Office of the Information and Privacy Commissioner of Alberta

Privacy Impact Assessments

AFNIGC - Privacy Education Series

September 27, 2017

Chris Stinner
Senior Information and Privacy Manager
Office of the Information and Privacy Commissioner of Alberta

Schedule

- PIA 5Ws
- PIA Drafting Process
- PIA Components
- Information Flows
- Privacy Risk Analysis
- Risky Practices (scenarios)
- Odds and Ends

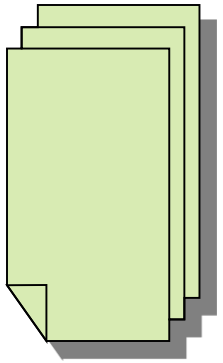
(break around here)

PIA 5Ws


THIS LOOKS LIKE A GREAT IDEA, MIKE! DID YOU REMEMBER TO DO A PIA?
PIA?! PERSONAL INCOME ACCOUNTING?! PUBLIC INPUT ARRANGEMENT?! PRIVATE INVESTIGATION AGENCY?! PRETTY INTERESTING ANECDOTE?!
ATIP

What is a PIA?

- A Privacy Impact Assessment evaluates how a project will affect privacy
- A comprehensive risk assessment
- A PIA is an exercise in due diligence
- A PIA is prospective
- A written report that may be:
  - Submitted to a 3rd party for review
  - Used as an internal reference
  - Hopefully not forgotten...!



A PIA is not…

- Project charter
- Technical architecture
- Contract
- Security assessment
- Marketing bumf
- (Although it has elements of all of the above)
- Get out of jail free card

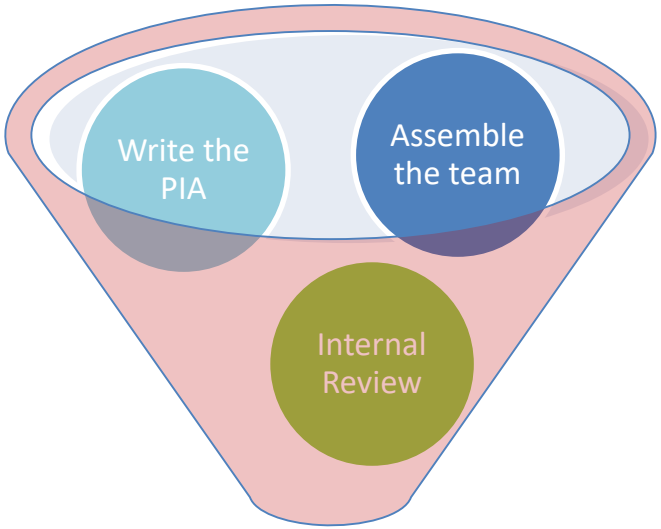
Why do a PIA?

- Risk mitigation
- Saves time and money
- Confirms legal authority to collect, use, and disclose personal information
- Marketing/communications
- Ethics
- Sometimes you have to!

Mandatory triggers…

- *Health Information Act*
  - Mandatory for proposed systems and practices that collect, use or disclose identifiable health information (section 64)
- Usage-based Insurance
  - Superintendent of Insurance requirement
- Provincial Ministry policies

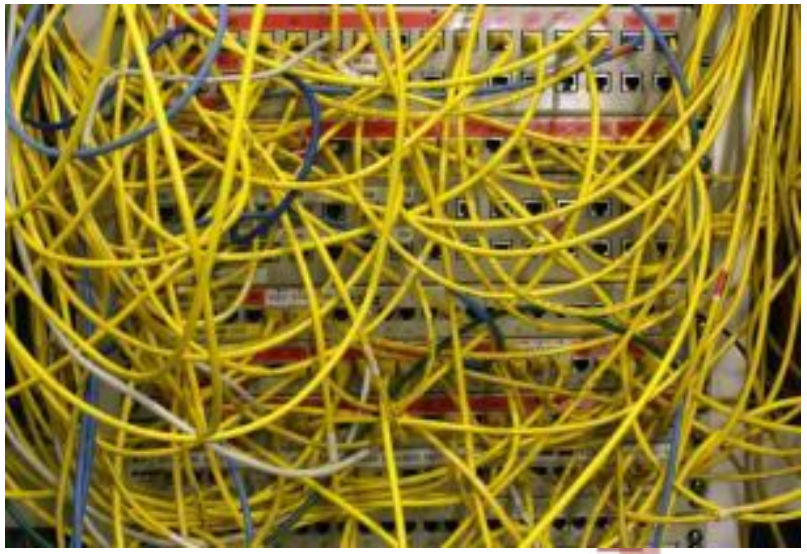
PIA Drafting Process



Who should write a PIA?

- Someone with an intimate understanding of your business, who knows privacy law, your regulatory environment, technology, risk analysis, security, records management, project management, communications and who can achieve executive buy-in

- Or you can assemble a team…
  - Privacy lead
  - Business area
  - Legal counsel
  - Information technology
  - Records management
  - Communications



Timing

- When to start writing PIA
  - Too early?
  - Too late?
- Privacy should be considered when developing business requirements
- Start considering privacy early
- PIA simply becomes a matter of documenting the privacy design

PIA Components

- A Project Overview
- B Privacy Management
- C Project Privacy Analysis
- D Project Privacy Risks and Mitigation Plans
- E Policy and Procedure Attachments

PIA Requirements Document

- The OIPC guide contains the format and will guide you as to what information is required for each section.

- Available at:
  - OIPC homepage > PIAs > PIA Requirements
  - Or at: https://goo.gl/xYFLCl

[A] PIA Overview

- Provides a brief overview of the project to be assessed
  - Considerations
  - Amendment to previous PIA
  - Previous related submissions
- Key parts of the project or initiative
  - Key players
  - Business rationale for the project
  - Where will health information be stored or accessed

[B] Privacy Management

- Addresses your overall privacy management within your organization
- Organizational structure
  - Who is responsible for privacy
- How your organization manages privacy
  - How employees are trained in privacy
  - How privacy policies are developed and implemented
  - Incident response

[C] Project Privacy Analysis

- Focus on the privacy topics related to your project
- List the personal information/health information to be collected, used or disclosed
- Information flow diagram and Legal authorities table
- Notice
- Consent
- Data matching Contracts and agreements
- Is information leaving Alberta?

[D] Project Privacy Risk Mitigation

- Access controls
  - Who will have access to the information
  - How many people will have access
  - Will access be the same for all individuals
- Authentication of users
- Privacy risk assessment and mitigation plans
- How compliance will be monitored
- PIA compliance

[E] Policies and Procedures

- Attach copies of policy documents to your PIA
- General privacy policies
- Project specific policies
- Privacy policy table

Policies and Procedure Examples

Privacy accountability
Access to Health Information
Correction requests
Training and awareness
Collection of Health Information
Use of Health Information
Disclosure of health information
Research
Third parties
PIA’s
Records retention and disposition

Records retention and disposition
Information classification
Risk assessment
Physical security of data and equipment
Network and communications security
Access Controls
Monitoring and auditing
Incident response
Business Continuity
Change control
Project specific policies

Elements of a good PIA

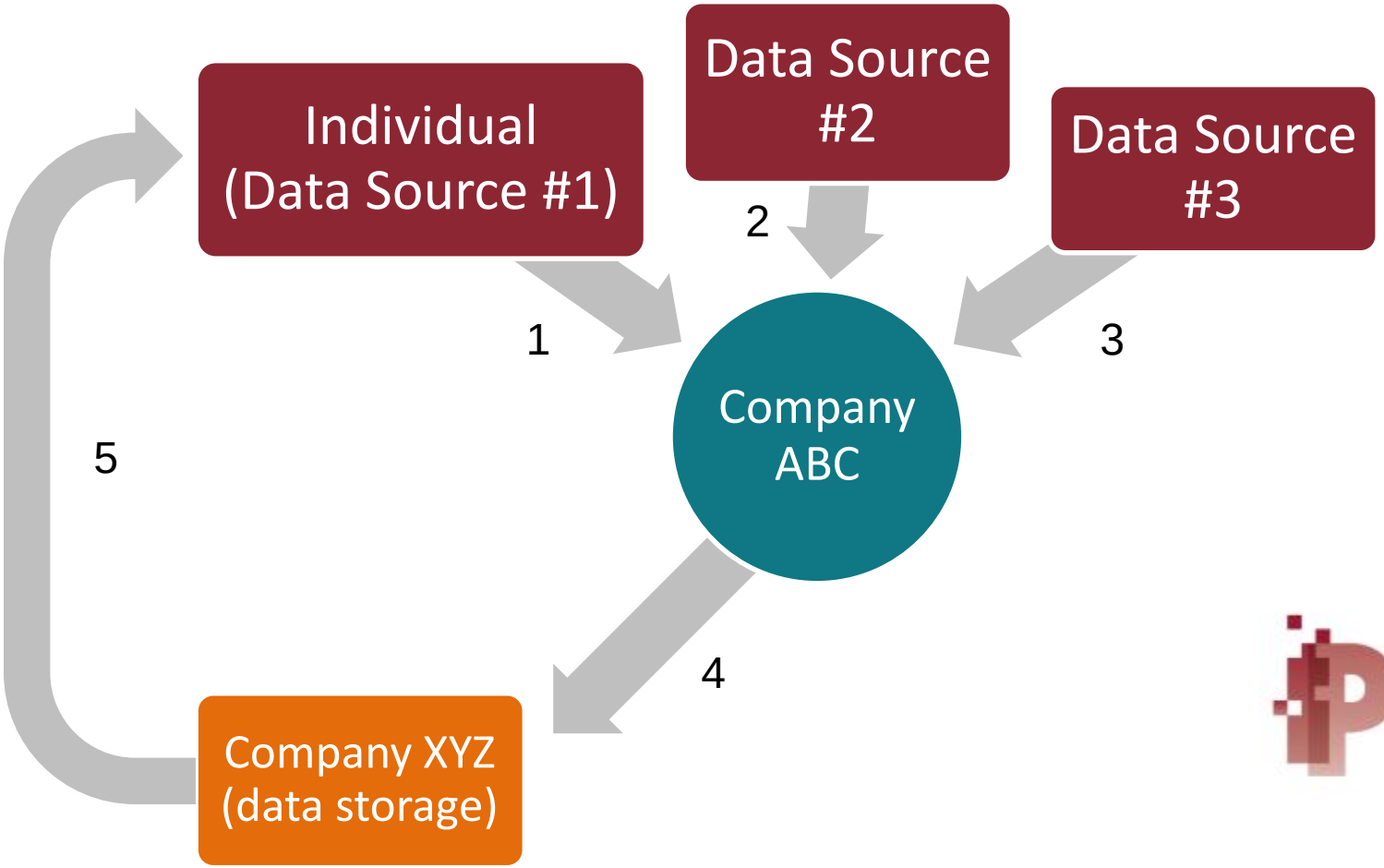
- Description of privacy organization
- Is there a “privacy culture?”
- Overview of the project and benefits
- Legal authority to collect, use and disclose personal or health information
- Information flow
- Analysis of privacy risks and mitigations
- Communications & consultation
- Review & compliance plans

Information Flows

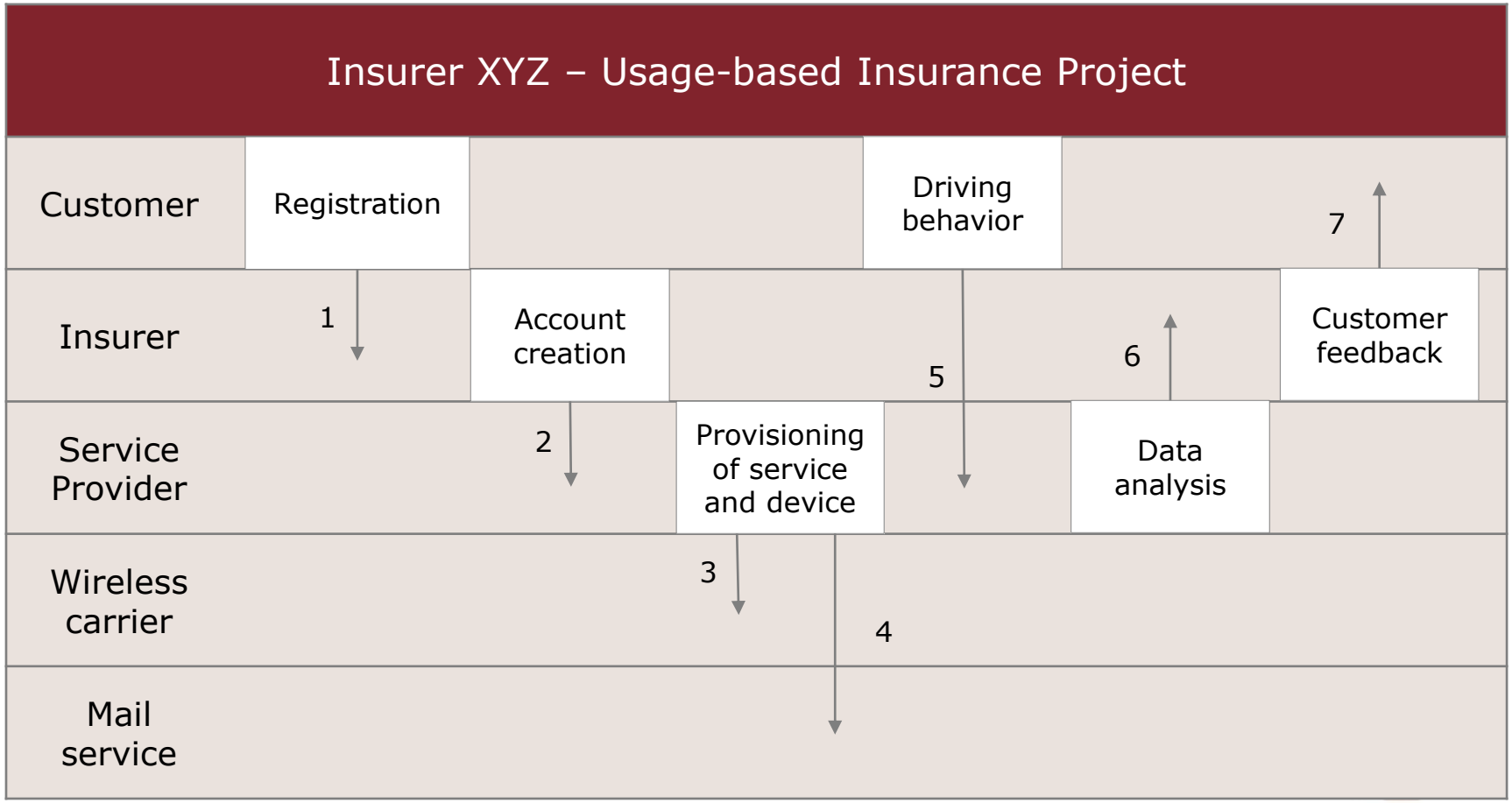
- Information Flow Diagrams

- Legal Authorities and Purposes Table

The heart of a good PIA: Information flow diagram



Example information flow



Tips for a good information flow diagram

- Keep it simple
- Important to reflect information crossing organizational boundaries
- Incorporate a narrative
- Label information flows
- These can be referenced in legal authorities, privacy risk assessment, mitigation plan, and elsewhere

Legal Authorities Table

Info Flow #	Description	Type of Information	Purpose	Legal Authority
1	Customer registers for program	Name, DOB, DL #, address, phone #, driving history, claims history, bank account #	personal information collected to sign up customer	Individual Consent
2	Registration validated and account created/modified	Name, address	Validate registration and get customer the telematics device they need	Section 16 of PIPA

Privacy Risk Analysis

- Risk Analysis
- Risk Considerations
- Risk Mitigation Table
- Examples

The Brains of a good PIA: Risk analysis & mitigation

- Identify potential threats to privacy
  - Consider impact and magnitude
  - Should be project-specific
- Determine ways to reduce risk
  - Mitigate
  - Transfer (hard to do for privacy)
  - Eliminate/Avoid
  - Accept
- **We recognize that you can't eliminate all risk**

Risk Mitigation Table

Privacy Risk	Description	Mitigation Measures	Policy Reference
What is the risk	Describe the risk	Administrative, technical and physical measures	Refer to policies and procedures that mitigate this risk.
…			

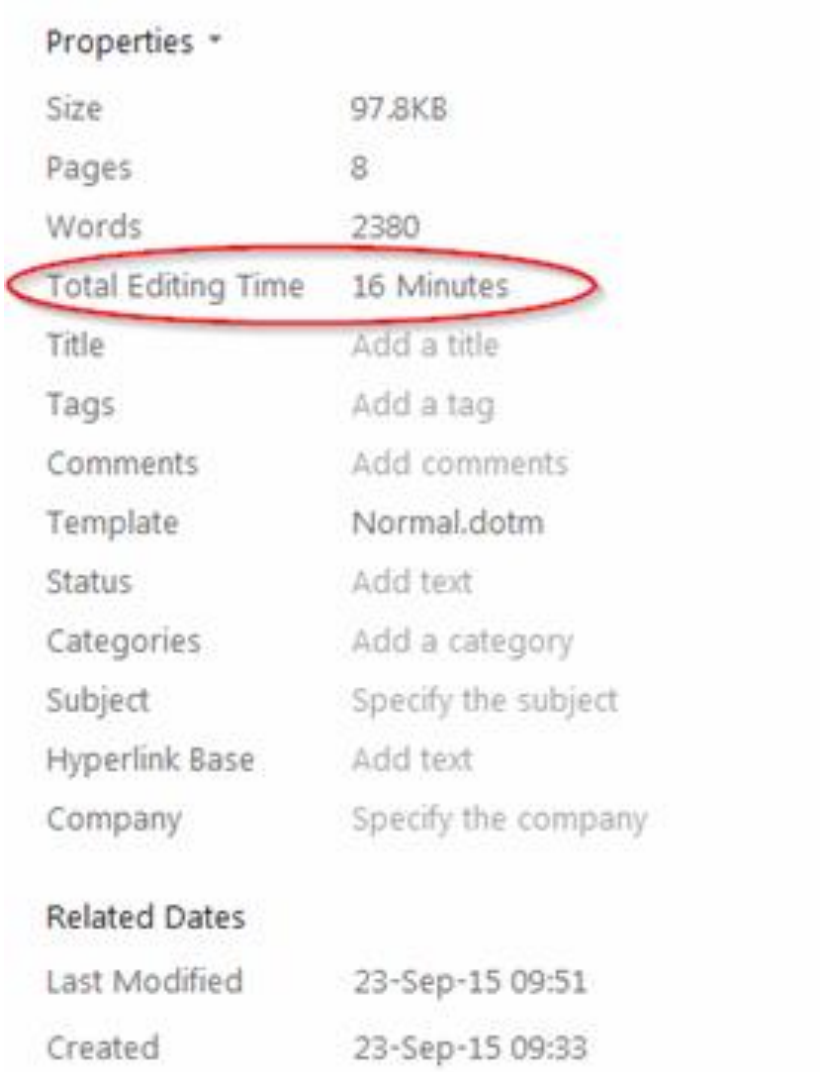
Sample Privacy risks

- Inappropriate use of data systems
- Information security risks
  - Confidentiality
  - Availability
  - Integrity
- Information management and retention
- Lack of privacy awareness among participants
- Secondary uses of data
- Public reaction to program

Odds and Ends

- The Bad
- The Ugly
- The Good
- The afterlife

Examples

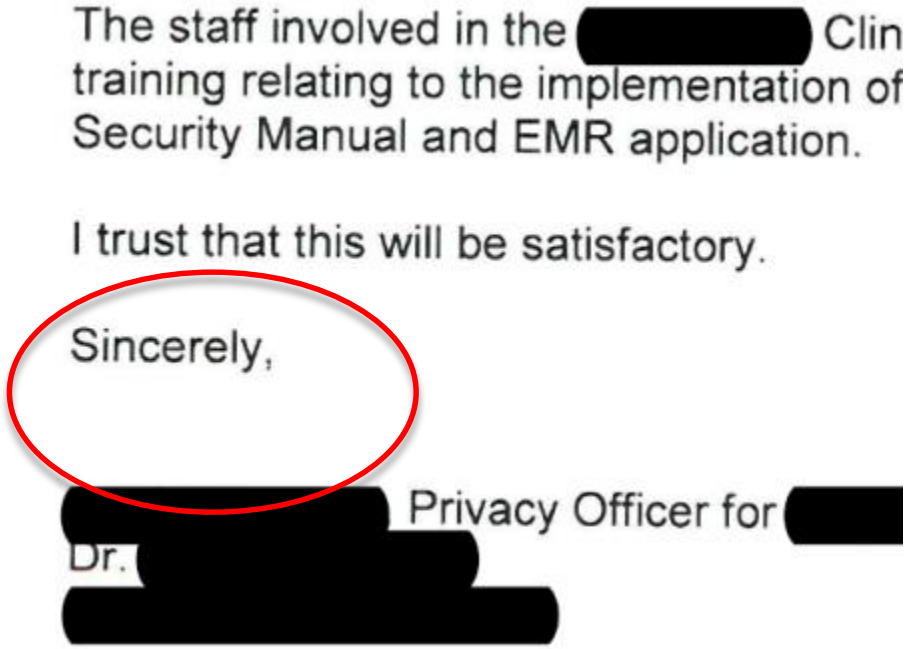


Properties

Size	97.8KB
Pages	8
Words	2380
Total Editing Time	16 Minutes
Title	Add a title
Tags	Add a tag
Comments	Add comments
Template	Normal.dotm
Status	Add text
Categories	Add a category
Subject	Specify the subject
Hyperlink Base	Add text
Company	Specify the company

Related Dates

Last Modified	23-Sep-15 09:51
Created	23-Sep-15 09:33



The staff involved in the [redacted] Clin
training relating to the implementation of
Security Manual and EMR application.

I trust that this will be satisfactory.

Sincerely,

[redacted] Privacy Officer for [redacted]
Dr. [redacted]

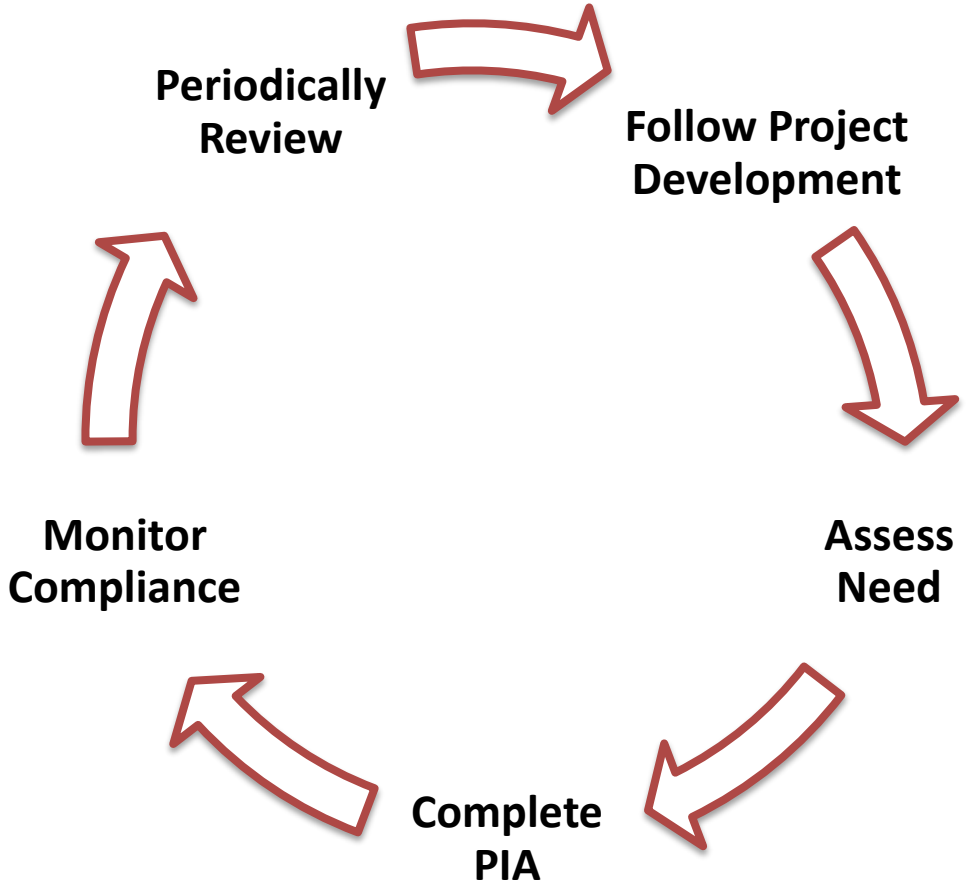
What happens after I submit my PIA?

- PIA received, then SIPM assigned to review
- SIPM may contact you with questions and/or to seek clarifications
- Process is meant to be collaborative and constructive
- OIPC review time: aim is to give preliminary results of review within 45 calendar days

PIA Acceptance

- Review goes on until acceptance
- Upon acceptance by the Commissioner's office, the organization receives a letter of acceptance
- "Acceptance" is not "approval"

The PIA's done…Now what?



Questions?

Office of the Information and
Privacy Commissioner of Alberta

Thank you!

Chris Stinner
Senior Information and Privacy Manager

Office of the Information and Privacy Commissioner of Alberta
410-9925 109 St NW
Edmonton, AB
T5K 2J8

https://www.oipc.ab.ca
@ABoipc
780 422 6860

Resources

- Privacy Impact Assessment Requirements
  https://www.oipc.ab.ca/action-items/privacy-impact-assessments.aspx

- Guidance for Electronic Health Record Systems
  https://www.oipc.ab.ca/resources/a-to-z.aspx?op=g&page=1

- Alberta Medical Association website
  https://www.albertadoctors.org/leaders-partners/emrs/privacy

- Service Alberta PIA templates
  https://www.servicealberta.ca/foip/resources/3540.cfm