Privacy Impact Assessment for Ministries

Table of Contents

Use this privacy impact assessment (PIA) template if you work for or are a service provider to a ministry in the Government of B.C. and are starting a new initiative or significantly changing an existing initiative.

Before you start

- An initiative is an enactment, system, project, program, or activity
- Find PIA templates for initiative update, enactments or broader public sector use
- Contact your Ministry Privacy Officer (MPO) for help with your PIA
- Find information on the PIA review process and question-by-question guidance
- Protecting privacy involves managing records and providing reasonable security for information throughout its lifecycle. Contact your Government Records Officer for

questions about information management and your Ministry Information Security Officer for questions about information security.

- If you have any questions, email Privacy.Helpline@gov.bc.ca or phone 250 356-1851

PART 1: GENERAL INFORMATION

Privacy, Compliance and Training Branch (PCT) intake number / PIA file number:

Initiative title:	ServicesNow – Genesys Cloud
Ministry:	Ministry of Health
Branch or unit:	Health Insurance BC
Your name and title:	Vinicius Cid, Sr. Privacy Analyst
Your email:	Vinicius.cid@gov.bc.ca
Initiative Lead name and title:	Rod Broadbent, Director, Technology Solutions
Initiative Lead email:	Rod.broadbent@gov.bc.ca
Ministry Privacy Officer:	Quinn Fletcher
MPO email:	MOH.privacy.officer@gov.bc.ca

Commented [CVCH1]: Provisional - confirm once PIA goes back to HIBC

Your MPO will complete the questions in the table below.

FOR MPO USE ONLY
Is this a PI or non-PI assessment?
PI
Is this initiative a data-linking program under FOIPPA?
No
Is this initiative a common or integrated program or activity under FOIPPA?
No
Related PIAs, if any:
CITZ21029 – Services BC-Health Helpdesk
Does this initiative involve disclosures of sensitive personal information outside of Canada?

No
Provide a brief summary of the initiative to be published in the Personal Information Directory. This summary may be similar to the answer to question 1.
As part of implementing the HIBC Integrated Transition and Transformation Plan (ITTP) - Contact Centre and IVR, the Genesys Cloud solution is selected to be the new the contact centre system for the HIBC program upon transition from Maximus to Pacific Blue Cross Solutions (PBCS). Genesys Cloud is a call center software offered as a SaaS solution, and there will be integration between the HIBC contact centre system, the IVR and Service BC's HCCS as it is the case today. Currently, Maximus operates the HIBC contact center using Cisco Contact Manager which is hosted in the Maximus data centre.
Is there an Information Sharing Agreement as part of this initiative? If yes, please have the Information Sharing Agreement Supplement attached to this PIA when submitting to PCT.

1. What is the initiative?

Service BC (SBC) delivers provincial government services and information at the SBC Provincial Contact Centre (CC) to residents and clients throughout British Columbia (BC). The CC also provides direction to government websites and online services. The CC provides services on behalf of the Ministry of Health (MoH), in particular assistance related to the Medical Services Plan (MSP) and the PharmaCare prescription program. Health Insurance BC (HIBC) administers the day-to-day operations of these programs on behalf of the MoH; they also manage the health-related CC operations.

Previously, MAXIMUS had been contracted to operate CC services delivered by HIBC and used their own technical infrastructure to that end. Now, Pacific Blue Cross Solutions(PBCS) is being onboarded on that role. While health services delivered by the CC will remain the same, there will be changes to the software being used.

The Genesys Cloud solution has been selected by PBCS to be the new the CC system for the HIBC program. Genesys a call center software offered as a SaaS solution, and there will be

integration between the HIBC contact centre system, the IVR and Service BC's HCCS like in the current solution. Genesys will replace the MAXIMUS-operated Cisco Contact Manager, which is hosted in their own data centers.

By selecting Genesys Cloud as the HIBC contact centre replacement application, PBCS is leveraging a state-of-the-art cloud-based solution, and is poised to implement a wide variety of new service offerings and transformation opportunities with respect to caller experience, workforce management, quality assurance, live agent support and IVR.

The HIBC contact centre will be formally transitioned upon assumption of service, currently scheduled for April 2023, and will continue throughout the duration of the PBCS-HIBC contract with the Ministry of Health.

2. What is the scope of the PIA?

This PIA deals with PBCS' onboarding as operators of HIBC's contact center, and their introduction of Genesys Cloud to replace the existing call center software solution by MAXIMUS. This PIA will not reassess contact center operations, which is documented in CITZ21029.

3. What are the data or information elements involved in your initiative?

Genesys, upon PBCS assumption of service, will collect PI data in call logs and call recordings. This could include the following:

- Citizen's Name
- Personal Health Number (PHN)
- Birth Month and Year
- Month, Day and Year of Service
- Practitioner Number
- Payment Number
- Assignment Effective Date Month, Day and Year
- Facility Number
- Appointment Date Month, Day and Year

Commented [CVCH2]: I'm wondering whether any of the infosys integrations currently available to CC agents will change as a result of the PBCS transition (e.g. will they have access to more/less/different systems to validate information or do their jobs, aside from Genesys?)

- College of Pharmacists ID
- MSP Billing Number
- Drug Identification Number

No additional information is expected to be collected, used and/or disclosed as a result of the PBCS transition and introduction of Genesys Cloud.

3.1 Did you list personal information in question 3?

Personal information **is any recorded information about an identifiable individual, other than business contact information. Personal information includes information that can be used to identify an individual through association or reference.**

Yes.

4. How will you reduce the risk of unintentionally collecting personal information?

N/A

PART 2: COLLECTION, USE AND DISCLOSURE

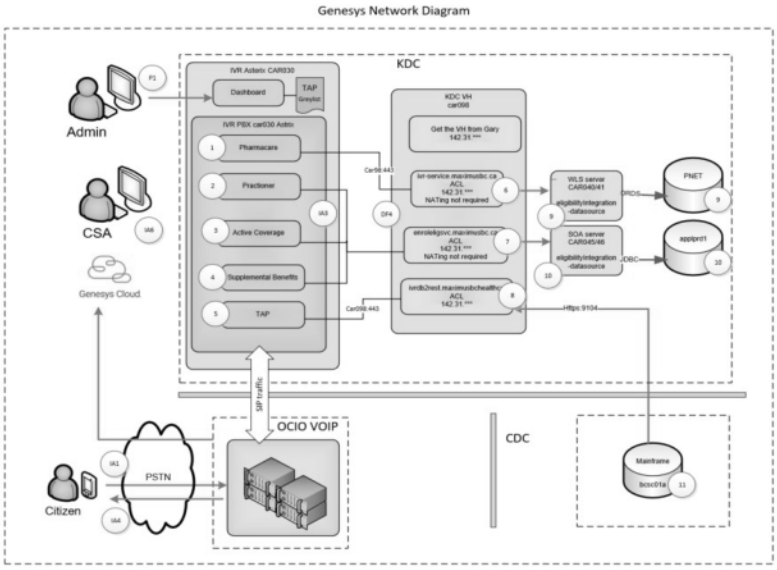
5. Collection, use, and disclosure

Commented [CVCH3]: Table built assuming there's no net new PI collection/use/disclosure being introduced, merely a change due to the introduction of PBCS and Genesys.

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: Citizens' calls will be recorded by Genesys as part of the contact center's operations to deliver health services to them.	Collection	26 (a),(c) [27(1)(e), 27(1)(c)(iii)	Pharmaceutical Services Act s. 22 (1)

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
The calls will often contain PI as citizens provide personal information related to MSP or PharmaCare services.			
Step 2: Certain PBCS staff may access logfiles and call recording for investigation and training purposes. Contents of logfiles and call recordings are not stored or passed to any other Genesys components.	Use	32(a)	

Optional: Insert a drawing or flow diagram here or in an appendix if you think it will help to explain how each different part is connected.



6

Commented [CVCH4]: I'll need more details to understand how recordings are managed - e.g. if they're not being stored, how are PBCS staff accessing them - listening in live, for instance?

Commented [CVCH5]: I have to admit understanding this flow chart was a struggle, and I'd wager it would be even truer for CITZ once they review the PIA - wondering if PBCS has a more layman-friendly diagram.

6. Collection Notice

The PBCS onboarding and introduction of Genesys will not change what citizens hear when they call the contact center. The collection notice will remain as follows:

"The personal information you provide will be collected for the purpose of enrolment in the Medical Services Plan, Pharmacare, as well as providing a range of services related to provincial health programs. Personal information is collected under the authority of, the Pharmaceutical Services Act and section 26 (a) and (c) of the Freedom of Information and Protection of Privacy Act ("FOIPPA"). Information may be disclosed pursuant to section 33 of FOIPPA. If you have any questions about the collection and use of your personal information, please contact the Health Insurance BC Chief Privacy Office, Health Insurance BC Chief Privacy Office PO Box 9035 Station Provincial Government Victoria, BC V8W 9E3 or call 604 683-7151 (Vancouver) or 1 800 663- 7100 (toll-free). To hear this message again, press pound. To continue press 1."

Commented [CVCH6]: Confirm - verbiage borrowed from existing call center process

FOR MPO USE ONLY

If applicable, list the exception to a collection notice.

PART 3: STORING PERSONAL INFORMATION

7. Is any personal information stored outside of Canada?

No.

8. Does your initiative involve sensitive personal information?

Yes.

9. Is the sensitive personal information being disclosed outside of Canada under FOIPPA section 33(2)(f)?

No.

10. Where and how are you storing the personal information involved in your initiative?

Commented [CVCH7]: Confirm w/ PBCS whether data is stored in Canada and if so, where/how

PART 4: ASSESSMENT OF DISCLOSURES OUTSIDE OF CANADA

N/A

PART 5: SECURITY OF PERSONAL INFORMATION

11. Does your initiative involve digital tools, databases or information systems?

Yes.

18.1 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.

Commented [CVCH8]: Presumably so - confirm whether STRA has been initiated

12. Are all digital records stored on government servers and are all physical records stored in government offices with government security?

Commented [CVCH9]: Possibly not - check w/ PBCS

13. 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.

Strategy	
We allow employees only in certain roles access to information	X
Employees that need standing or recurring access to personal information must be approved by the appropriate authority	X
We use audit logs to see who accesses a file and when	X
Describe any additional controls:	

PART 6: ACCURACY, CORRECTION, AND RETENTION

Commented [CVCH10]: For this part, it might suffice to say that the Call center would be using the same process as they had been using under MAXIMUS - confirm w/ PBCS if that's the case.

In Part 6 you will demonstrate that you will make a reasonable effort to ensure the personal information that you have on file is accurate and complete.

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

FOIPPA section 28 states that a public body must make every reasonable effort to ensure that an individual's personal information is accurate and complete.

15. Requests for correction

FOIPPA gives an individual the right to request correction of errors or omissions to their personal information. You must have a process in place to respond to these requests.

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

Type "yes" or "no" to indicate your response.

22.2 Sometimes it's not possible to correct the personal information. FOIPPA requires that you make a note on the record about the request for correction if you're not able to correct the record itself. Will you document the request to correct or annotate the record?

Type "yes" or "no" to indicate your response.

22.3 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 recipient of the request for correction. Will you ensure that you conduct these notifications when necessary?

Type "yes" or "no" to indicate your response.

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

Type "yes" or "no" to indicate your response.

- If yes, go to question 24
- If no, skip ahead to Part 7

17. Do you have an approved information schedule in place related to personal information used to make decisions?

FOIPPA requires that ministries keep personal information for a minimum of one year after it is used to make a decision about an individual. In addition, the Information Management Act requires that you dispose of government information only in accordance with an approved information schedule or with the approval of the Chief Records Officer.

Type "yes" or "no" to indicate your response.

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.

PART 7: PERSONAL INFORMATION BANKS

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

18. Will your initiative result in a Personal Information Bank?

N/A

Commented [CVCH11]: No net new PIB expected.

PART 8: ADDITIONAL RISKS

19. Risk response

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

Add new rows if necessary.

Possible risk	Response
Risk 1: Storage and/or disclosure outside of Canada due to Genesys being hosted in cloud servers that may be accessed by parties outside of the country.	

Commented [CVCH12]: May not be a risk at all - confirm w/ PBCS

Possible risk	Response
Risk 2: Personal information within recorded calls exposed improperly	
Risk 3:	

Commented [CVCH13]: Here I just need to understand how access to recordings are managed, and the purpose for said access being granted.

PART 9: SIGNATURES

You have completed a Privacy Impact Assessment. PCT will review, comment and sign this document first before returning it to your program area for signatures.

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

PCT Summary

This section summarizes PCT's review of the PIA and identifies decisions made that are not otherwise noted.

PCT Comments:

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			
PCT Manager or Director Only required if personal information is involved			

Ministry Signatures

This PIA accurately documents the data elements, information flow, and information about disclosure and storage outside of Canada at the time of signing. If there are any significant

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.

Please ensure that you have reviewed the privacy risks and risk responses in Part 4: Assessment of Disclosures Outside of Canada.

Ministry Comments

Role	Name	Electronic signature	Date signed
Initiative Lead			
Assistant Deputy Minister or designate Only required if personal information is involved			

	Name	Electronic signature	Date signed
Ministry Information Security Officer Only required if MISO was involved in conducting the PIA			

Privacy Impact Assessment for Ministries

Table of Contents

Use this privacy impact assessment (PIA) template if you work for or are a service provider to a ministry in the Government of B.C. and are starting a new initiative or significantly changing an existing initiative.

Before you start

- An initiative is an enactment, system, project, program, or activity
- Find PIA templates for initiative update, enactments or broader public sector use
- Contact your Ministry Privacy Officer (MPO) for help with your PIA
- Find information on the PIA review process and question-by-question guidance
- Protecting privacy involves managing records and providing reasonable security for information throughout its lifecycle. Contact your Government Records Officer for

questions about information management and your Ministry Information Security Officer for questions about information security.

- If you have any questions, email Privacy.Helpline@gov.bc.ca or phone 250 356-1851

PART 1: GENERAL INFORMATION

Privacy, Compliance and Training Branch (PCT) intake number / PIA file number:

Initiative title:	ServicesNow – Genesys Cloud
Ministry:	Ministry of Health
Branch or unit:	Health Insurance BC
Your name and title:	Vinicius Cid, Sr. Privacy Analyst
Your email:	Vinicius.cid@gov.bc.ca
Initiative Lead name and title:	Rod Broadbent, Director, Technology Solutions
Initiative Lead email:	Rod.broadbent@gov.bc.ca
Ministry Privacy Officer:	Quinn Fletcher
MPO email:	MOH.privacy.officer@gov.bc.ca

Commented [CVCH1]: Provisional - confirm once PIA goes back to HIBC

Your MPO will complete the questions in the table below.

FOR MPO USE ONLY
Is this a PI or non-PI assessment?
PI
Is this initiative a data-linking program under FOIPPA?
No
Is this initiative a common or integrated program or activity under FOIPPA?
No
Related PIAs, if any:
CITZ21029 – Services BC-Health Helpdesk
Does this initiative involve disclosures of sensitive personal information outside of Canada?

No
Provide a brief summary of the initiative to be published in the Personal Information Directory. This summary may be similar to the answer to question 1.
As part of implementing the HIBC Integrated Transition and Transformation Plan (ITTP) - Contact Centre and IVR, the Genesys Cloud solution is selected to be the new the contact centre system for the HIBC program upon transition from Maximus to Pacific Blue Cross Solutions (PBCS). Genesys Cloud is a call center software offered as a SaaS solution, and there will be integration between the HIBC contact centre system, the IVR and Service BC's HCCS as it is the case today. Currently, Maximus operates the HIBC contact center using Cisco Contact Manager which is hosted in the Maximus data centre.
Is there an Information Sharing Agreement as part of this initiative? If yes, please have the Information Sharing Agreement Supplement attached to this PIA when submitting to PCT.

1. What is the initiative?

Service BC (SBC) delivers provincial government services and information at the SBC Provincial Contact Centre (CC) to residents and clients throughout British Columbia (BC). The CC also provides direction to government websites and online services. The CC provides services on behalf of the Ministry of Health (MoH), in particular assistance related to the Medical Services Plan (MSP) and the PharmaCare prescription program. Health Insurance BC (HIBC) administers the day-to-day operations of these programs on behalf of the MoH; they also manage the health-related CC operations.

Previously, MAXIMUS had been contracted to operate CC services delivered by HIBC and used their own technical infrastructure to that end. Now, Pacific Blue Cross Solutions(PBCS) is being onboarded on that role. While health services delivered by the CC will remain the same, there will be changes to the software being used.

The Genesys Cloud solution has been selected by PBCS to be the new the CC system for the HIBC program. Genesys a call center software offered as a SaaS solution, and there will be

integration between the HIBC contact centre system, the IVR and Service BC's HCCS like in the current solution. Genesys will replace the MAXIMUS-operated Cisco Contact Manager, which is hosted in their own data centers.

By selecting Genesys Cloud as the HIBC contact centre replacement application, PBCS is leveraging a state-of-the-art cloud-based solution, and is poised to implement a wide variety of new service offerings and transformation opportunities with respect to caller experience, workforce management, quality assurance, live agent support and IVR.

The HIBC contact centre will be formally transitioned upon assumption of service, currently scheduled for April 2023, and will continue throughout the duration of the PBCS-HIBC contract with the Ministry of Health.

2. What is the scope of the PIA?

This PIA deals with PBCS' onboarding as operators of HIBC's contact center, and their introduction of Genesys Cloud to replace the existing call center software solution by MAXIMUS. This PIA will not reassess contact center operations, which is documented in CITZ21029.

3. What are the data or information elements involved in your initiative?

Genesys, upon PBCS assumption of service, will collect PI data in call logs and call recordings. This could include the following:

- Citizen's Name
- Personal Health Number (PHN)
- Birth Month and Year
- Month, Day and Year of Service
- Practitioner Number
- Payment Number
- Assignment Effective Date Month, Day and Year
- Facility Number
- Appointment Date Month, Day and Year

Commented [CVCH2]: I'm wondering whether any of the infosys integrations currently available to CC agents will change as a result of the PBCS transition (e.g. will they have access to more/less/different systems to validate information or do their jobs, aside from Genesys?)

- College of Pharmacists ID
- MSP Billing Number
- Drug Identification Number

No additional information is expected to be collected, used and/or disclosed as a result of the PBCS transition and introduction of Genesys Cloud.

3.1 Did you list personal information in question 3?

Personal information is any recorded information about an identifiable individual, other than business contact information. Personal information includes information that can be used to identify an individual through association or reference.

Yes.

4. How will you reduce the risk of unintentionally collecting personal information?

N/A

PART 2: COLLECTION, USE AND DISCLOSURE

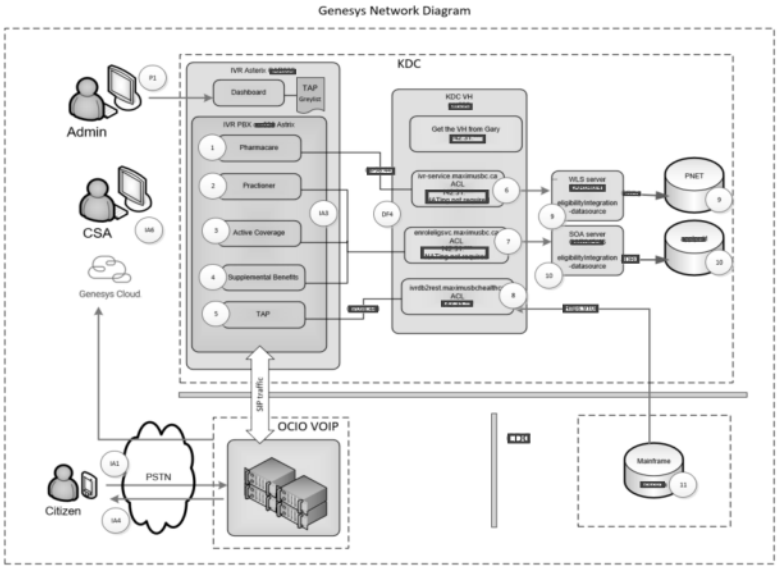
5. Collection, use, and disclosure

Commented [CVCH3]: Table built assuming there's no net new PI collection/use/disclosure being introduced, merely a change due to the introduction of PBCS and Genesys.

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: Citizens' calls will be recorded by Genesys as part of the contact center's operations to deliver health services to them.	Collection	26 (a),(c) [27(1)(e), 27(1)(c)(iii)	Pharmaceutical Services Act s. 22 (1)

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
The calls will often contain PI as citizens provide personal information related to MSP or PharmaCare services.			
Step 2: Certain PBCS staff may access logfiles and call recording for investigation and training purposes. Contents of logfiles and call recordings are not stored or passed to any other Genesys components.	Use	32(a)	

Optional: Insert a drawing or flow diagram here or in an appendix if you think it will help to explain how each different part is connected.



6

Commented [CVCH4]: I'll need more details to understand how recordings are managed - e.g. if they're not being stored, how are PBCS staff accessing them - listening in live, for instance?

Commented [CVCH5]: I have to admit understanding this flow chart was a struggle, and I'd wager it would be even truer for CITZ once they review the PIA - wondering if PBCS has a more layman-friendly diagram.

6. Collection Notice

The PBCS onboarding and introduction of Genesys will not change what citizens hear when they call the contact center. The collection notice will remain as follows:

Commented [CVCH6]: Confirm - verbiage borrowed from existing call center process

"The personal information you provide will be collected for the purpose of enrolment in the Medical Services Plan, Pharmacare, as well as providing a range of services related to provincial health programs. Personal information is collected under the authority of, the Pharmaceutical Services Act and section 26 (a) and (c) of the Freedom of Information and Protection of Privacy Act ("FOIPPA"). Information may be disclosed pursuant to section 33 of FOIPPA. If you have any questions about the collection and use of your personal information, please contact the Health Insurance BC Chief Privacy Office, Health Insurance BC Chief Privacy Office PO Box 9035 Station Provincial Government Victoria, BC V8W 9E3 or call 604 683-7151 (Vancouver) or 1 800 663- 7100 (toll-free). To hear this message again, press pound. To continue press 1."

FOR MPO USE ONLY

If applicable, list the exception to a collection notice.

PART 3: STORING PERSONAL INFORMATION

7. Is any personal information stored outside of Canada?

No.

8. Does your initiative involve sensitive personal information?

Yes.

9. Is the sensitive personal information being disclosed outside of Canada under FOIPPA section 33(2)(f)?

No.

10. Where and how are you storing the personal information involved in your initiative?

Commented [CVCH7]: Confirm w/ PBCS whether data is stored in Canada and if so, where/how

PART 4: ASSESSMENT OF DISCLOSURES OUTSIDE OF CANADA

N/A

PART 5: SECURITY OF PERSONAL INFORMATION

11. Does your initiative involve digital tools, databases or information systems?

Yes.

18.1 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.

Commented [CVCH8]: Presumably so - confirm whether STRA has been initiated

12. Are all digital records stored on government servers and are all physical records stored in government offices with government security?

Commented [CVCH9]: Possibly not - check w/ PBCS

13. 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.

Strategy	
We allow employees only in certain roles access to information	X
Employees that need standing or recurring access to personal information must be approved by the appropriate authority	X
We use audit logs to see who accesses a file and when	X
Describe any additional controls:	

PART 6: ACCURACY, CORRECTION, AND RETENTION

Commented [CVCH10]: For this part, it might suffice to say that the Call center would be using the same process as they had been using under MAXIMUS - confirm w/ PBCS if that's the case.

In Part 6 you will demonstrate that you will make a reasonable effort to ensure the personal information that you have on file is accurate and complete.

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

FOIPPA section 28 states that a public body must make every reasonable effort to ensure that an individual's personal information is accurate and complete.

15. Requests for correction

FOIPPA gives an individual the right to request correction of errors or omissions to their personal information. You must have a process in place to respond to these requests.

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

Type "yes" or "no" to indicate your response.

22.2 Sometimes it's not possible to correct the personal information. FOIPPA requires that you make a note on the record about the request for correction if you're not able to correct the record itself. Will you document the request to correct or annotate the record?

Type "yes" or "no" to indicate your response.

22.3 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 recipient of the request for correction. Will you ensure that you conduct these notifications when necessary?

Type "yes" or "no" to indicate your response.

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

Type "yes" or "no" to indicate your response.

- If yes, go to question 24
- If no, skip ahead to Part 7

17. Do you have an approved information schedule in place related to personal information used to make decisions?

FOIPPA requires that ministries keep personal information for a minimum of one year after it is used to make a decision about an individual. In addition, the Information Management Act requires that you dispose of government information only in accordance with an approved information schedule or with the approval of the Chief Records Officer.

Type "yes" or "no" to indicate your response.

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.

PART 7: PERSONAL INFORMATION BANKS

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

18. Will your initiative result in a Personal Information Bank?

N/A

Commented [CVCH11]: No net new PIB expected.

PART 8: ADDITIONAL RISKS

19. Risk response

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

Add new rows if necessary.

Possible risk	Response
Risk 1: Storage and/or disclosure outside of Canada due to Genesys being hosted in cloud servers that may be accessed by parties outside of the country.	

Commented [CVCH12]: May not be a risk at all - confirm w/ PBCS

Possible risk	Response
Risk 2: Personal information within recorded calls exposed improperly	
Risk 3:	

Commented [CVCH13]: Here I just need to understand how access to recordings are managed, and the purpose for said access being granted.

PART 9: SIGNATURES

You have completed a Privacy Impact Assessment. PCT will review, comment and sign this document first before returning it to your program area for signatures.

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

PCT Summary

This section summarizes PCT's review of the PIA and identifies decisions made that are not otherwise noted.

PCT Comments:

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			
PCT Manager or Director Only required if personal information is involved			

Ministry Signatures

This PIA accurately documents the data elements, information flow, and information about disclosure and storage outside of Canada at the time of signing. If there are any significant

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.

Please ensure that you have reviewed the privacy risks and risk responses in Part 4: Assessment of Disclosures Outside of Canada.

Ministry Comments

Role	Name	Electronic signature	Date signed
Initiative Lead			
Assistant Deputy Minister or designate Only required if personal information is involved			

	Name	Electronic signature	Date signed
Ministry Information Security Officer Only required if MISO was involved in conducting the PIA			

Privacy Impact Assessment for Ministries

Table of Contents

Use this privacy impact assessment (PIA) template if you work for or are a service provider to a ministry in the Government of B.C. and are starting a new initiative or significantly changing an existing initiative.

Before you start

- An initiative is an enactment, system, project, program, or activity
- Find PIA templates for initiative update, enactments or broader public sector use
- Contact your Ministry Privacy Officer (MPO) for help with your PIA
- Find information on the PIA review process and question-by-question guidance
- Protecting privacy involves managing records and providing reasonable security for information throughout its lifecycle. Contact your Government Records Officer for

questions about information management and your Ministry Information Security Officer for questions about information security.

- If you have any questions, email Privacy.Helpline@gov.bc.ca or phone 250 356-1851

PART 1: GENERAL INFORMATION

Privacy, Compliance and Training Branch (PCT) intake number / PIA file number:

Initiative title:	ServicesNow – Genesys Cloud
Ministry:	Ministry of Health
Branch or unit:	Health Insurance BC
Your name and title:	Vinicius Cid, Sr. Privacy Analyst
Your email:	Vinicius.cid@gov.bc.ca
Initiative Lead name and title:	~~Rod~~ Rob Broadbent, Director, Technology Solutions
Initiative Lead email:	~~Rod~~Rob.broadbent@gov.bc.ca
Ministry Privacy Officer:	Quinn Fletcher
MPO email:	MOH.privacy.officer@gov.bc.ca

Your MPO will complete the questions in the table below.

FOR MPO USE ONLY
Is this a PI or non-PI assessment?
PI
Is this initiative a data-linking program under FOIPPA?
No
Is this initiative a common or integrated program or activity under FOIPPA?
No
Related PIAs, if any:
CITZ21029 – Services BC-Health Helpdesk
Does this initiative involve disclosures of sensitive personal information outside of Canada?

Commented [WM1]: ServiceNow?

Commented [CVCH2]: Provisional - confirm once PIA goes back to HIBC

Commented [JM3]: To Vini – PIA not available on Ministry SP, are you able to provide us with this document?

No
Provide a brief summary of the initiative to be published in the Personal Information Directory. This summary may be similar to the answer to question 1.
As part of implementing the HIBC Integrated Transition and Transformation Plan (ITTP) - Contact Centre and IVR, the Genesys Cloud solution is selected to be the new ~~the~~ contact centre system for the HIBC program upon transition from Maximus to Pacific Blue Cross Solutions (PBCS). Genesys Cloud is a call center software offered as a SaaS solution, and there will be integration between the HIBC contact centre system, the IVR and Service BC's HCCS as it is the case today. Currently, Maximus operates the HIBC contact center using Cisco Contact Manager which is hosted in the Maximus data centre.
Is there an Information Sharing Agreement as part of this initiative? If yes, please have the Information Sharing Agreement Supplement attached to this PIA when submitting to PCT.

1. What is the initiative?

Service BC (SBC) delivers provincial government services and information at the SBC Provincial Contact Centre (CC) to residents and clients throughout British Columbia (BC). The CC also provides direction to government websites and online services. The CC provides services on behalf of the Ministry of Health (MoH), in particular assistance related to the Medical Services Plan (MSP) and the PharmaCare prescription program. Health Insurance BC (HIBC) administers the day-to-day operations of these programs on behalf of the MoH; they also manage the health-related CC operations.

Previously, MAXIMUS had been contracted to operate CC services delivered by HIBC and used their own technical infrastructure to that end. Now, Pacific Blue Cross Solutions(PBCS) is being onboarded on that role. While health services delivered by the CC will remain the same, there will be changes to the software being used.

The Genesys Cloud solution has been selected by PBCS to be the new the CC system for the HIBC program. Genesys is a call center software offered as a SaaS solution, and there will be

integration between the HIBC contact centre system, the IVR and Service BC's HCCS like in the current solution. Genesys will replace the MAXIMUS-operated Cisco Contact Manager, which is hosted in their own data centers.

By selecting Genesys Cloud as the HIBC contact centre replacement application, PBCS is leveraging a state-of-the-art cloud-based solution, and is poised to implement a wide variety of new service offerings and transformation opportunities with respect to caller experience, workforce management, quality assurance, live agent support and IVR.

The HIBC contact centre will be formally transitioned upon assumption of service, currently scheduled for April 2023, and will continue throughout the duration of the PBCS-HIBC contract with the Ministry of Health.

Commented [SC4]: Factual?

2. What is the scope of the PIA?

This PIA deals with PBCS' onboarding as operators of HIBC's contact center, and their introduction of Genesys Cloud to replace the existing call center software solution by MAXIMUS. This PIA will not reassess contact center operations, which is documented in CITZ21029.

3. What are the data or information elements involved in your initiative?

Genesys, upon PBCS assumption of service, will collect PI data in call logs and call recordings. This could include the following:

- Citizen's Name
- Personal Health Number (PHN)
- Birth Month and Year
- Month, Day and Year of Service
- Practitioner Number
- Payment Number
- Assignment Effective Date Month, Day and Year
- Facility Number
- Appointment Date Month, Day and Year

Commented [CVCH5]: I'm wondering whether any of the infosys integrations currently available to CC agents will change as a result of the PBCS transition (e.g. will they have access to more/less/different systems to validate information or do their jobs, aside from Genesys?)

Commented [WM6R5]: In terms of Genesys Cloud, there are no system integration with other information systems.

- College of Pharmacists ID
- MSP Billing Number
- Drug Identification Number

No additional information is expected to be collected, used and/or disclosed as a result of the PBCS transition and introduction of Genesys Cloud.

3.1 Did you list personal information in question 3?

Personal information is any recorded information about an identifiable individual, other than business contact information. Personal information includes information that can be used to identify an individual through association or reference.

Yes.

4. How will you reduce the risk of unintentionally collecting personal information?

N/A

PART 2: COLLECTION, USE AND DISCLOSURE

5. Collection, use, and disclosure

Commented [CVCH7]: Table built assuming there's no net new PI collection/use/disclosure being introduced, merely a change due to the introduction of PBCS and Genesys.

Commented [WM8R7]: Correct

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: Citizens' calls will be recorded by Genesys as part of the contact center's operations to deliver health services to them.	Collection	26 (a),(c) [27(1)(e), 27(1)(c)(iii)	Pharmaceutical Services Act s. 22 (1)

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
The calls will often contain PI as citizens provide personal information related to MSP or PharmaCare services.			
Step 2: Certain PBCS staff may access logfiles and call recording for investigation and training purposes. Contents of logfiles and call recordings are not stored or passed to any other Genesys components.	Use	32(a)	

Commented [CVCH9]: I'll need more details to understand how recordings are managed - e.g. if they're not being stored, how are PBCS staff accessing them - listening in live, for instance?

Commented [WM10R9]: The recordings are being stored. The statement is specific about the recordings are being stored in the same Genesys Cloud system.

6. Collection Notice

The PBCS onboarding and introduction of Genesys will not change what citizens hear when they call the contact center. The collection notice will remain as follows:

Commented [CVCH11]: Confirm - verbiage borrowed from existing call center process

Commented [WM12R11]: Please see the notice with a slight difference.

~~*"The personal information you provide will be collected for the purpose of enrolment in the Medical Services Plan, Pharmacare, as well as providing a range of services related to provincial health programs. Personal information is collected under the authority of, the Pharmaceutical Services Act and section 26 (a) and (c) of the Freedom of Information and Protection of Privacy Act ("FOIPPA"). Information may be disclosed pursuant to section 33 of FOIPPA. If you have any questions about the collection and use of your personal information, please contact the Health Insurance BC Chief Privacy Office, Health Insurance BC Chief Privacy Office PO Box 9035 Station Provincial Government Victoria, BC V8W 9E3 or call 604 683-7151 (Vancouver) or 1 800 663- 7100 (toll-free). To hear this message again, press pound. To continue press 1."*~~

Commented [JM13]: Is it Maximus former privacy notice?

"The personal information you will provide will be collected for the following purposes: Enrolment in the Medical Services Plan and Application for a BC Services Card and its authorized

programs. Personal information is collected under the authority of the Medicare Protection Act and section 26 (c) of the Freedom of Information and Protection of Privacy Act ("FIPPA"). Information may be disclosed pursuant to section 33 of FIPPA. If you have any questions about the collection and use of your personal information, please contact: The Health Insurance BC Chief Privacy Office, Health Insurance BC, Chief Privacy Office, PO Box 9035 Station Provincial Government , Victoria, BC V8W 9E3 or call 604 683-7151 (Vancouver) or 1 800 663-7100 (toll-free). Your call may be recorded for quality assurance and training purposes. To hear this message again, press pound. To continue, press 1."

Commented [SC14]: Is the purpose also for making general medical inquiries? Confirm actual purpose and seek compliance with FIPPA Freedom of Information and Protection of Privacy Act (gov.bc.ca)

FOR MPO USE ONLY

If applicable, list the exception to a collection notice.

PART 3: STORING PERSONAL INFORMATION

7. Is any personal information stored outside of Canada?

No.

8. Does your initiative involve sensitive personal information?

Yes.

9. Is the sensitive personal information being disclosed outside of Canada under FOIPPA section 33(2)(f)?

No.

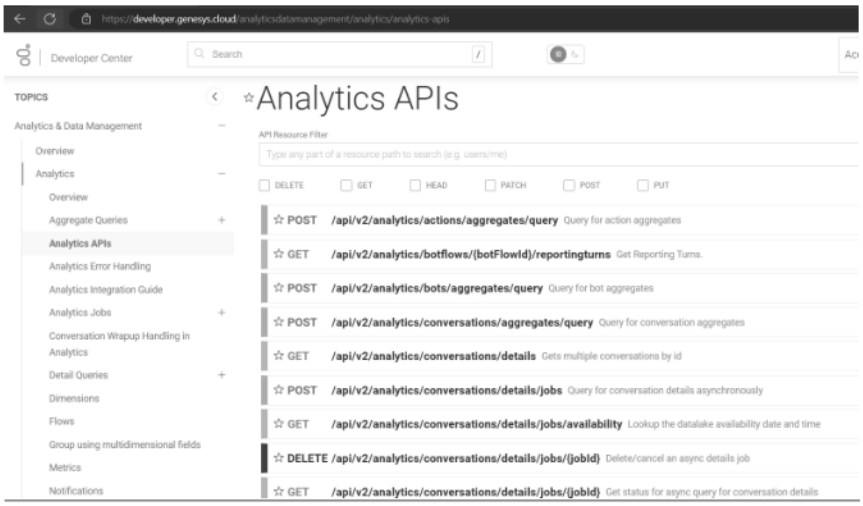
10. Where and how are you storing the personal information involved in your initiative?

Genesys Cloud is comprised of micro services running in a multi tenant environment, it does not have a database, its data is stored in JSON objects. The two Amazon (AWS) datacentres for the Canadian region are in Montreal and Toronto. Data can be extracted from the application through the use of RESTAPI calls which Genesys provides through its developer tools:

Commented [CVCH15]: Confirm w/ PBCS whether data is stored in Canada and if so, where/how

Commented [WM16R15]: Added

Commented [JM17]: Ming/Darlington – To confirm interplay between Genesys Cloud and provider E3



PART 4: ASSESSMENT OF DISCLOSURES OUTSIDE OF CANADA

N/A

PART 5: SECURITY OF PERSONAL INFORMATION

11. Does your initiative involve digital tools, databases or information systems?

Yes.

18.1 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.

Commented [CVCH18]: Presumably so - confirm whether STRA has been initiated

Commented [WM19R18]: Yes

12. Are all digital records stored on government servers and are all physical records stored in government offices with government security?

Commented [CVCH20]: Possibly not - check w/ PBCS

Commented [WM21R20]: No physical records are stored. All digital records are stored on the Genesys Cloud platform.

13. 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.

Strategy	
We allow employees only in certain roles access to information	X
Employees that need standing or recurring access to personal information must be approved by the appropriate authority	X
We use audit logs to see who accesses a file and when	X
Describe any additional controls:	

PART 6: ACCURACY, CORRECTION, AND RETENTION

In Part 6 you will demonstrate that you will make a reasonable effort to ensure the personal information that you have on file is accurate and complete.

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

FOIPPA section 28 states that a public body must make every reasonable effort to ensure that an individual's personal information is accurate and complete.

15. Requests for correction

FOIPPA gives an individual the right to request correction of errors or omissions to their personal information. You must have a process in place to respond to these requests.

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

Type "yes" or "no" to indicate your response.

22.2 Sometimes it's not possible to correct the personal information. FOIPPA requires that you make a note on the record about the request for correction if you're not able to correct the record itself. Will you document the request to correct or annotate the record?

Type "yes" or "no" to indicate your response.

Commented [CVCH22]: For this part, it might suffice to say that the Call center would be using the same process as they had been using under MAXIMUS - confirm w/ PBCS if that's the case.

Commented [WM23R22]: Correct

Commented [AAS24R22]: NEW: It seems part 6 needs to be completed. Per the comments above, there seems to be no difference from what was done with Maximus. Does the referenced PIA - CITZ21029 - speak to this process? Can I copy and paste from it?

Commented [JM25]: Suggestion to provide additional details on the same process, for accountability reasons. Need to have a self supporting document in a 5 years time.

22.3 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 recipient of the request for correction. Will you ensure that you conduct these notifications when necessary?

Type "yes" or "no" to indicate your response.

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

Type "yes" or "no" to indicate your response.

- If yes, go tobookmark:// foippa_requires_that/ question 24
- If no, skip ahead to Part 7

17. Do you have an approved information schedule in place related to personal information used to make decisions?

FOIPPA requires that ministries keep personal information for a minimum of one year after it is used to make a decision about an individual. In addition, the Information Management Act requires that you dispose of government information only in accordance with an approved information schedule or with the approval of the Chief Records Officer.

Type "yes" or "no" to indicate your response.

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.

PART 7: PERSONAL INFORMATION BANKS

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

18. Will your initiative result in a Personal Information Bank?

N/A

Commented [CVCH26]: No net new PIB expected.

PART 8: ADDITIONAL RISKS

19. Risk response

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

Add new rows if necessary.

Possible risk	Response
Risk 1: Storage and/or disclosure outside of Canada due to Genesys being hosted in cloud servers that may be accessed by parties outside of the country.	
Risk 2: Personal information within recorded calls exposed improperly	Ability to listen to recorded calls will only be granted to Supervisor and Quality Assurance (QA) roles. Any access requests for these two roles will be reviewed and approved by the Manager via the Access Management process facilitated by the ServiceNow tool. Conversely, any staff offboarding would be accompanied by removal of all their access to the system and recorded calls.
Risk 3:	

Commented [CVCH27]: May not be a risk at all - confirm w/ PBCS

Commented [WM28R27]: Correct

Commented [CVCH29]: Here I just need to understand how access to recordings are managed, and the purpose for said access being granted.

PART 9: SIGNATURES

You have completed a Privacy Impact Assessment. PCT will review, comment and sign this document first before returning it to your program area for signatures.

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

PCT Summary

This section summarizes PCT's review of the PIA and identifies decisions made that are not otherwise noted.

PCT Comments:

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			
PCT Manager or Director Only required if personal information is involved			

Ministry Signatures

This PIA accurately documents the data elements, information flow, and information about disclosure and storage outside of Canada at the time of signing. If there are any significant 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.

Please ensure that you have reviewed the privacy risks and risk responses in Part 4: Assessment of Disclosures Outside of Canada.

Ministry Comments

Role	Name	Electronic signature	Date signed
Initiative Lead			

Role	Name	Electronic signature	Date signed
Assistant Deputy Minister or designate Only required if personal information is involved			

	Name	Electronic signature	Date signed
Ministry Information Security Officer Only required if MISO was involved in conducting the PIA			

Section One

1) ***Who is involved*** *in this project/program?*
    - *Please specify:*
        - Programs/branches within the Ministry:
            - All Ministry branches that serve providers, pharmacies and beneficiaries falling under the Medical Services Division and the Pharmaceutical Services Division
        - External partners
            - Service BC – Health Contact Centre Services

2) *Provide a* ***description*** *of the project/program.*

    As part of implementing the HIBC Integrated Transition and Transformation Plan (ITTP) - Contact Centre and IVR, the Genesys Cloud solution is selected to be the new the contact centre system for the HIBC program upon transition from Maximus to Pacific Blue Cross Solutions (PBCS). Genesys Cloud is a call center software offered as a SaaS solution, and there will be integration between the HIBC contact centre system, the IVR and Service BC's HCCS as it is the case today. Currently, Maximus operates the HIBC contact center using Cisco Contact Manager which is hosted in the Maximus data centre.

3) *What is the* ***purpose*** *of this project/program?*
    - What problem are you trying to solve? At its foundation, PBCS is taking responsibility for HIBC contact centre services for the Ministry of Health
    - What will be the benefit? By selecting Genesys Cloud as the HIBC contact centre replacement application, PBCS is leveraging a state-of-the-art cloud-based solution, and is poised to implement a wide variety of new service offerings and transformation opportunities with respect to caller experience, workforce management, quality assurance, live agent support and IVR. Genesys Cloud is currently used by PBC today, this product implementation will benefit from the breadth of existing mature business practices.

4) *What is the* ***start date*** *for the project/program?*

    Project work, beyond detailed planning, on behalf of the HIBC contact centre transition will begin immediately upon acceptance of this PIA.

5) *What is the* ***end date*** *(if applicable)? Alternately, specify if this will be an* ***on-going*** *program.*

    The HIBC contact centre will be formally transitioned upon assumption of service, currently scheduled for April 2023, and will continue throughout the duration of the PBCS-HIBC contract with the Ministry of Health.

6) *Are you aware of any* ***previous privacy impact assessments*** *that have been completed that are related to this project/program?*

    A PIA for the current HIBC IVR was submitted by Maximus.

Section Two

Additionally, the following details will be necessary to complete a PIA. It is ok if you do not have these details figured out yet. Our office is happy to assist you on these details, if you are not able to provide them currently.

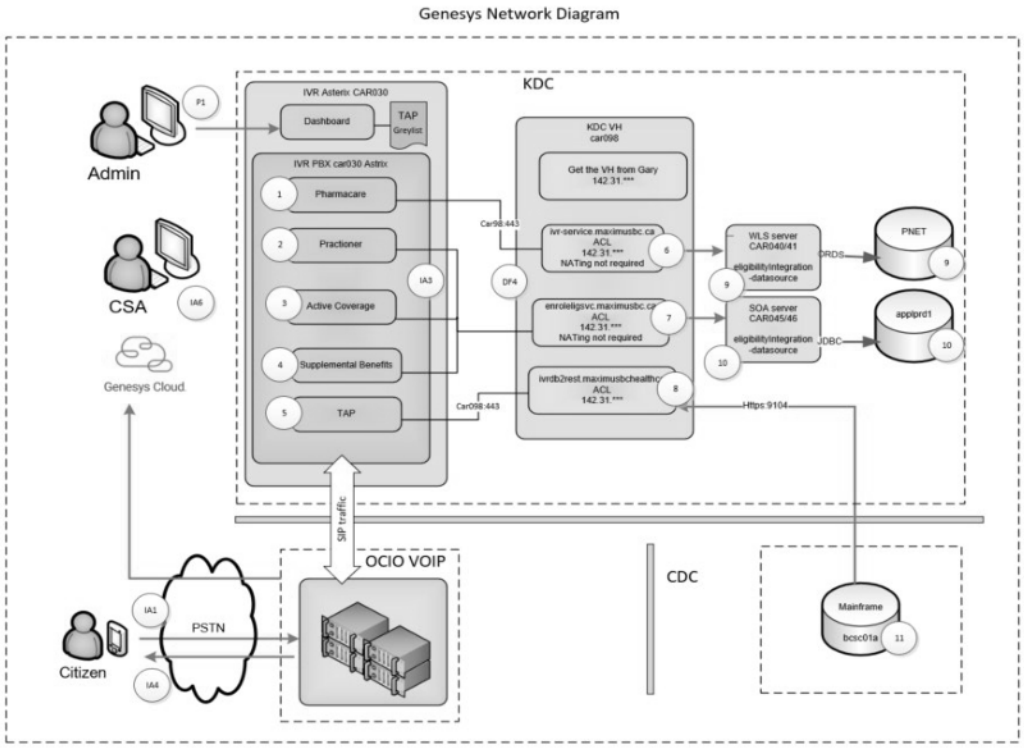
1) What **types of personal information** will be collected used or disclosed in this project/program?

   Genesys, upon PBCS assumption of service, will collect PI data in call logs and call recordings. This could include the following:

   - Citizen's Name
   - Personal Health Number (PHN)
   - Birth Month and Year
   - Month, Day and Year of Service
   - Practitioner Number
   - Payment Number
   - Assignment Effective Date Month, Day and Year
   - Facility Number
   - Appointment Date Month, Day and Year
   - College of Pharmacists ID
   - MSP Billing Number
   - Drug Identification Number

2) A **data flow description** that details the entire "*information life cycle*" from creation/collection to retention/destruction. Think about every step that will be taken, by whom, using what tools, when handling the data, etc.

   Genesys Network Diagram



Description	Data Contents	PI Control
• **Callers reach the contact centre agents via the self-service Interactive Voice Response (IVR) for the following use cases. During the calls, callers may be asked to provide PII data as stated in the previous question (see above)** ○ **Pharmacy Application** ○ **Practitioner Information Application** ○ **Practitioner Information Application** ○ **Travel Assistance Application** ○ **Active Coverage Application** ○ **Supplementary Benefits Application**	• The PII data may be included in the logfiles, and call recordings stored within the Genesys platform. • Leaders (team supervisors, QA supervisors, managers and administrators) may access the logfiles and call recording for investigation and training purposes. • The contents of the logfiles and call recordings are not stored and are not passed (in raw form) to any other components.	• Only Leaders (team supervisors, QA supervisors, managers and administrators) are granted access to the logfiles and call recordings. They will access the data via Genesys platform.

3) If you are collecting personal information directly from an individual, do you provide the individual with a collection notice?

   Yes

4) Will there be an **Information Sharing Agreement** associated with this project/program?

   No

5) What are your procedures and processes for **securely storing and/or sharing the information?**

   Only Leaders (team supervisors, QA supervisors, managers and administrators) are granted access to the logfiles and call recordings. They will access the data via Genesys software.

6) If applicable, you may need to have procedures in place to enable individuals to **update or correct** their own personal information. If you do have procedures, please describe them here.

   N/A