPO fills in collection, use, disclosure	MPO fills in FOIPPA authority	MPO fills in other legal authority
Step 1: Business will open app and scan QR presented by citizen. QR code is scanned.	Collection	26(a) per the Order of the Provincial Health Officer [made under s.30, 31, 32 of the Public Health Act]	Order of the Provincial Health Officer s.12(1)(h), PIPA
Step 2: The public key is hard coded into the app and is only used to read and verify the QR code, and the app displays the results to the app user. The public key is a way to verify the signature of the QR code, signed with a private key by an issuer (PHSA/Health). This confirms its authenticity. There will be no disclosure of	Use	32(a)	s.15(1)(h), PIPA

Use this column to describe the way personal information moves through your initiative step by step as if you were explaining it to someone who does not know about your initiative.	MPO fills in collection, use, disclosure	MPO fills in FOIPPA authority	MPO fills in other legal authority
<p>personal information back to PHSA or the business.</p> <p>The public keys used to verify are encoded in the verifier app, so the app does not have network connectivity to connect with a verification server. There is no database and no logging of transactions by design.</p>			
<p>Step 3: Display vaccination status for verification. Individuals over the age of 18 must also present supporting photo identification which will also be viewed and collected.</p>	Collection	26(a) per the Order of the Provincial Health Officer [made under s. 30, 31, 32 of the Public Health Act]	Order of the Provincial Health Officer s.12(1)(h), PIPA
<p>Step 4: Business or public bodies may only retain copies of proof of vaccination with individual's consent per the Order of the Provincial Health Officer.</p>	Collection	26(a) per the Order of the Provincial Health Officer [made under s. 30, 31, 32 of the Public Health Act]	s.7, 12(1)(h) PIPA

8. Collection Notice

FOIPPA states that a public body needs to provide a written or verbal collection notice when collecting personal information directly from the individual the information is about.

Personal information (vaccination status and name) will only be viewed by the business scanning the QR code. Businesses and public bodies are responsible for fulfilling any notification requirements that may apply.

PART 3: SECURITY OF PERSONAL INFORMATION

In Part 3 you will share information about the privacy aspect of securing personal information. People, organizations or governments outside of your initiative should not be able to access the personal information you collect, use, store or disclose. You need to make sure that the personal information is safely secured in both physical (e.g. your office building) and technical (e.g. online cloud service) environments. What security measures are in place?

9. Digital tools, databases or information systems

Does your initiative involve a digital tool, database or information system?

Yes.

- If yes, you may need to involve your [MPO](#) and possibly your [Ministry Information Security Officer](#) (MISO). Together you can decide whether your initiative needs a security assessment.

9.1 Do you or will you have a security assessment to help you ensure the initiative meets the reasonable security requirements of [FOIPPA section 30](#)?

Yes. See STRA #S2021-55

- If you answered yes to question 9.1, skip the rest of part 3 and go to part 4.

10. Physical security

Are all physical records stored in government buildings with government security?

n/a

11. Technical security

Are all records stored on government servers?

n/a

12. Controlling and tracking access

Please check each strategy that describes how you limit or restrict who can access personal information and how you keep track of who has accessed personal information in the past.

Insert your own strategies if needed.

n/a

PART 4: ACCURACY, CORRECTION AND RETENTION

In Part 4 you will demonstrate that you make a reasonable effort to ensure the personal information that you have on file is accurate and complete.

13. Requests for correction

FOIPPA gives an individual the [right to request correction of errors or omissions](#) to their personal information. You must have a plan in place to respond to these requests.

13.1 Do you have a process in place to correct personal information?

Yes. If there is a discrepancy in vaccination status, the citizen can submit a form to immunizationrecord.gov.bc.ca or call a dedicated helpline. This information is available on the BC immunization website.

13.2 Sometimes it's not possible to correct the personal information. Will you make a note on the record that the correction was requested, if you're not able to correct the record itself?

Yes

13.3 If you receive a request for correction from an individual and you know you disclosed their personal information in the last year, FOIPPA requires you to notify the other public body or third party of the request for correction. Will you ensure that you conduct these notifications when necessary?

No. The app is designed to preserve a citizen's anonymity and therefore it is not possible for PHSA to notify third parties to which citizens have disclosed their vaccination status.

13.4 Does your initiative use personal information to make decisions that directly affect an individual?

Yes

- If yes, go to question 14
- If no, skip ahead to part 5.

14. Decisions affecting individuals

Describe what decisions are made that directly affect individuals and what personal information is used to make the decisions.

The province of BC has mandated that individuals must be partially vaccinated to enter non-essential business, starting September 13, 2021, and fully vaccinated by October 24, 2021.

14.1 How will you make sure that the personal information is accurate and complete?

Existing processes are in place related to records in the Provincial Immunization Registry (PIR), which is a Provincial Health Services Authority owned system. PIR will be receiving daily updates from the Ministry's Enterprise Master Patient Index (via SFTP), which will ensure that patient demographic information is up to date.

14.2 FOIPPA requires that ministries keep personal information for a minimum of one year after it is used to make a decision. Do you have an approved information schedule in place related to this information?

n/a – no PI will reside in the app; it will continue to reside in the PIR and be kept for a minimum of 1 year.

14.3 If you answered no, describe how you will ensure the information will be kept for a minimum of one year after it's used to make a decision that directly affects an individual.

n/a

PART 5: AGREEMENTS AND INFORMATION BANKS

Please provide some information about whether your initiative will involve an information sharing agreement, research agreement or personal information bank.

15. Does your initiative involve or will it be part of a regular and systematic exchange of personal information with partners in or outside government?

No.

16. Does your initiative involve sharing personal information with a third party for research or statistical purposes?

No.

17. Will your initiative result in a personal information bank?

A personal information bank (PIB) is a collection of personal information searchable by name or other unique identifier.

No.

PART 6: ADDITIONAL RISKS

Part 6 asks that you reflect on the risks to personal information in your initiative and list any risks that have not already been addressed by the questions in the template.

18. Risk response

Describe any additional risks that arise from collecting, using, storing, accessing or disclosing personal information in your initiative that have not been addressed by the questions on the template.

Possible risk	Response
Risk 1: Screenshots are taken of a citizen's name and vaccination status and saved to the business owner's phone.	<p>Businesses will be told that they are not to do this without consent as per the Order of the Provincial Health Officer – and there are fines for breaking the Order.</p> <p>As per the PHO:</p> <ul style="list-style-type: none"> - An operator must not scan the QR code on a vaccine card, or paper record of vaccination, with any tool other than a BC Vaccine Card Verifier App. - Subject to section 7, an organizer must not retain proof of vaccination or identification provided by a participant, or use it for any purpose other than to confirm that a participant has been vaccinated, as required by this Order. - Despite section 6, with the written consent of a participant, an organizer may keep a record of the fact that the participant has provided proof of being vaccinated in compliance with this Part until this Order expires or is repealed, and the organizer may rely upon this record to satisfy the requirements in this Part with respect to future participation by the participant in an event at the same place.
Risk 2: App can be downloaded and used by any member of the public, who can then scan anyone's QR code.	Data is minimized to only display vaccine status and name. The BC Vaccine card verifier app is the app that businesses will be

Possible risk	Response
	told to use in the PHO. This app will not display anything further than name and status.
Risk 3: The public are not convinced that the business will not receive information other than their name and vaccination status.	Provide messaging for the public about the privacy measures related to the app. This messaging is available on multiple channels, including websites, briefings, and the media
Risk 4: Someone with a SMART Health Card reader can access additional PI kept in the QR Code.	Provide public messaging about the potential sensitivity of the QR code and to not share it with others. Businesses will be told to use only the BC Vaccine Card Verifier App. Minimal personal information is stored in the QR code, thus minimizing risk to individuals if this were to occur.

PART 7: SIGNATURES

You have completed a Privacy Impact Assessment. All you need now are signatures. The Privacy, Compliance and Training Branch (PCT) will sign this first before returning it to your program area for signatures.


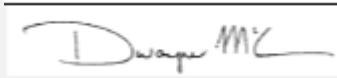
PCT will review the PIA and create a summary of their review.

PCT Summary and Comment

PCT has reviewed the ministry's PIA outlining the BC Vaccine Card Verifier App which indicates the associated activities to carry out the PHO's Orders mandating citizens to provide proof of COVID-19 vaccination status in order to engage in high-risk public activities. The Verifier App works in conjunction with the Vaccine QR code to scan for vaccination results of the individual accessing services or participating in activities. Appropriate collection and use authorities have been indicated. The OIPC was consulted on this PIA, which raised inquiries about the technical security measure of the App, but all concerns have been appropriately addressed.

PCT Signatures



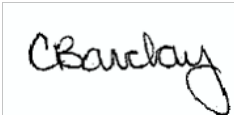
This PIA is based on a review of the material provided to PCT as of the date below.


Role	Name	Electronic Signature	Date Signed
PCT Privacy Advisor	Jessica Bouchard		September 23, 2021
PCT Manager, Privacy Operations	Dwayne McCowan		September 23, 2021

Ministry Signatures

This PIA accurately documents the data elements and information flow at the time of signing. If there are any changes to the overall initiative, including to the way personal information is collected, used, stored or disclosed, the program area will engage with their MPO and if necessary, complete a PIA update to submit to PCT. Your ministry may choose to add signatories.

Ministry Comments

Role	Name	Electronic Signature	Date Signed
Initiative lead	Pamela Smith		October 3, 2021
Executive Director	Jeff Aitkin		October 4, 2021
Assistant Deputy Minister or designate Only required if personal information is involved	Corrie Barclay		October 13, 2021

	MISO Name	Electronic Signature	Date Signed by MISO
Ministry Information Security Officer	Wayman Yee		October 5, 2021