



Privacy Impact Assessment for Integrated Program Agreement Between Justice and Community Partners PIA#PSSG21059

Part 1 – General

Name of Ministries:	Ministry of Public Safety and Solicitor General, BC Corrections, Policing and Security Branch, and Community Safety and Crime Prevention Ministry of Attorney General, BC Prosecution Service Ministry of Social Development and Poverty Reduction Ministry of Housing		
PIA Drafter:	Krista D'Argis, Privacy Analyst		
Email:	Krista.Dargis@gov.bc.ca	Phone:	1 888 952-7968
Program Manager:	Erin Gunnarson, A/Provincial Director, Strategic Operations		
Email:	Erin.Gunnarson@gov.bc.ca	Phone:	778-974-3001

1. Description of the Initiative

The Blue Ribbon Panel Report on Crime Reduction (2014) reflected extensive consultation with stakeholders across the province, reviewing existing crime reduction activities and identifying their strengths as well as potential gaps, challenges and issues. Through this process, the Panel observed widespread frustration regarding the lack of collaboration amongst relevant government ministries, local community leaders and organizations citing disjointed approaches, fragmented interventions, and the propensity of many professionals to work in isolation from others. The report also identified a lack of effective information sharing practices as a serious concern.

Many of the professionals consulted spoke of the lack of clarity within their own agency and among stakeholders about when, how, and what information can be shared while complying with privacy protection laws and policies. It was frequently suggested that the government should publish clear guidelines on information sharing under existing laws for the purposes of public safety, child protection and crime reduction, or even legislate in that area if necessary.

The White Paper on Justice Reform (2013) also outlined the importance of choosing integrated approaches and recognizing that the actions of one part of the system have effects on the others.

This analysis invites criminal justice partners and social and community stakeholders to develop an integrated approach to working together in order to create common client engagement, stability, successful community integration, and harm reduction actions in ways that are sensitive to diverse individual as well as group needs.



Privacy Impact Assessment for Integrated Program Agreement Between Justice and Community Partners PIA#PSSG21059

Evidence shows that an integrated approach to justice client management is associated with a reduction in recidivism, increased engagement with health/social service agencies, improved health and wellbeing of clients, fewer police interactions, and decreased time in custody.

The use of integrated approaches and integrated team models requires the sharing of information. Sharing information assists with identifying justice clients' criminogenic needs and aligning the associated risks to available resources to provide the best quality supports and improve outcomes. Information sharing also brings more resources and expertise to case management and can begin to bridge existing gaps.

It is important to note that integrated case management initiatives are currently operating amongst criminal justice partners and social service agencies throughout BC. This integrated approach between community services and the criminal justice system is consistent with similar approaches in the United Kingdom and more recently in Alberta.

In British Columbia, examples of such programs include the Downtown Community Court in Vancouver, Integrated Transitional Release Planning (ITRP) - Homelessness Intervention Project (HIP), Vancouver Intensive Supervision Unit (VISU), Integrated Case Management Team (Kamloops), and Victoria Integrated Community Outreach Team (VICOT), just to name a few.

The following public bodies and government Institutions below are most often involved in justice related integrated case management and are stakeholders in this project:

- Correctional Service Canada (CSC)
- Royal Canadian Mounted Police (RCMP)
- Vancouver Police Department (VPD)
- Ministry of Attorney General (AG)
- Ministry of Public Safety and Solicitor General (PSSG)
- Ministry of Social Development and Poverty Reduction (SDPR)
- Ministry of Housing (HOUS)

In the fall of 2012, the Justice & Public Safety Council (formerly the Justice Reform Council) recommended the development of an Information Sharing Agreement and protocols to ensure the continued routine multi-agency dialogue and coordination to strategically manage all common clients in BC. The Integrated Program Agreement between Justice and Community Partners (the agreement) is intended to address these directives.



Privacy Impact Assessment for Integrated Program Agreement Between Justice and Community Partners PIA#PSSG21059

The agreement addresses all current information sharing activities that occur between partners in the context of the case management of justice clients, including within formal integrated initiatives and daily operations.

“Justice clients” are defined as shared clients that are involved with one or more partner agencies and can be defined as follows:

- Individuals who have either been named on a Report to Crown Counsel (RCC) that contains an allegation of a criminal offence or offences and who were 18 years of age or older at the time of the alleged offence; or
- Individuals who have pled guilty or have been found guilty of at least one charge and who were 18 years of age or older at the time of the offence. This includes guilty pleas or findings of guilt that are entered for lesser or included offences.

The objective of this agreement is to enable integrated, risk based approaches to the delivery of services for justice clients; to enhance collaboration by the sharing of information to provide efficient and effective case management of justice clients; to reduce recidivism and keep communities safe; and, to engage partners in the development of a IPA and protocols in compliance with the *Freedom of Information and Protection of Privacy Act* and any other applicable legislation.

2. Scope of this PIA

The PIA will assess the privacy implications of information sharing in the context of the agreement for PSSG, AG, VPD, SDPR and HOUS. Note that the information sharing in scope of this project is only in the context of the case management of justice clients and information sharing in the context of law enforcement, even where it may overlap, is out of scope of the PIA. Additionally, note that this PIA will not assess the privacy implications of CSC or RCMP as a different privacy legislation and policies apply to them as federal agencies. Furthermore, this PIA will not assess VPD’s use of the Police Records Information Management Environment (PRIME-BC) where the relevant information is likely to be stored and accessed by VPD.

3. Related Privacy Impact Assessments

AG08029 - Downtown Community Court Project

SDSI14010 - Integrated Case Management System (ICM) 4.0



Privacy Impact Assessment for Integrated Program Agreement Between Justice and Community Partners PIA#PSSG21059

PIA 03-M014 - CORNET II

JAG13045 – JUSTIN

PSSG03009 – ELVIS

06-S001 – VISTA

PSSG18049 - CRV

4. Elements of Information or Data

The following personal information of a justice client may be exchanged where necessary and appropriate under the agreement. Note that the list of data elements is not exhaustive:

- Name, address, email address, or telephone number;
- Age, date of birth, gender, religious beliefs, sexual orientation, marital or family status;
- Identifying number (i.e., court file number or police file number, symbol or other particular assigned to an individual);
- Health care history, including physical or mental disabilities and addiction;
- Identified needs and risk factors;
- Educational, financial, criminal or employment history
- Enrollment in services and programs;
- Personal views or opinions regarding the Common Client held by a Partner;
- Professional assessments performed by a Partner;
- Outcomes relating to involvement in the judicial system;
- Internal assessments;
- Participation or enrollment in services and programs;
- Photos for the purpose of identification;
- Criminogenic needs;
- Court orders and court ordered conditions, and
- Risk factors/level.



Privacy Impact Assessment for Integrated Program Agreement Between Justice and Community Partners PIA#PSSG21059

The agreement outlines the sharing the personal information of individuals involved or relevant to the case management of the justice client where necessary and appropriate. Such persons may include the relevant victim(s), witnesses and the justice client's family and friends. It may also involve employers, landlords, contact information of other agencies integral to the case management of client, etc. Examples of data elements include:

- Age, date of birth, gender, religious beliefs, sexual orientation, marital or family status;
- Identifying number (i.e. court file number or police file number, symbol or other particular assigned to an individual);
- Health care history, including physical or mental disabilities and addiction;
- Educational, financial, criminal or employment history;
- Personal views or opinions;
- Photos for identification; and
- Relationship to the justice client.

The agreement may also include sharing the professional opinions of employees of the Partners.

Part 2 – Protection of Personal Information

5. Storage or Access outside Canada

The personal information of relevant justice clients engaging with Ministry Partners will only be located within Canada on BC Government infrastructure and will only be accessed within Canada.

6. Data-linking Initiative*

In FOIPPA, "data linking" and "data-linking initiative" are strictly defined. Answer the following questions to determine whether your initiative qualifies as a "data-linking initiative" under the Act.

1. Personal information from one database is linked or combined with personal information from another database;

Yes



Privacy Impact Assessment for Integrated Program Agreement Between Justice and Community Partners PIA#PSSG21059

2.The purpose for the linkage is different from those for which the personal information in each database was originally obtained or compiled;	No
3.The data linking is occurring between either (1) two or more public bodies or (2) one or more public bodies and one or more agencies.	N/A

7. Common or Integrated Program or Activity*

In FOIPPA, "common or integrated program or activity" is strictly defined. Answer the following questions to determine whether your initiative qualifies as "a common or integrated program or activity" under the Act.	
1. This initiative involves a program or activity that provides a service (or services);	Yes
2. Those services are provided through: (a) a public body and at least one other public body or agency working collaboratively to provide that service; or (b) one public body working on behalf of one or more other public bodies or agencies;	Yes
3. The common or integrated program/activity is confirmed by written documentation that meets the requirements set out in the FOIPP regulation.	Yes
Please check this box if this program involves a common or integrated program or activity based on your answers to the three questions above.	X



Privacy Impact Assessment for Integrated Program Agreement Between Justice and Community Partners PIA#PSSG21059

8. Personal Information Flow Table

Personal Information Flow Table			
	Description/Purpose	Type	FOIPPA Authority
1.	A public body involved in the agreement is collecting the personal information of a justice client or an individual relevant to the case management of a justice client as it relates directly to the integrated case management of said client.	Collection	26(c) [27(1)(e)]
2.	A public body involved in the agreement is using the personal information collected to facilitate the integrated case management of the justice client.	Use	32(a) and (c)
3.	A public body involved in the agreement disclosing the personal information of a justice client or an individual relevant to the case management of the client to facilitate the integrated case management of the client.	Disclosure	33(2)(d) and (k)

9. Risk Mitigation Table

Risk Mitigation Table				
	Risk	Mitigation Strategy	Likelihood	Impact
1.	Public body employees could access personal information and use or disclose it for personal purposes.	Standards of Conduct Privacy Training Criminal Record checks Access to the systems, which are auditable, requires an unique user specific login ID and password.	Low	High
2.	Request may not actually be from Partners (i.e. their email address may be being used by someone else)	Where any doubt may exist, Partners will confirm the source of communications prior to the release of information.	Low	High
3.	A client's personal information	Personal information may be	Low	High



Privacy Impact Assessment for Integrated Program Agreement Between Justice and Community Partners PIA#PSSG21059

<p>is compromised when transferred to another partner of the IPA.</p>	<p>transferred between Partners in person, by phone, by email, and by fax.</p> <p>When using email with agencies outside of the BC Government infrastructure, ministries will not use names or provide personal information in the body of the email and instead will provide the information on a password protected document attached to the email.</p> <p>The password will be provided independently.</p> <p>Ministries sharing information internally to BC Government or disclosing personal information with agencies that have a compatible encryption certificate may use the BC Government Exchange Web Services (EWS) system to email the personal information as the information will be encrypted at rest and in transit.</p> <p>Ministries may also disclose personal information through secure File Transfer Services (SFTS).</p>	
---	---	--

10. Collection Notice

A collection notice will not be required as part of this initiative as per section 27(3) of FoIPPA as the personal information will not be collected directly from the individual justice client and the indirect collection will be authorized as per section 27(1)(e) of FoIPPA.



Privacy Impact Assessment for Integrated Program Agreement Between Justice and Community Partners PIA#PSSG21059

Part 3 – Security of Personal Information

11. Please describe the physical security measures related to the initiative (if applicable).

AG, PSSG, SDPR, HOUS and VPD utilize appropriate security controls and mitigation measures to protect information in their care (see related PIAs). Access to physical locations are controlled via key or pass-card access.

The BC Government SFTS, associated SharePoint site, LAN Drives, JUSTIN, CORNET, COAST, VISTA, ELVIS and ICM databases are located on BC Government servers, which are secured by 24/7 professional security personnel, extensive video surveillance, biometric access controls and bullet resistant entrances, along with related measures to ensure appropriate physical security.

12. Please describe the technical security measures related to the initiative (if applicable).

The personal information located in ICM, COAST, EWS, VISTA, ELVIS, BC Government SFTS, and associated SharePoint site and LAN Drives requires individual BC Government IDIR accounts and password; and is limited to authorized personnel.

Regarding the personal information located in CORNET and JUSTIN, users will access the CORNET or JUSTIN application from a government workstation by logging into their workstations and local network using their government provided IDIR user ID and password, and then they log into the CORNET or JUSTIN application with their CORNET or JUSTIN Oracle user ID and password.

BC Government firewalls as well as additional intrusion prevention mechanisms will be used to protect the personal information that will be stored on CORNET, JUSTIN, COAST, ELVIS, VISTA, ICM, SFTS, EWS system and associated SharePoint site and LAN Drives as the information will be located within the secure BC Government infrastructure.

13. Does your agency rely on security policies other than BC Government the Information Security Policy?

In addition to the Information Security Policy, the following policies speak to the security of personal information in BC Corrections custody:

Management Services Policy Manual
2.4 – Information Incidents
13 – Release of Information
16.1 – Information Systems



Privacy Impact Assessment for Integrated Program Agreement Between Justice and Community Partners PIA#PSSG21059

16.2 – Systems Security

16.3 – Information Systems Authorization and Training

Adult Custody Policy Manual

7.5 – Access to Information

9.1.6 – Confidentiality of Personal Medical Information

14. Please describe any access controls and/or ways in which you will limit or restrict unauthorized changes (such as additions or deletions) to personal information.

PSSG, AG, SDPR and HOUS employees require security clearance as part of their hiring process, which will therefore be in place before any employees' access buildings or personal information.

The EWS system, COAST, ELVIS, VISTA, ICM, associated SharePoint sites, LAN Drives, and SFTS are only accessible through a valid BC government user ID and password. The access to these systems and to JUSTIN and CORNET is limited based on need-to-know and roles.

15. Please describe how you track who has access to the personal information.

Tracking takes place in the Ministries' case management systems at multiple levels when sensitive information is accessed, when new records are created, read, modified. Audit information cannot be modified and is immediately available for review.

Additionally, access to the branch headquarters and BC Corrections' correctional centres, headquarters and community corrections offices is limited to authorized personnel only. The access to areas of the buildings secured by swipe card/passcode access can be tracked and audited.

In terms of the SFTS, access and attempted access are logged.

Auditing will be undertaken on receipt of a credible complaint, information incident, data quality concerns, criminal or operational intelligence (with data security implications).

In terms of the EWS, Microsoft Exchange generates several logs:

- EWS is hosted in Internet Information Services (IIS) on the Exchange server which records activity in the IIS logs. These logs are archived and retained for 13 months unless there is a litigation hold.



Privacy Impact Assessment for Integrated Program Agreement Between Justice and Community Partners PIA#PSSG21059

o The EWS client protocol can be used both by internal and external clients through the Reverse Proxy service, Threat Management Gateway (TMG). Connections through TMG are logged with client IP address and these logs are retained for 7 days.

- Message Transport logs include message tracking (Exchange server to Exchange server - internal only) which provides a detailed record of message activity, such as sent, received, date\time and message subject. These logs are archived and retained for 13 months unless there is a litigation hold.

- Exchange also produces various protocol logs for a short time on the server for troubleshooting purposes. The protocol logs age out or are deleted as space requires.

There will be the ability to track who has accessed the documents on the LAN Drive and SharePoint, but there will not be audit logging. Changes to permissions are also tracked, so administrators have a record of who was granted access, by whom and when.

Part 4 – Accuracy/Correction/Retention of Personal Information

16. How is an individual's information updated or corrected? If information is not updated or corrected (for physical, procedural or other reasons) please explain how it will be annotated? If personal information will be disclosed to others, how will the ministry notify them of the update, correction or annotation?

An individual, who believes there is an error or omission in their personal information in the custody or under the control of VPD, SDPR, AG, PSSG or HOUS may request that the relevant public body correct the information. If the information is not corrected, an annotation will be made to the file, and if the information has been provided to another party in the last 12 months, the party will be advised of the request.

17. Does your initiative use personal information to make decisions that directly affect an individual(s)? If yes, please explain.

Yes, the personal information collected will be used to support the case management of the common justice client.



Privacy Impact Assessment for Integrated Program Agreement Between Justice and Community Partners PIA#PSSG21059

18. If you answered "yes" to question 17, please explain the efforts that will be made to ensure that the personal information is accurate and complete.

Partners will make every reasonable effort to ensure that the information is accurate and complete and will confirm and validate the identity of individuals during in-person interviews. That said, personal information is not exhaustive and is constantly being updated and therefore cannot be relied upon as complete. Any such personal information is provided as a supplement to, and not a substitute for knowledge, expertise, skill, and professional judgment.

Note that as part of eServices identity management, individuals being supervised by BC Corrections are asked to provide their fingerprint biometric at admission to confirm identity (see 293-50/PIA-ICON2).

A picture of the individual may also be taken at admission and this picture is used to continuously monitor the individual's identity during their supervision. These steps help ensure that the right personal information is added to the right CORNET file.

19. If you answered "yes" to question 17, do you have approved records retention and disposition schedule that will ensure that personal information is kept for at least one year after it is used in making a decision directly affecting an individual?

Partners have approved records retention and disposition schedules that will ensure that personal information is kept for at least one year after it is used in making a decision directly affecting an individual.

Part 5 – Further Information

20. Does the initiative involve systematic disclosures of personal information? If yes, please explain.

There will be disclosures of personal information amongst Partners as part of day-to-day operations and through more specific formal programs/initiatives.

Please check this box if the related Information Sharing Agreement (ISA) has been prepared. If you have general questions about preparing an ISA, please contact the Privacy and Access Helpline.

An IPA



Privacy Impact Assessment for Integrated Program Agreement Between Justice and Community Partners PIA#PSSG21059

Information Sharing Agreement – Required Information	
Description	As part of the Partners in Justice Client Case Management project, Partners will regularly exchange personal information of common clients in order to facilitate the case management of those clients.
Primary ministry/government agency involved	Ministry of Public Safety and Solicitor General
All other ministries/government agencies and public bodies involved	Ministries of Attorney General, Social Development and Poverty Reduction and Housing Correctional Service Canada (CSC) Royal Canadian Mounted Police (RCMP) Vancouver Police Department
Business contact title	Privacy and Information Management Analyst
Business contact telephone number	1 888 952-7968
Indication of whether or not personal information is involved	Yes
Start date	2020
End date (if applicable)	N/A

21. Does the program involve access to personally identifiable information for research or statistical purposes? If yes, please explain.

No.

22. Will a personal information bank (PIB) result from this initiative?

There will be no new PIB for this initiative.



Privacy Impact Assessment Integrated Program Agreement Between Justice and Community Partners PIA#PSSG21059

Part 6 – Privacy, Compliance and Training (PCT) Comments and Signatures

PCT has reviewed the ministry's Initiative PIA detailing information sharing in the context of the Integrated Program Agreement between Justice and Community Partners for Public Safety and Solicitor General, Ministry of Attorney General, Vancouver Police Department and Ministry of Social Development and Poverty Reduction. The ministry has indicated appropriate collection, use, and disclosure authorities for this program. The Office of the Information and Privacy Commissioner (OIPC) has reviewed this initiative and has no outstanding concerns.

Joann Berekoff

Privacy Analyst
Privacy, Compliance and Training
Branch
Corporate Information and Records
Management Office
Ministry of Citizens' Services

Signature

September 12, 2022

Date

Kirsten Nicholson

A/Director
Privacy, Compliance and Training
Branch
Corporate Information and Records
Management Office
Ministry of Citizens' Services

Signature

September 16, 2022

Date



Privacy Impact Assessment Integrated Program Agreement between Justice and Community Partners PIA#PSSG21059

Part 7 – Program Area Comments and Signatures

Melissa Sexsmith
Ministry Privacy Officer
Information Systems Branch
Ministry of Attorney General


Signature

September 20, 2022
Date

BC Corrections signatures

Erin Gunnarson
Provincial Director Strategic
Operations
BC Corrections
Ministry of Public Safety and
Solicitor General


Signature

January 26, 2023
Date

Lisa Sweet
Assistant Deputy Minister
BC Corrections
Ministry of Public Safety and
Solicitor General


Signature

January 27, 2023
Date



Privacy Impact Assessment Integrated Program Agreement Between Justice and Community Partners PIA#PSSG21059

Community Safety and Crime Prevention signatures

Stephen Ford

Executive Director,
Community Programs and
Service Delivery
Victim Services and Crime
Prevention Division
Ministry of Public Safety
and Solicitor General

Signature

November 15, 2022

Date

Taryn Walsh

Assistant Deputy Minister
Community Safety and Crime
Prevention
Ministry of Public Safety and
Solicitor General

Signature

November 15, 2022

Date



Privacy Impact Assessment Integrated Program Agreement between Justice and Community Partners

PIA#PSSG21059

BC Prosecution Service signatures

Brian Anderson

Executive Director, Business
Operations

BC Prosecution Service Ministry of
Attorney General and Minister
responsible for Housing

Signature

December 13, 2022

Date

Peter Juk KC

Assistant Deputy Attorney General
BC Prosecution Service
Ministry of Attorney General and
Minister responsible for Housing

Signature

December 1, 2022

Date

Policing and Security Branch signatures

Brian Sims

Executive Director, Serious
and Organized Crime
Policing and Security Branch
Ministry of Public Safety and
Solicitor General

Signature

November 25, 2022

Date

Glen Lewis

Associate Director of Police
Services
Policing and Security Branch
Ministry of Public Safety and
Solicitor General

Signature

November 25, 2022

Date



Privacy Impact Assessment Integrated Program Agreement between Justice and Community Partners PIA#PSSG21059

Ministry of Social Development and Poverty Reduction signatures

Chris Mutadi

Director, Information Security and
Privacy
Ministry of Social Development and
Poverty Reduction

A handwritten signature in black ink, appearing to read "C. Mutadi".

Signature

Nov 25, 2022

Date

Raymond Fieltsch

Assistant Deputy Minister, Service
Delivery Division
Ministry of Social Development and
Poverty Reduction

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

Signature

Nov 25, 2022

Date

Vancouver Police Department signatures

Adam Palmer

Chief Constable
Office of the Chief Constable
Vancouver Police Department

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

Signature

DEC. 22/22

Date



Privacy Impact Assessment for Integrated Program Agreement Between Justice and Community Partners

PIA#PSSG21059

Ministry of Housing Signatures

Meghan Will

A/Assistant Deputy Minister,
Homelessness Policy and
Partnerships
Ministry of Housing

Signature

Jan 3, 2023

Date