

**ANNUAL REPORT
2021**

**OFFICE OF THE
INFORMATION AND PRIVACY
COMMISSIONER**

**PROVINCE OF PRINCE EDWARD
ISLAND**





Prince Edward Island Île-du-Prince-Édouard

Legislative Assembly

Information and
Privacy Commissioner
PO Box 2000, Charlottetown PE
Canada C1A 7N8

Assemblée législative

Commissaire à l'information et
à la protection de la vie privée
C.P. 2000, Charlottetown PE
Canada C1A 7N8

March 3, 2023

The Honourable Colin LaVie, MLA
Speaker of the Legislative Assembly
Province of Prince Edward Island
P.O. Box 2000
Charlottetown, PE
C1A 7N8

Honourable Speaker:

I am pleased to present to you the enclosed 2021 Annual Report of the Office of the Information and Privacy Commissioner, for the period January 1, 2021 to December 31, 2021. This is the nineteenth report from this office and is submitted to you pursuant to subsection 59(1) of the *Freedom of Information and Protection of Privacy Act*.

Sincerely,

Signed: *Denise N. Doiron*

Denise N. Doiron
Information and Privacy Commissioner

Enclosure

DND/kj

TABLE OF CONTENTS

Page

I. Commissioner’s Message	1
II. Overview of the OIPC	3-4
Staff	4
Mandate	4
Mission	4
Vision	4
Values	4
III. Legislative Responsibility	5
<i>Freedom of Information and Protection of Privacy Act (“FOIPP Act”)</i>	5
<i>Health Information Act (“HIA”)</i>	5
IV. Commissioner’s Decisions	6-22
Decisions under the <i>FOIPP Act</i>	6-21
1. Refusals to conduct an inquiry	6
2. Decisions resulting from advice requested by public bodies	7
3. Decisions resulting from access reviews	8-11
4. Decisions resulting from privacy complaints	12
5. Voluntary breach reports.....	13-21
Decisions under the <i>HIA</i>	22
1. Decisions resulting from access reviews	22
2. Decisions resulting from privacy complaints	22
3. Decisions resulting from mandatory breach reporting.....	22
V. Privacy Impact Assessments.....	23-24
VI. Financial Information	25
Budget	25
VII. Statistics.....	26-28
Table A: Requests for Review, <i>FOIPP Act</i>	26
Table B: Privacy Complaints, <i>FOIPP Act</i>	27
Table C: Reviews, <i>HIA</i>	28
Statistics of Public Bodies	29
Appendix A: Part I Public Bodies, Access Requests and Reviews	30
Appendix B: Part II Public Bodies, Access Requests and Reviews	31
Appendix C: Part III public bodies - Access Requests and Reviews	32



**OFFICE OF THE INFORMATION
AND PRIVACY COMMISSIONER**

Commissioner's Message:

2021 was my first full year as Information and Privacy Commissioner, and it was an interesting year. The COVID-19 pandemic continued for an unprecedented second year and continues presently. Our office has continued to weather the pandemic fairly well and experienced minimal disruptions throughout 2021. We appreciated the flexibility of having the option to work remotely if necessary, as a result of the upgrades to our equipment in late 2020.

It was a record year for our office in several aspects. We had a record number of new files opened and more Privacy Impact Assessments submitted for review than in any other year, and increased numbers of requests from public bodies seeking decisions on authorization to extend the time they have to respond to an access request. We also reached a record high in the number of files we were able to close throughout the year. However, although we closed a record number of files in 2021, the new and continuing files exceeded the number we were able to close. Consequently, at the end of 2021 we had more files carried over into 2022 than ever before.

Our office has experienced a significant increase in workload and an increase in the complexity of issues. As a result, we have struggled to keep up with the work required with our present level of staffing. The Legislative Management Committee recognized the need for increased resources for our office and recommended funding be added to our budget to allow for the addition of two new staff, which was approved by the Legislative Assembly for the 2022-23 budget year. We are grateful for the recognition of need for more resources within our office, and the support to assist in addressing that need.

We have a number of changes and improvements planned for the next few years, with a view to modernizing our office, improving efficiency, and addressing the growing backlog. I look forward to outlining our plans and providing details on our progress in next year's report.

Respectfully submitted,

Denise N. Doiron,
Information and Privacy Commissioner

Overview of the OIPC:

The Information and Privacy Commissioner is an independent officer of the Legislative Assembly, appointed on the recommendation of the Standing Committee on Legislative Assembly Management. The appointment is for a term of five years, by resolution of the Legislative Assembly, supported by at least two-thirds of the members present. The Commissioner's oversight responsibilities are grounded in these purposes of the *Freedom of Information and Protection of Privacy Act* ("the FOIPP Act"):

- *to allow any person a right of access to the records in the custody or under the control of a public body subject to limited and specific exceptions as set out in this Act;*
- *to control the manner in which a public body may collect personal information from individuals, to control the use that a public body may make of that information, and to control the disclosure by a public body of that information;*
- *to allow individuals, subject to limited and specific exceptions as set out in this Act, a right of access to personal information about themselves that is held by a public body;*
- *to allow individuals a right to request corrections to personal information about themselves that is held by a public body; and*
- *to provide for independent reviews of decisions made by public bodies under this Act and the resolution of complaints under this Act.*

and these purposes of the *Health Information Act* ("the HIA"):

- *to establish a set of rules for custodians regarding the collection, use, disclosure, retention and secure destruction of personal health information that protects the confidentiality of personal health information and the privacy of the individual to whom the personal health information relates;*
- *to enable personal health information to be shared and accessed, where appropriate, for the better provision of health services and the planning and management of the health care system;*
- *to provide an individual with the right to examine and receive a copy of the individual's personal health information maintained by a custodian, subject to limited and specific exceptions, as set out in this Act;*
- *to provide an individual with the right to request the correction of or amendment to the individual's personal health information maintained by a custodian, as set out in this Act;*
- *to establish mechanisms to ensure the accountability of persons having custody or control of personal health information and to safeguard the security and integrity of the personal health information in their custody or control;*
- *to provide for an independent review of decisions made by custodians and the resolution of complaints made with respect to custodianship of personal health information; and*
- *to provide effective remedies for contraventions of this Act.*

Staff:

In 2021, we were a three-person office, consisting of the Information and Privacy Commissioner, the Adjudicator and an Administrative Assistant. The plan is to increase the office compliment to five within the next year or two, with the addition of a Case Management Officer and Investigator.

Mandate:

The Information and Privacy Commissioner provides independent oversight of decisions of public bodies under the *FOIPP Act* and custodians under the *HIA*. The independence of the office is vital for the proper fulfillment of the Commissioner's duties. The Commissioner is sworn to conduct the affairs of the office with an impartial approach. The Commissioner does not take sides between a given applicant or complainant and a public body or custodian. Rather, the Commissioner's role is to conduct an investigation to determine the facts, request submissions, and make findings in an impartial manner.

Mission:

In addition to fulfilling the purposes of the *FOIPP Act* and the *HIA*, the mission of the office also includes the following goals:

- To educate public bodies, health care custodians, and citizens regarding the principles of information access and privacy standards and rights established by the *FOIPP Act* and the *HIA*;
- To operate the office in a fiscally responsible manner, and to manage and conduct the office with respect, honesty and integrity; and
- To provide staff with a healthy work environment, and a challenging and flexible workplace that recognizes resourcefulness and dedication.

Vision:

The vision of the office is of provincial public bodies and health information custodians who foster a culture of openness, transparency and respect for personal privacy, and value the security of the personal information they hold.

Values:

Fairness, openness, transparency, and a respect for privacy are the broad values which guide the activities of this office.

Legislative Responsibility:

Freedom of Information and Protection of Privacy Act

Under the *FOIPP Act*, the Information and Privacy Commissioner is responsible for monitoring how public bodies administer the *FOIPP Act*, and for performing other duties to ensure that the purposes of the *FOIPP Act* are achieved.

The Commissioner's primary duties are to perform independent reviews of decisions of public bodies respecting access to information requests and requests for correction of personal information, and to investigate complaints that an individual's personal information has been collected, used, or disclosed by a public body in violation of the *FOIPP Act*.

In addition to the Commissioner's functions relating to reviews, the Commissioner performs other duties to ensure that the *FOIPP Act's* purposes are achieved, including:

- *conducting investigations to ensure compliance with any provision of the FOIPP Act or compliance with rules relating to the destruction of records set out in any other enactment of Prince Edward Island;*
- *making an order described in subsection 66(3) whether or not a review is requested;*
- *informing the public about the FOIPP Act;*
- *commenting on the implications for freedom of information or for protection of personal privacy of proposed legislative schemes or programs of public bodies;*
- *commenting on the implications for protection of personal privacy of using or disclosing personal information for record linkage;*
- *authorizing the collection of personal information from sources other than the individual the information is about;*
- *bringing to the attention of the head of a public body any failure by the public body to assist applicants under section 8; and*
- *giving advice and recommendations of general application to the head of a public body on matters respecting the rights or obligations of a head under the FOIPP Act.*
- *giving advice and recommendations to the head of a public body on any matter respecting any rights or duties under the FOIPP Act.*

Health Information Act

Since July 1, 2017, the Commissioner has been responsible for overseeing that health information of Islanders is dealt with by custodians in a manner consistent with the provisions of the *HIA*. The *HIA* sets out uniform requirements to protect the personal health information of Islanders while concurrently serving their health care needs. The intent of the proposed legislation is for health care custodians to permit Islanders access to their own personal health information, and to balance the protection of their personal privacy with the need to appropriately collect, use and disclose their personal health information.

Decisions under the FOIPP Act

Commissioner's Decisions, 2021:

Refusals to Conduct Inquiries:

Section 64(1) of the FOIPP Act permits the Commissioner to refuse to conduct an inquiry if, in the opinion of the Commissioner,

- the subject matter of a request for a review under section 60 has been dealt with in an order or investigation report of the Commissioner; or
- the circumstances warrant refusing to conduct an inquiry.

Refusal letters were written in relation to certain files but were not issued publicly. They are available to the public with personal information severed, but must be requested. One Order for a refusal to conduct an inquiry was issued by Commissioner Doiron in 2021:

RI-21-001, February 9, 2021, Re: Department of Agriculture and Land

An Applicant requested a review of the Public Body's decision in relation to an access to information request more than 60 days after the Applicant had been notified of the Public Body's decision. The Commissioner declined to allow an extension of time, pursuant to subclause 61(2)(a)(ii) and refused the request for review.

There are no specific criteria set out in the FOIPP Act for allowing an extension to the time for requesting a review. I must make a decision on whether to allow an extension based on reasonableness. I must also take into consideration procedural fairness to both the Applicant and the Public Body, as the intent of the legislation is not only to provide applicants with a right to request a review, but also to provide some degree of finality or closure around requests for access to information. Therefore, I must be persuaded that there is reasonable justification for the Applicant to have not made the request within the statutorily required time period.
- Commissioner, Order No. RI-21-001 at para 11

Decisions resulting from Advice requested by Public Bodies

Section 51 of the *FOIPP Act* permits the head of a public body to ask the Commissioner to give advice and recommendations on any matter respecting any rights or duties under the *FOIPP Act*.

One advice and recommendations decision was issued by Commissioner Doiron in 2021:

Order No. AR 21-001, January 5, 2021

Re: Department of Agriculture and Land

An Investigation Panel of the Island Regulatory and Appeals Commission was requested by the Minister of the Department of Agriculture and Land to conduct an investigation under the *Lands Protection Act*, R.S.P.E.I. 1988, Cap. L-5, and report to the Minister its findings and recommendations. The Public Body asked the Commissioner for advice and recommendations pursuant to section 51 of the *Freedom of Information and Protection of Privacy Act*, R.S.P.E.I. 1988, Cap. F-15.01 ("*FOIPP Act*"), regarding proactive disclosure of the report of the Investigation Panel.

The Commissioner recommended that the Public Body not proactively disclose the Report of the Investigation Panel, and for the Public Body to process an access to information request that was submitted to the Public Body, and follow the requirements of the *FOIPP Act* in processing the request. The Commissioner also recommended the Public Body consider certain mandatory and discretionary exceptions to disclosure.

The FOIPP Act provides a right to access information and a right of protection of privacy. Openness and transparency of government is desirable, but not at any expense. A public body has an obligation to balance the desire for openness and transparency and the right of access to information with the right of privacy, and the FOIPP Act provides the mechanism to achieve that balance.
- Commissioner, Order No. AR-21-001 at para 28

Decisions Resulting from Access Reviews

If an individual is not satisfied with the decision of a public body relating to their request for access, the individual may request a review by the Commissioner within 60 days of receiving the decision of the public body. Alternatively, a third party who is not satisfied with the decision of a public body to disclose information to an applicant, may request a review by the Commissioner within 20 days of receiving notice of the decision. The request for review must be in writing to the Office of the Information and Privacy Commissioner, and there is no fee.

Section 66 of the *FOIPP Act* authorizes the Commissioner to issue orders relating to access to information reviews. Four such orders were issued by the Commissioner and Adjudicator in 2021. Table A, on page 26, sets out the above statistics in detail.

FI-21-001, January 18, 2021

Re: Department of Economic Growth, Tourism and Culture

An applicant made a request for access to information to a Public Body, the Department of Economic Growth, Tourism and Culture. Responsive records included information of third parties. The Public Body conducted the required third-party consultations and decided to release the information to the applicant. Two third parties objected to the release of their information, and claimed that disclosure would be harmful to their business interests pursuant to section 14 of the *FOIPP Act*, and requested reviews by the Commissioner. Third Party 1's request for review was abandoned or withdrawn prior to decision. The Commissioner determined that Third Party 2 did not meet the burden of proof establishing that all three parts of the test set out in section 14 were met, and confirmed the decision of the Public Body to disclose the information to the applicant.

FI-21-002, May 7, 2021

Re: Department of Finance

An applicant requested access to information, and the responsive records included information of third parties. The Public Body conducted the required third-party consultations and decided to release the information to the applicant. A third party, who did not respond to the Public Body's request for consultation within the requested time, objected to the Public Body's decision to release their information, and complained that the Public Body should have given them more time to respond to the consultation request. The third party requested a review by the Commissioner, claiming that some of the pages were not "records" and therefore not subject to the *FOIPP Act*, and that disclosure of the records would be harmful to their business interests pursuant to section 14 of the *FOIPP Act*.

The Commissioner confirmed that the Public Body did not have authority to give the third party more time to respond to the consultation request than what was specified in the legislation. The Commissioner also determined that the records in issue were "records" and subject to the *FOIPP Act*, and found the third party did not meet the burden of proof establishing that all three parts of the test set out in section 14 of the *FOIPP Act* [harm to business interests] were met. The

Commissioner confirmed the decision of the Public Body to disclose the information to the applicant.

While the emails contain personal pleasantries, the records also contain information related to the Public Body's business. The emails discuss setting up meetings with government officials and other business involving government participation. Personal comments made in emails that otherwise pertain to business discussions involving government business does not disqualify the records from application of the FOIPP Act.

- Commissioner, Order No. FI-21-002 at para 30

FI-21-003, June 18, 2021

Re: Department of Economic Growth, Tourism and Culture

An applicant requested access to all records exchanged between a former CEO and a named employee, and all records of the CEO that mention a named private contractor, or a named company, for a five-month period in 2011. The Public Body provided the Applicant with responsive records, severing information under sections 15 (unreasonable invasion of personal privacy), and 22 (advice to officials) of the *FOIPP Act*. The Applicant requested a review regarding the Public Body's decisions to withhold information, and with respect to their duties to applicants pursuant to section 8 of the *FOIPP Act*.

The Commissioner found that the Public Body properly applied the exceptions to disclosure when making their decision to withhold information from the responsive records. The Commissioner also found that the Public Body had complied with their duties to the Applicant pursuant to section 8 of the *FOIPP Act*.

The FOIPP Act does not expressly place a burden of proof on one party or another with respect to a claim about whether a public body met its duty to assist an applicant under section 8 of the FOIPP Act. However, previous decisions from this office have held that the burden of proof for whether a public body has met its section 8 duties rests with the public body.

- Commissioner, Order No. FI-21-003 at para 22

I agree with the comments of Commissioner Rose that the burden of proof for a mandatory obligation of a public body is on the public body. It should be noted, though, that under section 8 of the FOIPP Act, the obligation of a public body to assist an applicant and to respond openly, accurately and completely, while mandatory, is not one of perfection. The public body must act reasonably. Because the duty is mandatory and it is the public body's obligation, it is the public body's responsibility to show that they acted reasonably with respect to their duty to assist an applicant and respond openly, accurately and completely. Although submissions from an applicant are also considered in making the assessment of whether a public body acted reasonably, the burden of proof regarding whether the public body met their duty under section 8 of the FOIPP Act lies with the public body.

- Commissioner, Order No. FI-21-003 at para 23

A public body's decision would not be reasonable if, for example, it can be established that the head of the public body made a decision in bad faith or for an improper purpose, or took into account irrelevant considerations, or failed to take into account relevant considerations. The head of a public body must

show that all relevant factors for and against access were considered in a balanced and judicious manner when making their determination ...

- Commissioner, Order No. FI-21-003 at para 52

The Applicant alleges that the Public Body intentionally delayed disclosing these records. The Applicant claims that the record is significant to their litigation claims against government, and asserts the Public Body therefore deliberately delayed disclosing these records for the purpose of interfering with their litigation.

I am not in a position to assess whether the record at issue is significant to the Applicant's litigation against government. Nor is the Applicant's claim that the record is significant to their litigation relevant to the determination of whether the Public Body met its duty under section 8 of the FOIPP Act. Even if I were to accept the Applicant's claims as accurate, for the purposes of this review, the relevant factor is whether there is evidence to substantiate that the Public Body deliberately delayed disclosure of the record.

- Commissioner, Order No. FI-21-003 at paras 79-80

FI-21-004, August 25, 2021

Re: Department of Economic Growth, Tourism and Culture

An applicant requested access to all records exchanged between a named employee of the Public Body and a named employee of another public body, or that made mention of a named third-party individual, for a six-month period. The Public Body claimed that some of the responsive records were subject to solicitor-client privilege, pursuant to section 25 of the *FOIPP Act*. The applicant objected to the Public Body's claim of solicitor-client privilege on the grounds that none of the parties named in the access to information requests were lawyers.

The Commissioner confirmed that, based on the affidavit and supplementary information provided by the Public Body, the Public Body was authorized to refuse access to the responsive records withheld pursuant to section 25 of the *FOIPP Act*.

The Applicant in this matter was unable to provide much in the way of specific evidence, and I did not expect any. Applicants are at a disadvantage when seeking a review of a public body's claim of solicitor-client privilege over a record. Records over which solicitor-client privilege is claimed are typically withheld from an applicant in their entirety, so applicants have little or no information about the content or context of the records. In the present matter, the Public Body withheld, in their entirety, all 36 pages of records over which they claimed solicitor-client privilege. The Applicant therefore had no opportunity to review the surrounding context of the withheld information and generally had very little to go on. Despite the lack of information about the withheld records, the Applicant made fairly extensive submissions regarding solicitor-client privilege in general, which were well thought out and well presented.

- Commissioner, Order No. FI-21-004 at para 21

The Public Body's position is that they provided sufficient evidence, which was "clear, cogent and convincing", in its initial affidavit and established that the records are subject to solicitor-client privilege. Respectfully, I disagree.

The Public Body provided minimal information in its affidavit to explain the contents of the records in issue and how solicitor-client privilege would apply. What was described as "details" in the affidavit was more an assertion of privilege, rather than details describing how privilege attached to the records. This assists little in assessing whether the claim of privilege was appropriately applied.

- Commissioner, Order No. FI-21-004 at paras 40-41

When a public body chooses not to provide to the Commissioner the records over which solicitor-client privilege is claimed, it is more difficult to meet their burden of proof in a review. An assertion of solicitor-client privilege is not sufficient. To meet their burden of proof for a claim of solicitor-client privilege, a public body must present sufficient evidence, which must show on a balance of probabilities that it is more likely than not that the records are subject to solicitor-client privilege.

It may be advisable, in some circumstances, for a public body to provide more evidence in the form of particulars of the records, or severed copies of the records without disclosing the information that is subject to solicitor-client privilege. This is particularly important if the public body is advised that more evidence is needed for the purpose of the review. The risk of a public body not providing enough evidence is that the public body might not persuade the Commissioner that they have properly claimed solicitor-client privilege.

- Commissioner, Order No. FI-21-004 at paras 43 and 44

I would not describe the evidence presented by the Public Body as "ample evidence". However, that is not the standard that the Public Body is required to provide. The Public Body is merely required to provide sufficient evidence to persuade me that, on a balance of probabilities, they applied clause 25(1)(a) of the FOIPP Act appropriately.

-Commissioner, Order No. FI-21-004 at para 51

Usually, if information a public body is authorized to refuse to disclose can be severed from a record, an applicant has a right of access to the remainder of the record. However, this does not apply to records subject to solicitor-client privilege. If a record is found to be subject to solicitor-client privilege, a public body is entitled to withhold the entire record.

-Commissioner, Order No. FI-21-004 at para 54

Decisions resulting from Privacy Complaints

An individual who believes that their privacy rights are not being protected by a public body, may make a written complaint to the Commissioner's office. The Commissioner is authorized to attempt to resolve such complaints. If the complaint cannot be resolved, the Commissioner will investigate and issue an order or investigation report. Four of the 13 privacy complaints made in 2021 were closed the same year, by way of resolution or refusal to conduct an investigation. Two orders were issued by the Adjudicator in privacy complaints from 2019 and 2020. Two privacy complaints from 2020 were brought forward to 2021. Table B, on page 27, sets out the above statistics in detail.

Order No. PP-21-001, March 9, 2021

Re: Health PEI

An employee worked in one area of the public body, but in their off hours, complained about the service in another area of the public body. The employee alleges that their employer disclosed this off-duty information to their manager (within the public body), contrary to the *FOIPP Act*.

The adjudicator found that the public body was authorized under clauses 37(1)(g) and (v) of the *FOIPP Act* to disclose the information to manage employees, specifically to address complaints about the Complainant. The adjudicator also found that the public body was authorized to use this information for the same purpose under clause 36(1)(c) of the *FOIPP Act*.

Order No. PP-21-002, September 29, 2021

Re: Department of Transportation and Infrastructure

The Complainant made an access to information request, and on review of the responsive records saw their name included in a couple of emails. The Complainant alleges that these instances are a breach of their privacy. One email is between employees of the Public Body who were working on the same matter. The Complainant's name was already known by the employees, so the adjudicator found that the employee of the Public Body did not "disclose" the personal information to their co-worker.

In the other email, the Complainant's name and an employee's opinion about the Complainant were disclosed to a private citizen. In the circumstances, the adjudicator found that disclosure of the personal information was not an unreasonable invasion of the Complainant's personal privacy, and the Public Body was authorized to disclose the personal information pursuant to clause 37(1)(a.1) of the *FOIPP Act*.

Voluntary Breach Reports, FOIPP Act

There is no provision in the *FOIPP Act* that provides for mandatory reporting of privacy breaches. However, some public bodies voluntarily notify the OIPC of investigations pertaining to privacy breaches they have experienced. In the event of a breach, the OIPC offers advice and guidance to the public bodies who have reported the breach.

The OIPC reviews the breach management procedures of public bodies in an attempt to ensure that appropriate measures have been put in place to prevent a similar breach in future. The following summaries reflect privacy breach reports voluntarily made to the OIPC by public bodies, which were closed in 2021. In all cases, the individuals affected by the breaches were notified by the public body.

BRF-19-017- Social Development and Housing (Child and Family Services)

The Public Body learned that an employee who had access to both current and historical child and family services files as part of their daily work had accessed various files without authorization, and had provided their own personal log-in information to a student performing on-the-job training under their supervision for the purposes of allowing the student to access files on ISM, the computer system used by this division for information management. ISM did not have a mechanism to disable or lock access to closed or inactive files. Shortly after the breach was discovered, the employee went on leave and did not return to work with this division.

The Public Body notified all affected individuals they had current contact information for regarding the breach, and voluntarily reported the breach to the OIPC. Child and Family Services updated its practices, began working with IT Shared Services to limit access to files stored in ISM, ensured that all hiring and student placements go through the HR office with training of all students on confidentiality and protection of privacy being normal practice upon hiring, and that confidentiality and protection of privacy expectations are outlined by HR and reviewed by the placement's supervisor. Child and Family Services also made plans to establish a quality and monitoring process on files as part of ongoing practice expectations, and that periodic checks of employees' access of client files is part of this audit work. Child and Family Services recognized the need to create a dedicated practice and procedure/policy to regularly conduct this work.

Based on the information provided by the Public Body, the Commissioner was satisfied that the incident involving the employee providing their personal log-in information to the student was an isolated incident that was solely the employee's decision, and not authorized or supported by the practice or policy of Child and Family Services or ITSS.

The Commissioner was also satisfied that the Public Body responded immediately to this breach, contained it, and put plans in place that would adequately mitigate risk of a similar breach of this nature from occurring in the future. The Commissioner recommended the Public Body do a final report to the affected individuals in relation to the steps the Public Body was taking to prevent risk of a similar breach from occurring in future.

BRF-20-022 - Justice and Public Safety (Emergency Measures Organization)

In 2020, the Public Body discovered a computer that may have been impacted during a malicious cyber incident had been reassigned to different employees after it had been put into service and had not been wiped between assignments. The original employee who was issued the computer had saved some of their own personal information to the computer and had not deleted it once their employment had ended in 2012. Their personal information was still on the computer each time it was reassigned, and when the cyber incident occurred.

The Public Body seized the computer and placed it in secure storage, notified the former employee (the “affected individual”) that their personal information may have been accessed by unauthorized individuals, and commenced an investigation.

After the investigation, the Public Body reported they were reasonably confident the affected individual’s personal information was not accessed during the cyber incident but were unable to confirm whether it was accessed by other individuals who had been assigned the computer after the affected individual. The Public Body scheduled the computer for destruction and offered the affected individual credit monitoring for a year to mitigate the effects of any potential unauthorized access.

The Public Body was unable to verify what policies existed in 2012 around reassignment of computers or whether any such policies were followed in this instance. However, the Public Body confirmed that there are currently policies in place that set out what steps are to be taken when an employee leaves their position and the computer they were using is reassigned.

The Commissioner was satisfied that the Public Body had sufficiently addressed any privacy issues that arose from these circumstances, and that the current policies were adequate.

BRF-20-026 - Social Development and Housing (AccessAbility Supports Program)

The Public Body learned of an incident where an inaccurately identified trustee had caused a cheque for AccessAbility supports to be sent to the wrong individual. The cheque disclosed to the recipient an individual’s name, the fact that they were receiving AccessAbility supports, and the amount they were receiving. The Public Body acknowledged that this was an unauthorized disclosure. The Public Body provided specific coaching to the employee and reinforced the importance of accuracy of information both to the employee and generally to all staff of the program area.

The Commissioner was satisfied that the Public Body adequately addressed the privacy concerns. During the course of the investigation, the Commissioner observed that the names of AccessAbility clients were included in file names and emails, and noted that this could be an unsafe practice for privacy, and suggested that the program may wish to review their file naming protocols.

BRF-20-027 - Social Development and Housing (AccessAbility Supports Program)

The Public Body learned of an incident in which an employee, who had two AccessAbility clients whose parents had the same name, was corresponding by email with the parent of one AccessAbility client believing it was the parent of the other client. The employee disclosed personal information of the other AccessAbility client and parent to this individual in their email.

The Public Body acknowledged that this was not an authorized disclosure, and verbally notified the affected individual of the unauthorized disclosure. The Public Body coached the employee and reinforced the importance of ensuring the employee is retrieving information from the correct file before communicating with a client. The Public Body also incorporated a practice of including the email addresses as an additional identifier for clients.

The Commissioner was satisfied that the Public Body adequately addressed the privacy concerns, but noted that it is quite common for a public body to be dealing with people with the same name and recommended the Public Body consider incorporating a policy requiring employees, with every file entry, and every communication with a client, to verify that they are working in the correct file with two factors of identification. The Commissioner suggested the Public Body periodically check for same names, and identify this fact in both files to alert employees of the risk of collecting, using or disclosing inaccurate personal information.

During the investigation, the Commissioner observed that the names of AccessAbility clients were included in file names and emails, and noted that this could be an unsafe practice for privacy, and suggested that the program may wish to review their file naming protocols as well.

The Commissioner also recommend that, in addition to the verbal notification, the Public Body follow up with the affected individual in writing and include particulars of the incident, remediation measures, the name and contact information of an individual within the Public Body to contact if the affected individual had questions, and the contact information for the Office of the Information and Privacy Commissioner.

BRF-20-028 - Justice and Public Safety (Attorney General's Office)

A person requested a copy of an autopsy report from the Public Body and provided a mailing address to receive the report. The Public Body located and mailed the report to the address provided. The same person contacted the Public Body a few weeks later, to ask if the report had been mailed, as they had not yet received it. It was then discovered that the requester had moved after requesting the report. However, they had not notified the Public Body they had moved or provided an updated mailing address. As the package had not been returned to the Public Body, and Canada Post was unable to locate it after conducting a search of their facilities, the Public Body considered this incident a privacy breach, and voluntarily reported it to the Office of the Information and Privacy Commissioner.

The Public Body put measures in place to avoid such occurrences in future, including calling requesters to confirm their mailing address before putting requested autopsy reports in the mail,

or requiring requesters to pick up the documents in person. The Commissioner was satisfied that the Public Body responded immediately to this breach, contained it, and that the outlined solutions would adequately mitigate risk of a similar breach of this nature in future.

BRF-20-029 - Public Schools Branch

In December 2020, the Public Body advised the affected individual that they had disclosed, in error, personal information about the affected individual when responding to an access to information request. The personal information was contained within a one-page record that was responsive to the access request, and the Public Body intended to sever it before disclosing the responsive records, but inadvertently missed severing it when processing the records. The Public Body contacted the applicant in the access request and asked them to delete the record containing the personal information and confirm when this was done, which they did, and the Public Body reissued the record with the personal information severed.

In their notification letter to the affected individual, the Public Body apologized, noted the breach was a result of human error, and indicated an intention to be more diligent in future. They also indicated they had sought guidance from the Office of the Information and Privacy Commissioner on how to proceed and advised the affected individual they had a right to request our office review the matter. However, the letter did not provide accurate contact information for our office, and the affected individual's name was misspelled.

The affected individual expressed concerns about the breach of privacy and the content of the notification letter. The Public Body responded the same day and provided the affected individual with more information about the breach and what steps they had taken to contain the breach and gave updated contact information for our office. They also indicated they were exploring the possibility of procuring technology that was specifically designed for the processing and severing of information, in order to assist in avoiding such errors in future.

The Commissioner was satisfied that the Public Schools Branch responded appropriately to this breach, contained it, and were taking steps to ensure mitigation of the risk of a future breach of this nature.

BRF-20-030 - Workers Compensation Board

The Public Body became aware of a privacy breach with respect to a mail-out error, after receiving a call from an employer who advised that they had received page 2 of another employer's Notice of Assessment in their package, which contained personal information of the other employer's employees. The employer was asked to return the incorrect page, and the Public Body commenced an investigation into the nature and scope of the mail-out error.

The Public Body determined that the mail-out error involved 28 employer packages. The Public Body contacted the 28 employers and requested that they return the pages with incorrect employee information. Not all employers had opened their packages yet, and the Public Body asked them to return their packages unopened. The Public Body determined 11 individuals were

affected by the privacy breach and notified them. Although not a breach of the employers' privacy, the Public Body also decided to notify the affected employers that their business information had been disclosed to other employers.

The Public Body was unable to identify a specific cause of the error but identified possible causes as: human or machine error in the page printing process, human error in inserting the pages into the envelope stuffing machine, or a malfunction of an envelope stuffing machine.

The Public Body also identified, as a contributing factor, that the technician did not follow the verification process in place at the time of the breach, which was designed to catch mail mismatch errors. In their report to our office, the Public Body indicated that if the verification process had been followed properly, the error would have been detected and the privacy breach avoided.

The Public Body provided targeted coaching to the technician on the required verification process and the importance of following procedures designed to protect personal information and prevent breaches. The Public Body recalibrated the envelope stuffing machine to stop at every 10th document to ensure the verification check is done, and also required the technicians to initial each count for additional accountability. All technicians were instructed on the process improvement and reminded of the importance of following procedure with the verification of every 10 documents.

The Commissioner was satisfied that the Public Body responded immediately to this breach, contained it, and that the outlined solutions will adequately mitigate risk of a similar breach of this nature in the future. The Commissioner recommended the Public Body do a final report to affected individuals on their findings and mitigation factors they have put in place.

BRF-21-031 - Justice and Public Safety (Probation Services)

A Youth Justice Worker employed by the Public Body reported that a briefcase containing personal information of five clients was stolen from the trunk of their vehicle overnight. The employee contacted the five affected individuals and their parents or guardians and notified them of the incident, apologized and assured them that every measure would be taken to ensure a similar incident did not occur in future. The employee also informed them of the right to file a complaint with the Office of the Information and Privacy Commissioner.

The employee reported the incident to their supervisor right away and took steps to find the briefcase. The briefcase was located in the backyard of a neighbour the same morning. The employee retrieved the briefcase, examined the files, and confirmed the files of the five affected individuals were accounted for and appeared untouched.

The Public Body reported that they had no specific policies and procedures regarding safety and security of files/personal information when it is necessary to transport confidential information, or with respect to handling transport of confidential information within the Youth Justice Services Division of the Public Body. However, they generally followed the departmental policy on documentation.

The Supervisor of Youth Justice Services met with all staff to discuss the incident, review current policies and discuss the importance of securing all confidential information, and the Public Body indicated the Supervisor would continue to have ongoing discussions with staff about Policies and Procedures with respect to securing, transporting and handling confidential information.

The Commissioner was satisfied that the employee had good reason for having files at home and that the files had been locked in the trunk of their car, but was concerned about the lack of policy and clear expectations of employees when transporting sensitive documents and personal information off-site. The Commissioner recommended the Public Body consider adding a policy specific to safety and security of personal information when not at a work site, during transport, etc. or adding to their current policy to clarify expectations for staff.

Given that the Public Body took swift action and, based on the information provided by the Public Body, the Commissioner was satisfied that the Public Body responded appropriately to this breach, contained it, and would take steps to ensure that the risk of a future breach of this nature will be avoided.

BRF-21-032 - Social Development and Housing (Child and Family Services)

The Public Body became aware of an unauthorized disclosure of personal information that occurred during a private social gathering. The report was that a Child and Family services employee with knowledge of the affected individual's circumstances disclosed to the host of the gathering that the affected individual, who was the host's current partner, was a former resident of a provincially-operated group home and had participated in certain confidential services provided by Child and Family Services. The affected individual learned about the breach from their partner, and brought it to the attention of the Child and Youth Care Worker Program at Holland College, who reported it to the Public Body.

The Public Body investigated the circumstances and confirmed the privacy breach did occur. The Public Body provided the affected individual the opportunity to participate in the investigation. The Public Body apologized for the breach and confirmed that they considered the circumstances to be a serious misconduct issue and had disciplined the employee.

To mitigate future risk, the Public Body took steps to promote awareness and training to ensure all employees of the Public Body are aware of the importance of privacy and their signed Oath of Confidentiality, and expectations to fulfill that Oath. The Public Body indicated that training and support for all staff was under review to ensure orientation for new employees around confidentiality, and to ensure ongoing training effectively supports this knowledge and the policy expectations.

The Commissioner was satisfied that the Public Body responded immediately to this breach, contained it, and that the outlined solutions would adequately mitigate risk of a similar breach of this nature in the future.

BRF-21-033 - Transportation and Infrastructure (Highway Safety Division)

The Public Body reported a privacy breach involving documents containing personal information of three individuals, including information about driver profiles, driver medical certificates, requests for re-examination and eye prescriptions. The documents had been in the possession of an employee who had been working in the field and required the documents as part of their work. When employee discovered the documents missing, they undertook an extensive search for them, and retraced their steps from their workday to look for them. The employee did not locate the documents and immediately reported the incident to their employer.

The Public Body notified the affected individuals in writing, with a brief description of the incident, an apology, and assurances that safeguards for personal information would be put in place to ensure a similar incident would not occur in future. The letters also informed the affected individual of their right to file a complaint with the Office of the Information and Privacy Commissioner. In addition, the Registrar and Deputy Registrar of Motor Vehicles met with each affected individual personally, gave each a letter outlining the circumstances of the breach, and showed them a copy of the missing documents pertaining to them.

The Commissioner was satisfied that the Public Body responded immediately to this breach, contained it, and would take steps to ensure that the risk of a future breach of this nature would be avoided. The Commissioner recommended that the Public Body consider adding a policy specific to safety and security of personal information when it is necessary to transport confidential information off-site for work purposes or adding to the Public Body's current policy to clarify expectations for staff regarding safety and security of files/personal information.

BRF-21-034 - Justice and Public Safety (Attorney General's Office)

The Public Body reported a privacy breach where an employee of the Prince County Hospital was inadvertently emailed a completed Autopsy Request Form containing personal information of another person instead of a blank form. When the recipient opened the email and discovered the form was already filled in, they contacted the Public Body to ask if it was sent by accident or as an example of what they were supposed to submit.

An Administrative Assistant confirmed the completed form was sent by accident and asked the recipient to delete the email and attachment. The Administrative Assistant then informed the Deputy Minister/Deputy Attorney General of the incident, and our office was notified. The Public Body wrote to the affected individual to notify them of the breach and the circumstances, apologized, and noted the Public Body took steps to ensure this does not happen again in the future.

Based on the information provided by the Public Body, the Commissioner was satisfied that the Public Body responded immediately to this breach, contained it, and would implement policy that will adequately mitigate risk of a similar breach of this nature in the future. The Commissioner recommended that, if the Public Body had not already done so as part of their remediation, they

consider implementing a blank file protocol which would make templates easier to find and attach to emails as examples.

The Commissioner also noted that the Public Body's letter to the affected individual indicated that they took steps to avoid an incident like this from happening in the future but did not spell out the steps taken, and recommended the Public Body provide more details in notification letters in future. Further, although the Public Body's letter to the affected individual indicated the breach had been reported to this office the individual was not advised they could make a privacy complaint to the Office of the Information and Privacy Commissioner, with contact information. The Commissioner suggested this information also be included in any correspondence regarding breach notifications in future.

BRF-21-035 - Justice and Public Safety (Access and Privacy Services Office)

The Public Body reported an incident where an employee of the Access and Privacy Services Office ("APSO") had inadvertently included unredacted records when scanning a decision letter and redacted records when responding to an access to information request, which were included in the attachments to an email sent to the applicant. The unredacted records contained personal information of three individuals that was not intended to have been disclosed to the applicant.

The breach was discovered the next morning, and the employee contacted the applicant, who indicated they had already opened the email and viewed the records. The employee requested the applicant delete the email and all attachments. The applicant confirmed by phone they had deleted the email with the attachments and had made no copies. The employee then resent the email with the correct decision letter and redacted records.

The employee contacted the three affected individuals by phone and email to notify them of the breach and apologized. A letter was sent to each of them offering an apology, advised the Office of the Information and Privacy Commissioner had been notified, and indicated that any recommendations made by this office would be accepted.

The Public Body advised that the breach was the result of human error and rushing to meet a deadline before a long weekend. It was noted that APSO's usual practice is to have all files reviewed twice before records are disclosed, once by the processing analyst and once by another analyst, but this step was missed in this instance.

The Commissioner was satisfied that the Public Body responded immediately to this breach, contained it, and was taking steps to ensure that the risk of a future breach of this nature would be avoided. The Commissioner observed that this was an inadvertent error and that her experience thus far with APSO was that the employees of that office are usually particularly vigilant regarding the collection, use, disclosure and security of personal information, especially when using email. The Commissioner noted that this breach exemplifies the importance of adhering to standard policies and procedures even in high-stress or time-sensitive situations.

BRF-21-036 - Justice and Public Safety (Probation Services)

The Public Body reported a potential privacy breach involving a missing file of a Probation Services client, which contained personal information of the client. The file was one of two files for the client and contained one page of case notes and one Probation Order. The other file for the client was not missing.

The circumstances reported were that a probation officer had met with the client at a Probation Services Office and had the file out during the meeting. During the meeting, the probation officer made some notes and placed the file back in the filing cabinet. The following week, the probation officer went to put some new documentation in the file but could not locate the file. The probation officer undertook an extensive search, including searching their office and home, and requested others to search their desks, offices, and filing cabinets, but the file was not located.

The Public Body considered the possibility the client had taken the file, as they had been left alone in the room for a period of time at the end of the meeting and had a lot of belongings in various bags in which the file could have been concealed, so would have had an opportunity to take it. The Public Body notified the client of the missing file, and what the contents of the file were, and advised the client they could make a complaint to the Office of the Information and Privacy Commissioner. They also inquired as to whether the client had taken the file, but the client denied this. The Public Body indicated that if the client did not have the file, it was likely still in the building but misfiled. The Public Body indicated it would continue looking for the file.

The Public Body notified the Office of the Information and Privacy Commissioner and the province's insurance and risk management program of the incident. The Commissioner was satisfied the Public Body responded appropriately to the potential breach and closed the file.

BRF-21-037 - Social Development and Housing (Child and Family Services)

The Public Body was advised by an employee they suspected their estranged spouse may have accessed a work cell phone that was in the employee's possession, and which had the capability to access the employee's government email account. The Public Body notified the Office of the Information and Privacy Commissioner of a potential breach and engaged with ITSS to investigate the circumstances. The cell phone was for emergency duty use only, had not been used by the employee for a number of months, and was password protected. An investigation provided no evidence of unauthorized access to the cell phone. The Public Body determined the complaint of a potential breach was not founded, and the Commissioner accepted this determination.

Comments of the OIPC

The OIPC encourages public bodies to be proactive in reporting privacy breaches to the Commissioner. The OIPC is able to assist by providing guidance or advice to reduce the chance of similar breaches occurring in future.

Decisions under the *Health Information Act*

Decisions resulting from access reviews

Under the *Health Information Act*, (“*HIA*”), if an individual is not satisfied with the decision of a custodian relating to their request for access to their own personal health information (PHI) or related to their request to correct their own PHI, the individual may request a review by the Commissioner. There were no decisions in relation to an *HIA* access review in 2021. Three access reviews were opened in 2021: two reviews were resolved and the other was carried forward to 2022.

Decisions resulting from privacy complaints

If an individual believes that their personal health information has been breached by a custodian, they may complain to the Commissioner. No decisions resulted from the two privacy complaints that were opened in 2021. Of the two files opened, both were brought forward to 2021. One complaint brought forward from 2020 resulted in an order by the Adjudicator.

Order No. HI-21-001, February 18, 2021, Re: *Health PEI*

The Health Information Act does not set out the onus of proof for matters related to collection, use or disclosure of personal health information. There is a mixed onus of proof with allegations of unauthorized disclosure of personal health information ... The same principles apply when reviewing a complaint of unauthorized access to personal health information. A complainant must show that the information is their personal health information, and that access occurred. If access has been shown, then the onus switches to the custodian, who must show that the access is authorized.

- Adjudicator, Order No. HI-21-001 at para 6

Decisions resulting from mandatory breach reporting

Section 64 of the *HIA* authorizes the Commissioner to issue orders relating to mandatory breach notifications by custodians. Six breach notifications were provided to the Commissioner by custodians in 2021. Of the six breach notifications, four were resolved and the other two were brought forward to 2021. One breach notification brought forward from 2019 was resolved in 2021 in addition to a breach notification brought forward from 2020.

Table C, on page 28, sets out the above statistics in detail.

Privacy Impact Assessments

As technology advances, there are ever more available and varied opportunities for organizations to utilize technological solutions to assist them with efficiencies in their work and customer service. Further, as technology has become so ingrained into our everyday lives, most people have become accustomed to its use and increasingly expect public bodies and custodians to offer online and other digital services, which are easily accessible at the consumer's own convenience. As a result, it has become much easier to collect, store, access, use, and disclose huge amounts of personal information. With the increasing expectations of the population to be able to easily and conveniently access services, the advancements in technology, and the vast amounts of personal information that can be collected by public bodies and custodians, it is more important than ever to assess the potential privacy risks of an organization's information practices.

A privacy impact assessment (PIA) is a process which helps an organization in identifying and managing the privacy risks arising from new projects, initiatives, technology systems, processes, strategies, policies, etc., including screening for factors that have potential for a widespread or serious impact on individuals, identifying and guiding the use of personal information across the organization, and identifying and mitigating potential information technology security risks. Done properly, and ideally before launching a new initiative, whether technological or otherwise, a PIA can help ensure that an organization is meeting its legal requirements and that potential privacy impacts are identified and either addressed or minimized before a problem occurs.

Health Information Act

Under section 25 of the *HIA*, it is mandatory for a custodian to prepare a PIA and submit it to the Commissioner for review and comment:

- (a) for the new collection, use or disclosure of personal health information (PHI) or any significant change to the collection, use or disclosure of PHI;
- (b) for the creation of, or significant modification to an existing, health information system or PHI communication technology; or
- (c) if a custodian performs data matching with PHI collected by it or with any PHI held by another custodian or another person.

In 2021, our office opened 32 PIA files. We believe there were likely more PIAs that should have been conducted and submitted to our office in 2021, particularly given the move by many health services providers to offer alternatives to in-person service delivery as a result of the pandemic and shortages of medical personnel, and implementation of a variety of technological assists for this purpose. Most of these "pivots" would have resulted in new collection or use of PHI and/or new or significant modification to existing communication technology, requiring a PIA to be conducted and submitted to our office for review and comment. We have observed an increase in PIAs coming in from custodians, but are aware there is still some work to do in this area around awareness of when a PIA should be conducted and submitted to our office.

Freedom of Information and Protection of Privacy Act

PIAs are not mandatory under the *FOIPP Act*, but some public bodies conduct PIAs and voluntarily submit them to our office for review and comment. In 2021, our office did not receive any voluntary PIAs from public bodies under the *FOIPP Act*.

Although not mandatory, we do strongly encourage public bodies to conduct a PIA any time they are undertaking a new initiative, implementing new technology, making significant changes to their existing technology, or engaging in a new or significant change to the collection, use or disclosure of personal information. We are also happy to review and comment on a PIA from a public body, if they choose to voluntarily submit it to our office. The process of conducting a PIA will assist a public body in identifying the impacts its programs and activities will have on individuals' privacy, identifying and effectively managing privacy risks, ensuring it is meeting its legal obligations, and is adhering to the basic principles of privacy protection.

Financial Information:

Budget:

This annual report covers activities of the office during the calendar year of 2021 in all respects except the budget. The reporting period of the budget is from April 1, 2021 to March 31, 2022. ¹

	2020-2021 Budget Forecast	2021-2022 Budget Estimate	2021-2022 Expenditures
Administration	4,900.00	4,900.00	4,907.00
Materials, Supplies, and Services	1,600.00	1,600.00	120.00
Professional Services	18,800.00	18,800.00	0.00
Salaries	287,000.00	295,000.00	295,156.00
Travel and Training	5,000.00	5,000.00	384.00
Total	317,300.00	325,300.00	300,567.00

The OIPC budget does not reveal all the operating expenses of the office, as some supplies and services the office receives are shared with other departments of the provincial government, including ITSS, Public Works and the Legislative Assembly (e.g. office space and utilities, photocopy paper, accounting services, printing services and IT support) and these costs are not reflected.

For information regarding Commissioner and staff expenses, which are included in the above list of expenditures, please refer to our website under "Proactive Disclosure". Due to website changes, this information is now posted under the heading "Transparency and Accountability".

¹ Some of this information is reproduced from page 150 of the *Prince Edward Island Estimates of Revenue and Expenditures 2021-2022*, at https://www.princeedwardisland.ca/sites/default/files/publications/budget_estimate_book_2020-2021_web.pdf

STATISTICS

**TABLE A – Summary of Requests for Review (Access to Information), FOIPP Act
January 1, 2021 – December 31, 2021**

Public Body	Carried over from 2020	2021 Requests /PIAs received	Resolved in 2021 without order/ decision	Withdrawn in 2021 without order/ decision	Refused in 2021 without order/ decision	Order/ Decision issued in 2021	Carried forward to 2022
Agriculture and Land	2	4	1	0	1	2	2
City of Charlottetown	2	5	0	0	0	0	7
City of Charlottetown (Police Services)	1	0	0	0	0	0	1
City of Summerside	1	0	1	0	0	0	0
Economic Growth, Tourism and Culture	13	2	1	0	0	3	11
Education, Early Learning and Culture	1	0	0	0	0	0	1
Education and Lifelong Learning	7	0	3	0	0	0	4
Environment, Energy and Climate Action	0	4	0	1	0	0	3
Executive Council Office (ECO)	2	0	0	0	0	0	2
ECO and Premier's Office	1	0	0	1	0	0	0
Finance	3	4	1	0	1	1	4
Fisheries and Communities	0	1	0	0	0	0	1
Health and Wellness	2	5	1	1	2	0	3
Health PEI	2	11	0	1	4	0	8
Island Regulatory and Appeals Commission	0	3	1	0	0	0	2
Justice and Public Safety	4	6	2	0	2	0	6
Mental Health Review Board (HW)	0	1	0	0	1	0	0
Office of the Child and Youth Advocate	0	1	1	0	0	0	0
Premier's Office	4	5	0	1	1	0	7
Public Schools Branch	3	0	0	0	0	0	3
Transportation, Infrastructure and Energy	5	2	1	1	0	0	5
Transportation and Infrastructure	0	10	1	0	1	0	8
UPEI	0	4	0	0	0	0	4
TOTAL	53	68	14	6	13	6	82

**TABLE B – Summary of Privacy Complaints, FOIPP Act
January 1, 2021 – December 31, 2021**

Public Body	Carried over from 2020	2021 Complaints	Resolved in 2021 without Investigation Report/ Order/ Decision	Refused in 2021 without Investigation Report/ Order/ Decision	Investigation Report/ Order/ Decision issued in 2021	Carried forward to 2022
City of Charlottetown	0	1	0	0	0	1
City of Summerside	1	0	0	0	0	1
Commission scolaire de langue française	0	2	1	0	0	1
Finance (ITSS)	1	0	0	0	0	1
Health and Wellness	0	5 (1 file with HPEI) (3 files with JPS)	0	2 (1 file with JPS)	0	3 (1 file with HPEI) (2 files with JPS)
Health PEI	1	4 (+ 1 file with HW)	1	0	1	3 (+ 1 file with HW)
Justice and Public Safety	0	(3 files with HW)	0	(1 file with HW)	0	(2 files with HW)
Transportation Infrastructure and Energy	2	0	0	0	1	1
Workers Compensation Board	0	1	0	0	0	1
TOTAL	5	13	2	2	2	12

**TABLE C – Summary of Reviews, Health Information Act
January 1, 2021 – December 31, 2021**

Custodian	Breach Reporting 2021 (BRH)	Access to Information Reviews 2021 (HIA)	Privacy Complaints 2021 (HIP)	Privacy Impact Assessment 2021 (PIA)	Carried Forward from 2020	Resolved/Refused/Closed in 2021	Report or Order issued in 2021	Carried forward to 2022
Health PEI	3 BRHs	3 HIAs	2 HIPs	4 PIAs	1 PIA 1 BRH 1 HIP	4 PIAs 3 BRHs 2 HIAs	1 HIP	1 PIA 1 BRH 1 HIA 2 HIPs
Can Immunize				2 PIAs		2 PIAs		
Emergency Services with Health PEI				1 PIA		1 PIA		
Nursing Home	1 BRH							1 BRH
Health and Wellness	1 BRH			2 PIAs		1 PIA 1 BRH		1 PIA
Education and Lifelong Learning				2 PIAs		1 PIA		1 PIA
Skip the Waiting Room				1 PIA		1 PIA		
Lab (National)					1 BRH	1 BRH		
Health PEI/Maple					1 PIA	1 PIA		
Maple				1 PIA				1 PIA
Pharmacies	1 BRH			15 PIAs		12 PIAs 1 BRH		3 PIAs
Optician				1 PIA		1 PIA		
Emergency services					1 PIA	1 PIA		
UPEI				3 PIAs		2 PIAs		1 PIA
TOTAL	6 BRHs	3 HIAs	2 HIPs	32 PIAs	6 3 PIAs 2 BRHs 1 HIP	35 27 PIAs 6 BRHs 2 HIAs	1 1 HIP	13 8 PIAs 2 BRHs 1 HIA 2 HIPs

Statistics of Public Bodies:

A list of public bodies and entities subject to the *FOIPP Act* can be found in Schedule 1 of the general regulations to the *FOIPP Act*, at pages 9 to 11. The public bodies in Part 1 of Schedule 1 are departments, branches and offices of the provincial government.

The Executive Council Office is not listed in the regulations, but it is specifically named in the definition of "public body" in the *FOIPP Act*.

Part II of Schedule 1 lists seven local public bodies which are included under the *FOIPP Act*. There are three educational public bodies listed and four municipal public bodies.

Part III of Schedule 1 lists over 88 designated public bodies which are included under the *FOIPP Act*.

Appendix A of this report sets out the number of access requests made to Part I public bodies in 2021. These statistics were provided by the Access and Privacy Services Office (APSO). The third column lists the number of reviews conducted by the OIPC for each public body, which information is also provided in Tables A and B on the previous pages.

Appendix B of this report sets out the number of access requests made to Part II local public bodies in 2021. The statistics for Appendix B were provided by the local public bodies, which include three educational public bodies and four municipal public bodies. This office received separate statistics from the City of Charlottetown and their police force. The statistics shown will reflect that. Once again, the third column lists the number of reviews conducted by the OIPC for each public body, which information is also provided in Tables A and B on the previous pages.

Appendix C sets out the number of access requests made to Part III public bodies in 2021. These statistics were provided by the Access and Privacy Services Office (APSO). The third column lists the number of reviews conducted by the OIPC for each public body, which information is also provided in Tables A and B on the previous pages.

It should be noted the requests for review to the OIPC in 2021 are not necessarily related to the same access requests recorded by a public body in 2021, as some may be reviews of 2020 decisions of public bodies. Further, the Appendices do not include informal responses to requests for access to information.

Appendix A: Schedule 1, Part I public bodies – Access Requests and Reviews

Public Body	Requests for access to records from public body, (general) 2021*	Requests for access to records from public body, (personal) 2021*	Requests for Review to OIPC, 2021
Agriculture and Land (AL)	22	0	4
Economic Growth Tourism and Culture (EGTC)	33	0 + 1 correction	2
Education and Lifelong Learning (ELL)	17	0	0
Environment, Energy and Climate Action (EECA)	29	0	4
Executive Council Office (EX)	15	0	0
Fisheries and Communities (FC)	8	0	1
Finance (FIN)	49	1	4
Health and Wellness (HW) Mental Health Review Board (MHRB)	72	3	5 1
Intergovernmental Affairs (IA)	3	0	0
Justice and Public Safety (JPS) Request to Disregard (JPS)	91	37	4 2
Premier's Office (PO)	35	1	5
PEI Public Service Commission (PSC)	4	0	0
Social Development and Housing (SDH)	25	11 + 1 correction	0
Transportation and Infrastructure	33	0	10
Transportation, Infrastructure and Energy (TIE)	2	0	2
TOTAL	440 access requests (general) to public bodies	53 access requests (personal) to public bodies and 2 correction requests	44 requests for review

*These statistics have been provided by the Access and Privacy Services Office.

**The number of total access review requests involving Part 1 public bodies is 44.

Appendix B: Schedule 1, Part II local public bodies - Access Requests and Reviews

Public Body	Requests for access to records from public body (general) 2021*	Requests for access to records from public body (personal) 2021*	Requests for Review to OIPC, 2021
City of Charlottetown	8	1	5
City of Charlottetown (Police Services)	18	18	0
City of Summerside	1	0	0
City of Summerside Police Services	4	1	0
Collège de l'Île	0	0	0
Holland College	0	1	0
Town of Cornwall	0	1	0
Town of Stratford	0	0	0
University of PEI	7	3	4
TOTAL	38 access requests to public bodies (general info)	25 access requests to public bodies (personal info)	9 access reviews

*Stats provided by each Public Body.

Appendix C: Schedule 1, Part III public bodies - Access Requests and Reviews

Public Body	Requests for access to records from public body (general) 2021 *	Requests for access to records from public body (personal) 2021 *	Requests for Review to OIPC, 2021
Elections PEI	0	0	0
Fathers of Confederation Buildings Trust	0	0	0
French Language School Board	0	0	0
Health PEI	71	16 + 4 corrections	11
Human Rights Commission	1	0	0
Island Waste Management Corporation	1	0	0
Island Regulatory and Appeals Commission	3	0	3
Office of the Child and Youth Advocate	0	0	1 (Advice)
PEI Cannabis Management Corporation	0	0	0
Office of the Police Commissioner	5	0	0
PEI Liquor Control Commission	3	0	0
Public Schools Branch	12	0	0
Workers Compensation Appeal Tribunal	0	0	0
Workers Compensation Board	4	0	0
TOTAL	100 access requests to public bodies (general info)	16 access requests to public bodies (personal info) + 4 correction requests	12 access reviews (including 1 advice file)

* These statistics have been provided by the Access and Privacy Services Office.